Features and Services Guide for Cisco Unified Communications Manager, Release 10.0(1)

First Published: 2013-12-03

Last Modified: 2020-11-12

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

Text Part Number: OL-27831-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

CONTENTS

PREFACE

CHAPTER 1

CHAPTER 49

Preface

This chapter provides information about the purpose, audience, organization, and conventions of this guide and provides information on how to obtain related documentation.

Note This document may not represent the latest Cisco product information available. You can obtain the most current documentation by accessing Cisco's product documentation page at `http://www.cisco.com/cisco/web/support/index.html` .

Purpose

The Cisco Unified Communications Manager Features and Services Guide provides the information that you need to understand, install, configure, manage, use, and troubleshoot Cisco Unified Communications Manager (formerly Cisco Unified CallManager) features.

Audience

The Cisco Unified Communications Manager Features and Services Guide provides information for network administrators who are responsible for managing the Cisco Unified Communications Manager system. This guide requires knowledge of telephony and IP networking technology.

Overview

The following table provides an overview of the organization of this guide.

Chapter	Description
Barge and Privacy, on page 1	Provides a description and configuration procedures for the Unified Communications Manager features Barge and Privacy.
Call Back, on page 39	Provides a description and configuration procedures for Cisco Call Back.
Call Control Discovery, on page 53	Provides a description and configuration procedures for the Call Control Discovery feature.
Call Display Restrictions, on page 103	Provides a description and configuration procedures for the Call Display Restrictions feature.
Call Park and Directed Call Park, on page 119	Provides a description and configuration procedures for the Unified Communications Manager Call Park and Directed Call Park features.
Call Pickup, on page 147	Provides a description and configuration procedures for the Unified Communications Manager Call Pickup feature.
Call Throttling and the Code Yellow State, on page 189	Provides a description of the call throttling feature and the service parameters you use to configure it.
Calling Party Normalization, on page 193	Provides a description of calling party normalization.
Extension Mobility, on page 463	Provides a description and configuration procedures for Cisco Extension Mobility for Unified Communications Manager.
Extension Mobility Cross Cluster, on page 497	Provides a description and configuration procedures for the Cisco Extension Mobility Cross Cluster feature for Unified Communications Manager.
Cisco Unified Communications Manager Assistant with Proxy Line Support, on page 305	Provides a description and configuration procedures for Cisco Unified Communications Manager Assistant (Cisco Unified CM Assistant) with proxy line support.
Cisco Unified Communications Manager Assistant with Shared Line Support, on page 345	Provides a description and configuration procedures for Cisco Unified Communications Manager Assistant (Cisco Unified CM Assistant) with shared line support.
Cisco Unified Communications Manager Auto-Attendant, on page 373	Provides a description and configuration procedures for Cisco Unified Communications Manager Auto-Attendant.
Cisco Unified Mobility, on page 233	Provides a description and configuration information for Cisco Unified Mobility, including the Mobile Connect and Mobile Voice Access features.

Chapter	Description
Cisco Jabber for Mobile, on page 298	Cisco Unified Communications Manager provides certain functionality for Cisco Mobile VoiP Clients that connect directly with Unified Communications Manager. This chapter discusses the features and the required configurations.
Web Dialer, on page 1093	Provides a description and configuration procedures for Cisco Web Dialer for Unified Communications Manager.
Client Matter Codes and Forced Authorization Codes, on page 379	Provides descriptions and configuration procedures for Client Matter Codes (CMC) and Forced Authorization Codes (FAC).
Custom Phone Rings, on page 389	Provides a description and configuration procedures for Unified Communications Manager custom phone rings.
Device Mobility, on page 393	Provides a description and configuration information for the Device Mobility feature.
Do Not Disturb, on page 413	Provides a description and configuration information for the Do Not Disturb feature.
External Call Control, on page 547	Provides a description and configuration information for the External Call Control feature.
External Call Transfer Restrictions, on page 567	Provides a description and configuration procedures for the External Call Transfer Restrictions feature.
Geolocations and Location Conveyance, on page 575	Provides a description and configuration procedures for geolocations, geolocation filters, and location conveyance.
Hold Reversion, on page 615	Provides a description and configuration information for the Hold Reversion feature.
Hotline, on page 629	Provides a description and configuration information for the Hotline feature.
Immediate Divert, on page 663	Provides a description and configuration procedures for the Unified Communications Manager Immediate Divert feature.
Intercom, on page 685	Provides a description and configuration information for the Unified Communications Manager Intercom feature.
Internet Protocol Version 6 (IPv6), on page 739	Provides information on IPv6 support for Unified Communications Manager and other components in the network.

Chapter	Description
	Provides a description of how licensing works with Unified Communications Manager.
Local Route Groups, on page 783	Provides a description and configuration procedures for the Local Route Groups feature.
Logical Partitioning, on page 795	Provides a description and configuration procedures for the Logical Partitioning feature.
Malicious Call Identification, on page 841	Provides a description and configuration procedures for the Unified Communications Manager Malicious Call Identification feature.
Monitoring and Recording, on page 851	Provides a description and configuration information for the call monitoring and call recording features.
Multilevel Precedence and Preemption, on page 907	Provides a description and configuration procedures for the Unified Communications Manager Multilevel Precedence and Preemption feature.
Music On Hold, on page 967	Provides a description and configuration procedures for Cisco Music On Hold.
BLF Presence, on page 17	Provides a description and configuration procedures for the Presence feature.
Quality Report Tool, on page 1029	Provides a description and configuration procedures for the Quality Report Tool (QRT) feature.
Single Sign-On, on page 1063	Provides a description of the Single Sign On feature.

Related Documentation

See the following documents for further information about related Cisco IP telephony applications and products:

- Installing Cisco Unified Communications Manager Release 8.6(1)
- Upgrading Cisco Unified Communications Manager Release 8.6(1)
- Cisco Unified Communications Manager Documentation Guide
- Release Notes for Cisco Unified Communications Manager Release 8.6(1)
- Cisco Unified Communications Manager System Guide
- Cisco Unified Communications Manager Administration Guide
- Cisco Unified Serviceability Administration Guide
- Cisco Unified Communications Manager Call Detail Records Administration Guide
- Cisco Unified Real-Time Monitoring Tool Administration Guide

- Troubleshooting Guide for Cisco Unified Communications Manager
- Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager
- Cisco Unified Communications Manager Bulk Administration Guide
- Cisco Unified Communications Manager Security Guide
- Cisco Unified Communications Solution Reference Network Design (SRND)

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in boldface.
italic font	Arguments for which you supply values are in italics.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in italic screen font.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords, are in angle brackets.
Action > **Reports**	Command paths in a graphical user interface (GUI).

Notes use the following convention:

Note Means reader take note. Notes contain helpful suggestions or references to material not covered in the publication.

Timesavers use the following conventions:

Note Timesave means the described action saves time. You can save time by performing the action described in the paragraph.

Tips use the following conventions:

Tip Means the information contains useful tips.

Cautions use the following convention:

Caution Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

Warnings use the following conventions:

Warning This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents.

Additional Information

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What’s New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at `http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html`.

Subscribe to the What’s New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Cryptographic Features

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

Further information regarding U.S. export regulations may be found at `http://www.access.gpo.gov/bis/ear/ear_data.html`.

CHAPTER 1

Barge and Privacy

This chapter provides information about how the single button barge/cBarge, barge, privacy, and privacy on hold features work with each other. These features work with only shared lines.

Barge adds a user to a call that is in progress. Pressing a softkey or feature button automatically adds the user (initiator) to the shared-line call (target), and the users currently on the call receive a tone (if configured). Barge supports built in conference and shared conference bridges.

The single button barge/cBarge feature allows the user to simply press the shared-line button to be added to the call. The single button barge/cBarge feature supports built in conferences and shared conference bridges.

The administrator enables or disables privacy and privacy on hold features. Privacy must be enabled for a device to activate privacy on hold. Users toggle the privacy feature on or off.

You enable or disable the privacy setting. When privacy is enabled, the system removes the call information from all phones that share lines and blocks other shared lines from barging in on its calls. When privacy is disabled, the system displays call information on all phones that have shared line appearances and allows other shared lines to barge in on its calls. You can configure privacy for all devices or configure privacy for each device. Users toggle the privacy feature on or off.

The privacy on hold feature preserves privacy when a private call on a shared line is put on hold. When privacy on hold is enabled, the calling name and number that are blocked when privacy is enabled remain blocked when the call is put on hold, and the system blocks other shared lines from resuming the held call. When privacy on hold is disabled and a private call is put on hold, the system displays calling name and number on all phones that have shared line appearances and allows other shared lines to resume the held call.

If privacy on hold is enabled, users can activate the feature while the call is on hold by toggling privacy on; likewise, users can deactivate privacy on hold by toggling privacy off while the call is on hold. If privacy on hold is disabled, toggling privacy on or off does not affect the held call.

If a private call is put on hold, retrieved at the same phone, and privacy is then toggled off, the system displays the call information on all phones that have shared line appearances but does not allow another phone to resume or barge the held call.

Administrators can configure privacy for all devices or for each device.

Configure Barge

The single button barge/cBarge, barge, privacy, and privacy on hold features work with each other. These features work with only shared lines.

Barge adds a user to a call that is in progress. Pressing a softkey or feature button automatically adds the user (initiator) to the shared-line call (target), and the users currently on the call receive a tone (if configured). Barge supports built in conference and shared conference bridges.

The single button barge/cBarge feature allows the user to simply press the shared-line button to be added to the call. The single button barge/cBarge feature supports built in conferences and shared conference bridges.

Perform the following steps to configure the barge feature with built in conference bridge.

Procedure

Step 1 Assign the Standard User or Standard Feature softkey template (both contain the barge softkey) to each device that accesses barge by using the built in conference bridge.

For more information, see topics related to configuring Cisco Unified IP Phones in the *Cisco Unified Communications Manager Administration Guide*

Step 2 Set the following optional Cisco CallManager service parameters:

a) To enable barge for all users, 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 Phone Configuration

b) Set the Party Entrance Tone clusterwide service parameter to True (required for tones) (or configure the Party Entrance Tone setting per directory number in the Directory Number Configuration window)

c) To enable single button barge for all users, 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 Phone Configuration

d) To allow a user to barge into a call when the phone is ringing or when the call is connected (the barger hears a ringback tone), set the Allow Barge When Ringing service parameter to True.

For more information. see topics related to configuring Cisco Unified IP Phones, service parameters for a service on a server, and directory number configuration settings in the *Cisco Unified Communications Manager Administration Guide*.

Step 3 In the End User Configuration window for each user that is allowed to access the barge with built-in conference bridge feature, associate the device that has the barge softkey template that is assigned to it.

For more information, see topics related to end user configuration in the *Cisco Unified Communications Manager Administration Guide*.

Step 4 Notify users that the barge feature is available.

See the phone documentation for instructions on how users access barge on their Cisco Unified IP Phone.

Related Topics

Party Entrance Tone, on page 8

Configure cBarge

The single button barge/cBarge, barge, privacy, and privacy on hold features work with each other. These features work with only shared lines.

Barge adds a user to a call that is in progress. Pressing a softkey or feature button automatically adds the user (initiator) to the shared-line call (target), and the users currently on the call receive a tone (if configured). Barge supports built in conference and shared conference bridges.

The single button barge/cBarge feature allows the user to simply press the shared-line button to be added to the call. The single button barge/cBarge feature supports built in conferences and shared conference bridges.

Perform the following steps to configure barge with shared conference bridge.

Procedure

Step 1 To create a softkey template that includes cBarge, make a copy of the Standard Feature softkey template. Modify this user-named copy to add the conference barge (cBarge) softkey to the Selected Softkeys in the Remote in Use call state.

See the *Cisco Unified Communications Manager Administration Guide* for more information on creating copies of standard softkey templates.

Step 2 Set the optional clusterwide service parameter Party Entrance Tone to True (required for tones), or configure the Party Entrance Tone setting per directory number in the Directory Number Configuration window. To enable single button cBarge for all users, 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 Phone Configuration

For more information, see the*Cisco Unified Communications Manager Administration Guide.*

Step 3 In the End User Configuration window for each user that is allowed to access the cBarge with shared conference bridge feature, associate the device that has the cBarge softkey template that is assigned to it. Disable privacy on phones to allow cBarge.

For more information, see the *Cisco Unified Communications Manager Administration Guide.*

Step 4 Notify users that the cBarge feature is available.

See the phone documentation for instructions on how users access cBarge on their Cisco Unified IP Phone.

Configure Privacy and Privacy on Hold

The single button barge/cBarge, barge, privacy, and privacy on hold features work with each other. These features work with only shared lines.

The privacy on hold feature preserves privacy when a private call on a shared line is put on hold. When privacy on hold is enabled, the calling name and number that are blocked when privacy is enabled remain blocked when the call is put on hold, and the system blocks other shared lines from resuming the held call. When privacy on hold is disabled and a private call is put on hold, the system displays calling name and number on all phones that have shared line appearances and allows other shared lines to resume the held call.

You enable or disable the privacy setting. When privacy is enabled, the system removes the call information from all phones that share lines and blocks other shared lines from barging in on its calls. When privacy is disabled, the system displays call information on all phones that have shared line appearances and allows other shared lines to barge in on its calls. You can configure privacy for all devices or configure privacy for each device. Users toggle the privacy feature on or off.

If privacy on hold is enabled, users can activate the feature while the call is on hold by toggling privacy on; likewise, users can deactivate privacy on hold by toggling privacy off while the call is on hold. If privacy on hold is disabled, toggling privacy on or off does not affect the held call.

If a private call is put on hold, retrieved at the same phone, and privacy is then toggled off, the system displays the call information on all phones that have shared line appearances but does not allow another phone to resume or barge the held call.

You can configure privacy for all devices or for each device.

Procedure

Step 1 If all phones in the cluster need access to privacy, keep the setting of the Privacy Setting clusterwide service parameter to True (default) and keep the Privacy field in the Phone Configuration window to Default. Continue with the following steps. If only certain phones in the cluster need access to privacy, set the Privacy Setting service parameter to False and set the Privacy field in the Phone Configuration window to On. Continue with the following steps.

For more information, see topics related to configuring Cisco Unified IP Phones and service parameters for a service on a server in the *Cisco Unified Communications Manager Administration Guide*.

Step 2 For each phone button template that has privacy, add Privacy to one of the feature buttons (some phone models use the Private button).

For more information, see topics related to phone button template configuration in the *Cisco Unified Communications Manager Administration Guide*.

Step 3 For each phone user that wants privacy, choose the phone button template that contains the Privacy feature button.

For more information, see topics related to configuring Cisco Unified IP Phones in the *Cisco Unified Communications Manager Administration Guide*.

Step 4 In the End User Configuration window, for each user that does not want information about the shared-line appearances to display, associate the device that has the Privacy feature button that is assigned to it.

For more information, see topics related to end user configuration in the *Cisco Unified Communications Manager Administration Guide*.

Step 5 To configure the optional privacy on hold feature, set the Enforce Privacy Setting on Held Calls service parameter to True.

For more information, see topics related to configuring service parameters for a service on a server in the *Cisco Unified Communications Manager Administration Guide*.

Step 6 Notify users that the privacy feature and the privacy on hold feature (if configured) are available.

See the phone documentation for instructions on how users access privacy on their Cisco Unified IP Phone.

Related Topics

Barge Privacy and Privacy on Hold, on page 5
Barge and Privacy, on page 1

Barge Privacy and Privacy on Hold

This section describes barge, single button barge/cBarge, privacy, and privacy on hold.

Barge

Barge allows a user to get added to a remotely active call that is on a shared line. Remotely active calls for a line comprise active (connected) calls that are made to or from another device that shares a directory number with the line. Barge supports this type of remote-in-use call.

Phones support barge in two conference modes:

- Built-in conference bridge at the target device (the phone that is being barged). This mode uses the barge softkey.
- 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 gets added to the call with all parties, and all parties receive a barge beep tone (if configured). If barge fails, the original call and status remain active.

If no conference bridge is available (built-in or shared), the barge request gets rejected, and a message displays at the barge initiator device.

Single Button Barge/cBarge

The single button barge/cBarge feature allows a user to simply press the shared-line button of the remotely active call, to be added to the call with all parties. All parties receive a barge beep tone (if configured). If barge fails, the original call and status remain active.

Phones support single button barge/cBarge in two conference modes:

- Built-in conference bridge at the target device (the phone that is being 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 gets added to the call with all parties, and all parties receive a barge beep tone (if configured). If barge fails, the original call and status remain active.

If no conference bridge is available (built-in or shared), the barge request gets rejected, and a message displays at the barge initiator device.

This table describes the differences between barge with built-in conference bridge and shared conference.

Table 1: Built-In and Shared Conference Bridge Differences

Action	Using Barge Softkey or Single Button Barge (Built In Conference Bridge at Target Device)	Using cBarge Softkey or Single Button cBarge (Shared Conference Bridge)
The standard softkey template includes the 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
User receives a barge setup tone, if configured.	Yes	Yes
To Conference displays as the name at the barge initiator phone.	To barge XXX	To Conference
To Conference displays as the name at the target phone.	To/From Other	To Conference
To Conference displays as the name 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.

Action	Using Barge Softkey or Single Button Barge (Built In Conference Bridge at Target Device)	Using cBarge Softkey or Single Button cBarge (Shared Conference Bridge)
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.

Built In Conference

You can use single button barge or the barge softkey only in the remote-in-use call state. A Built In conference bridge proves advantageous because neither a media interruption nor display changes to the original call occur when the barge is being set up.

Note To use the single button barge feature, ensure that single button barge is enabled on the device.

When the barge initiator releases the call, the barge call gets released between the barge initiator and target. The original call between the target device and the other party remains active. A barge disconnect tone (beep beep) plays to all remaining parties.

When the target device releases the call, the media between the barge initiator and the other party gets dropped briefly and then reconnects as a point-to-point call. The display changes at the barge initiator device to reflect the connected party.

When the other party releases the call, both the original call and the barge call get released.

When the barge initiator puts the call on hold, both the target device and the other party remain in the call.

When the target device puts the call on hold or in a conference or transfers it, the barge initiator gets released from the barge call while the original call also gets put on hold, in a conference, or transferred. The barge initiator can barge into a call again after the media gets reestablished at the target.

When the other party puts the call on hold or in a conference or transfers it, both the target device and the barge initiator remain in the call.

When network or Cisco Unified Communications Manager failure occurs, the barge call gets preserved (like all active calls).

Most Cisco Unified IP Phones include the Built In conference bridge capability, which barge uses.

Note Cisco Unified IP Phones 7940 and 7960 cannot support two media stream encryptions or SRTP streams simultaneously. To prevent instability due to this condition, the system automatically disables the Built In bridge for Cisco Unified IP Phones 7940 and 7960 when the device security mode is set to encrypted. For more information, see the *Cisco Unified Communications Manager Security Guide*.

The following settings activate or deactivate the built-in conference bridge:

- Enable or disable the built-in bridge by setting the Cisco Unified Communications Manager clusterwide service parameter, Built-in Bridge Enable, to On or Off.
- Enable or disable the built-in bridge for each device by using the Built In Bridge drop-down list box in the Phone Configuration window (choose on, off, or default). On or off settings override the Built-in Bridge Enable service parameter. Choosing default uses the setting of the service parameter.

Note To use barge with a built-in bridge, ensure the preceding items are enabled, privacy is disabled, and the barge softkey is assigned to each device or the single button barge feature is enabled. Otherwise, to use shared conference bridge, assign the cBarge softkey to each device or enable the single button cBarge feature.

For more information, see Barge Privacy and Privacy on Hold Configuration, on page 16.

Shared Conference

You can use single button cBarge or the cBarge softkey only in the remote-in-use call state. No standard softkey template includes the cBarge softkey. To access the cBarge softkey, the administrator adds it to a softkey template and then assigns the softkey template to a device.

Note To use the single button cBarge feature, ensure that it is enabled on the device.

When the cBarge softkey, or a shared-line, gets pressed, 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, which causes a brief media interruption. The call information for all parties gets changed 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 from the call, which leaves 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.

For more information, see Barge Privacy and Privacy on Hold Configuration, on page 16.

Phone Display Messages

When a user initiates a barge to a SIP device, the barge initiator phone displays “To Barge <Display name> (Shared Line DN).”

When a user initiates a barge to a SCCP device, the barge initiator phone displays “To Barge <Display name>.”

Party Entrance Tone

With the party entrance tone feature, a tone plays on the phone when a basic call changes to a multiparty call; that is, when a basic call changes to a barged call, cBarged call, ad hoc conference, meet-me conference, or a joined call. In addition, a different tone plays when a party leaves the multiparty call.

If the controlling device, that is, the originator of the multiparty call has a built-in bridge, the tone gets played to all parties if you configured party tone entrance for the controlling device. When the controlling device leaves the call, Cisco Unified Communications Manager identifies whether another device on the call can play the tone; if another device on the call can play the tone, Cisco Unified Communications Manager plays the tone. If the controlling device cannot play the tone, Cisco Unified Communications Manager does not play the tone even if you enable the party entrance tone feature.

When a barge call gets created, the party entrance tone configuration of the barge target that shares the line with the barge initiator determines whether Cisco Unified Communications Manager plays the party entrance tone.

When a cBarge call gets created, the party entrance tone configuration of the cBarge target that shares the line with the cBarge initiator determines whether Cisco Unified Communications Manager plays the party entrance tone. However, if the call for the target is an existing ad hoc conference that is in the same cluster, the party entrance tone configuration for the ad hoc conference controller determines whether Cisco Unified Communications Manager plays the tone.

To use the party entrance feature, ensure that you turned the privacy feature off for the devices and ensure that the controlling device for the multiparty call has a built-in bridge. In addition, either configure the Party Entrance Tone service parameter, which supports the Cisco CallManager service, or configure the Party Entrance Tone setting per directory number in the Directory Number Configuration window (Call Routing > Directory Number). For information on the service parameter, click the question-mark button in the Service Parameter Configuration window. For information on the Party Entrance Tone setting in the Directory Number Configuration window, see topics related to directory number configuration settings in the *Cisco Unified Communications Manager Administration Guide*.

Privacy

With privacy, you can enable or disable the capability of users with phones that share the same line (DN) to view call status and to barge the call. You enable or disable privacy for each phone or for all phones.

By default, the system enables privacy for all phones in the cluster. To enable all phones with privacy, leave the clusterwide service parameter set to True and leave the phone privacy setting set to default.

To configure certain phones with access to privacy, you perform the following steps to enable or disable privacy:

- Set a service parameter.
- Set the phone privacy setting to On.
- Add privacy button to phone button template.
- Add the phone button template that has privacy button to each device.

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 shows 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.

Privacy On Hold

With the privacy on hold feature, administrators can enable or disable the capability of users with phones that share the same line (DN) to view call status and retrieve calls on hold.

Administrators enable or disable privacy on hold for all phones. To enable privacy on hold, you must also enable the privacy feature for the phone or for all 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 enable all phones with privacy on hold, set the clusterwide privacy service parameter to True, set the clusterwide Enforce Privacy Setting on Held Calls service parameter to True, and leave the phone privacy setting to default.

To configure certain phones with access to privacy on hold, administrators set the Enforce Privacy Setting on Held Calls service parameter to True and set the Privacy setting for the phone to True:

- Set the Enforce Privacy Setting on Held Calls service parameter to True.
- Set a Privacy service parameter.
- Set the phone privacy setting to On.
- Add privacy button to phone button template.
- Add the phone button template that has privacy button to each device.

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 put the call on hold displays the status indicator for a held call; shared lines display the status indicators for a private and held call.

System Requirements for Barge Privacy and Privacy on Hold

The barge and privacy features require the following software component to operate:

- Cisco Unified Communications Manager 5.0 or later

The single button barge/cBarge and privacy on hold features require the following software component to operate:

- Cisco Unified Communications Manager 6.1(1) or later

To determine IP Phone support for the following features, see the related topics:

- IP Phones supporting Barge by using the single button barge/cBarge feature or the barge or cBarge softkey
- IP Phones supporting privacy with the Privacy button on the phone button template
- IP Phones supporting the built-in conference bridge capability

Note If the phone does not support a Privacy button, by default, the privacy for that phone remains Off (all devices sharing a line with that phone will display the phone information).

Related Topics

Report Support for Devices, on page 11

Report Support for Devices

Use the Cisco Unified Reporting application to generate a complete list of IP Phones that support barge and privacy. To do so, follow these steps:

1. Start Cisco Unified Reporting by using any of the methods that follow.

   The system uses the Cisco Tomcat service to authenticate users before allowing access to the web application. You can access the application

   - by choosing **Cisco Unified Reporting** in the **Navigation** menu in Cisco Unified Communications Manager Administration and clicking **Go.**
   - by choosing **File** > **Cisco Unified Reporting** at the **Cisco Unified Real Time Monitoring Tool** (RTMT) menu.
   - by entering https://<server name or IP address>:8443/cucreports/ and then entering your authorized username and password.

2. Click **System Reports** in the navigation bar.
3. In the list of reports that displays in the left column, click the **Unified CM Phone Feature List** option.
4. Click the **Generate a new report** link to generate a new report, or click the **Unified CM Phone Feature List** link if a report already exists.
5. To generate a report of all IP Phones that support built-in bridge, choose these settings from the respective drop-down list boxes and click the **Submit** button:

   Product: All

   Feature: Built In Bridge

   The List Features pane displays a list of all devices that support the built-in bridge feature. You can click on the Up and Down arrows next to the column headers (Product or Protocol) to sort the list.

6. To generate a report of all devices that support privacy, choose these settings from the respective drop-down list boxes and click the **Submit** button:

   Product: All

   Feature: Privacy

   The List Features pane displays a list of all devices that support the Privacy feature. You can click on the **Up** and **Down** arrows next to the column headers (Product or Protocol) to sort the list.

7. To generate a report of all devices that support single button barge, choose these settings from the respective drop-down list boxes and click the **Submit** button:

   Product: All

   Feature: Single Button Barge

   The List Features pane displays a list of all devices that support the Single Button Barge feature. You can click on the **Up** and **Down** arrows next to the column headers (Product or Protocol) to sort the list.

For additional information about the Cisco Unified Reporting application, see the *Cisco Unified Reporting Administration Guide*.

Interactions and Restrictions

This section describes the interactions and restrictions for barge, privacy, and privacy on hold.

Interactions

This section describes how barge and privacy interact with Cisco Unified Communications Manager applications and call processing features.

Barge and 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 avoid confusion for users and potential performance issues.

Note You can enable single button barge or single button cBarge for a device, but not both.

Barge and 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).

Barge and 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).

Configure PLAR

A barge, cBarge, or single button barge initiator can barge into a call via a shared line that is configured for PLAR; that is, 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 no matter what the state of the PLAR destination is.

To make barge, cBarge, or single button barge work with PLAR, you must configure barge, cBarge, or single button barge, as described in the Configure Barge, on page 2. In addition, you must configure the PLAR destination, a directory number that is used specifically for PLAR. The following example describes how to enable PLAR functionality for phones that are running SCCP and for phones that are running SIP.

A and A’ represent shared-line devices that you configured for barge, cBarge, or single button barge, and B1 represents the directory number for the PLAR destination. To enable PLAR functionality from A/A’, which are running SIP, see the following example:

Example for How to Configure PLAR

Procedure

Step 1 Create a partition, for example, P1, and a calling search space, for example CSS1, so CSS1 contains P1. (In Cisco Unified Communications Manager Administration, choose **Call Routing** > **Class of Control** > **Partition** or **Calling Search Space**.)

Step 2 Create a translation pattern, for example, TP1, which contains calling search space CSS1 and partition P1. Create a null pattern (blank pattern), but make sure that you enter the directory number for the B1 PLAR destination in the Called Party Transformation Mask field. (In Cisco Unified Communications Manager Administration, choose **Call Routing** > **Translation Pattern**.)

Step 3 Assign the calling search space, CS1, to either A or A'. (In Cisco Unified Communications Manager Administration, choose **Device** > **Phone**.)

Step 4 Assign the P1 partition to the directory number for B1, which is the PLAR destination. (In Cisco Unified Communications Manager Administration, choose **Call Routing** > **Directory Number**.)

Step 5 For phones that are running SIP, create a SIP dial rule. (In Cisco Unified Communications Manager Administration, choose **Call Routing** > **Dial Rules** > **SIP Dial Rules**. Choose 7940_7960_OTHER. Enter a name for the pattern; for example, PLAR1. Click **Save**; then, click **Add Plar**. Click **Save**.)

Step 6 For phones that are running SIP, assign the SIP dial rule configuration that you created for PLAR to the phones, which, in this example, are A and A'. ((In Cisco Unified Communications Manager Administration, choose **Device** > **Phone**. Choose the SIP dial rule configuration from the SIP Dial Rules drop-down list box.)

Restrictions

The following restrictions apply to Barge:

- The barge initiator cannot conference in additional callers.
- To enhance performance, disable built-in bridge or turn on privacy for those devices that do not have shared-line appearances or do not use Barge.
- CTI does not support Barge through APIs that TAPI/JTAPI applications invoke. CTI generates events for barge when it is invoked manually from an IP phone by using the barge or cBarge softkey.
- Cisco recommends that you do not configure cBarge for a user who has barge configured. Choose only one barge method for each user.
- The original call requires G.711 codec. If G.711 is not available, use cBarge instead.
- 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.
- Barge supports most Cisco Unified IP Phones that run SIP.
- A user cannot barge into an encrypted call if the phone that is used to barge is not configured for encryption. When barge fails in this case, a busy tone plays on the phone where the user initiated the barge.

  If the initiator phone is configured for encryption, the barge initiator can barge into an authenticated or nonsecure call from the encrypted phone. After the barge occurs, Cisco Unified Communications Manager classifies the call as nonsecure.

If the initiator phone is configured for encryption, the barge initiator can barge into an encrypted call, and the phone indicates that the call state equals encrypted.

A user can barge into an authenticated call, even if the phone that is used to barge is nonsecure. The authentication icon continues to display on the authenticated devices in the call, even if the initiator phone does not support security.

Tip You can configure cBarge if you want barge functionality, but Cisco Unified Communications Manager automatically classifies the call as nonsecure.

- 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.

  A message displays in Cisco Unified Communications Manager Administration when you attempt the following configuration:

  - In the Phone Configuration window, you choose Encrypted for the Device Security Mode (or System Default equals Encrypted), On for the Built In Bridge setting (or default setting equals On), and you click Insert or Update after you create this specific configuration.
  - In the Enterprise Parameter window, you update the Device Security Mode parameter.
  - In the Service Parameter window, you update the Built In Bridge Enable parameter.
- 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.

The following restrictions apply to privacy:

- To enhance performance, disable built-in bridge or turn on privacy for those devices that do not have shared-line appearances or do not use barge.
- CTI does not support privacy through APIs that TAPI/JTAPI applications invoke. CTI generates events when privacy gets enabled or disabled from an IP phone by using the privacy feature button.
- Privacy supports most Cisco Unified IP Phones that run SIP.

The following restriction applies to built-in conference bridge:

- To enhance performance, disable built-in bridge or turn on privacy for those devices that do not have shared-line appearances or do not use barge.
- The initiator cannot park a call, redirect a call, or use any feature that is using the CTI/JTAPI/TSP interface. The system supports only hold and unhold.
- Built-in conference bridge supports most Cisco Unified IP Phones that run SIP.

The following restrictions apply to privacy on hold:

- 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.

Related Topics

Report Support for Devices, on page 11

Install and Activate Barge, Privacy, and Privacy On Hold

Barge, privacy, and privacy on hold system features come standard with Cisco Unified Communications Manager software. The administrator activates the features after installation to make them available for system use. This section provides instructions to activate barge, privacy, and privacy on hold features.

Activate Barge

To activate barge with a built-in conference bridge, add the barge softkey to a softkey template, assign the softkey template to a device, set the Built-in Bridge Enable service parameter to On, and set the party entrance tone to True. To activate the single button barge feature, you must also enable it in the Device Profile Configuration window. See the Configure Barge, on page 2 for details.

Note To set barge with built-in conference bridge for all users, set the Built-in Bridge Enable service parameter to On. To set barge with built-in conference bridge for individual users, set the Built in Bridge field to On in the Phone Configuration window.

Activate cBarge

To activate barge with shared conference bridge, add the cBarge softkey to a softkey template, assign the softkey template to a device, and set the party entrance tone to True. To activate the single button cBarge feature, you must also enable it on the Device Profile Configuration window. See the Configure Barge, on page 2 for details.

Activate Privacy

The system automatically activates privacy in the Cisco Unified Communications Manager because the Privacy Setting service parameter is set to True and the phone has the privacy setting at Default. You must also add privacy to a phone button template and assign the phone button template to a device. See the Configure Privacy and Privacy on Hold, on page 4 for details.

Activate Privacy on Hold

The system automatically activates privacy on hold in the Cisco Unified Communications Manager when the Enforce Privacy Setting on Held Calls service parameter is set to True and the phone has the privacy feature that is configured.

See the Configure Privacy and Privacy on Hold, on page 4 for details.

Barge Privacy and Privacy on Hold Configuration

This section provides information to configure barge, privacy, and privacy on hold.

Tip Before you configure barge or privacy, see the Configure Barge, on page 2 and the Configure Privacy and Privacy on Hold, on page 4.

Service Parameters for Barge Privacy and Privacy On Hold

Cisco Unified Communications Manager provides five clusterwide service parameters: Built In Bridge Enable for the built-in conference bridge capability, Privacy Setting for the privacy feature, Enforce Privacy Setting on Held Calls setting for the privacy on hold feature, single button barge/cBarge policy for single button barge/cBarge features, and Party Entrance Tone for the tones that are played during barge. Set these parameters for each server in a cluster that has the Cisco CallManager service and barge is configured.

- Built In Bridge Enable-Default specifies Off. This parameter enables or disables the built-in conference bridge capability for phones that use the barge softkey. If Built in Bridge is set to On in Phone Configuration, the service parameter setting gets overridden.
- Privacy Setting-Default specifies True. This parameter enables or disables the privacy feature for phone users who do not want to display information on shared-line appearances. If only certain phones need the privacy feature, set the service parameter to False and set the Privacy field to On in Phone Configuration.

  If the Privacy field in the Phone Configuration window is set to default, the phone uses the setting that is configured in the Privacy Setting service parameter.
- Enforce Privacy Setting on Held Calls—Default specifies False. This parameter enables or disables the privacy on hold feature for phone users who want to preserve privacy on held calls.
- Single button barge/cBarge Policy-Default specifies Off. This parameter enables or disables the single button barge/cBarge feature for phone users who want to use the barge or cBarge feature by simply pressing the line button.
- Party Entrance Tone-Default specifies False. This parameter enables or disables the tones that play during barge.

CHAPTER 2

BLF Presence

This chapter provides information about the Busy Lamp Field (BLF) Presence feature which allows a user to monitor the real-time status of another user at a directory number or SIP URI.

Configure BLF Presence

The BLF Presence feature allows a user (watcher) to monitor the real-time status of another user at a directory number or SIP URI from the device of the watcher. A watcher can monitor the status of the user by using the following options:

- BLF/SpeedDial buttons
- Missed call, placed call, or received call lists in the directories window
- Shared directories, such as the corporate directory

Tip The following information assumes that the phones and SIP trunks exist in the Cisco Unified Communications Manager database. For information on how to add a phone or SIP trunk, see the Cisco Unified Communications Manager Administration Guide.

Perform the following steps to configure BLF presence features:

Note You do not need to configure BLF presence groups or the Default Inter-Presence Group Subscription parameter for BLF/SpeedDials.

Procedure

Step 1 If you have not already done so, configure the phones and SIP trunks that you plan to use with the BLF presence feature.

Step 2 Enable the BLF for Call Lists enterprise parameter.

Step 3 Configure the clusterwide service parameters for BLF presence in Cisco Unified Communications Manager Administration.

Step 4 To use BLF presence group authorization, configure BLF presence groups and permissions.

Step 5 Apply a BLF presence group to the directory number, SIP trunk, phone that is running SIP, phone that is running SCCP, end user, and application user (for application users that are sending BLF presence requests over the SIP trunk) in Cisco Unified Communications Manager Administration.

Step 6 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 7 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.

Apply the profile to the trunk. Reset the trunk for the changes to take effect.

If you checked Enable Application Level Authorization, check the Accept Presence Subscription check box in the Application User Configuration window for the application.

Step 8 Configure the SUBSCRIBE Calling Search Space and apply the calling search space to the phone, trunk, or end user, if required.

Step 9 Customize phone button templates for the BLF/SpeedDial buttons.

Step 10 If you have not already done so, configure the phone where you want to add the BLF/SpeedDial buttons; make sure that you choose the phone button template that you configured for the BLF/SpeedDial lines.

Step 11 Configure BLF/SpeedDial buttons for the phone or user device profile.

BLF Presence Feature

When you configure BLF Presence in Cisco Unified Communications Manager Administration, an interested party, known as a watcher, can monitor the real-time status of a directory number or SIP URI, a BLF presence entity, from the device of the watcher.

Note A SIP URI comprises a call destination configured with a user@host format, such as xten3@CompB.cisco.com or 2085017328@10.21.91.156:5060.

A watcher can monitor the status of the BLF presence entity (also called presentity) with the following options:

- BLF/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/SpeedDial buttons, the BLF presence entity displays as a speed dial on the device of the watcher.

Tip For BLF presence-supported phones that are running SIP, you can configure directory numbers or SIP URIs as BLF/SpeedDial buttons. For BLF presence-supported phones that are running SCCP, you can only configure directory numbers as BLF/SpeedDial buttons.

Tip You configure BLF/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 Cisco Unified Communications Manager.

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 display on the watcher device to indicate whether the BLF presence entity is on the phone, not on the phone, status 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/Speed Dial is configured, BLF presence group authorization does not apply to BLF/Speed Dials.

Note 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/Speed Dial that appears in a call list.

To allow BLF presence requests from outside the cluster, administrators must 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.

The SUBSCRIBE Calling Search Space determines how Cisco Unified Communications Manager routes BLF presence requests that come from the trunk or the phone. The SUBSCRIBE Calling Search Space that is associated with an end user gets used for extension mobility calls.

BLF Presence with Phones and Trunks

Tip Use the information in this section with the BLF Presence Groups, on page 22, the BLF Presence Authorization, on page 24, theBLF Presence with Route Lists, on page 21, and the SUBSCRIBE Calling Search Space, on page 26. The following information assumes that the phones and trunks have permission to view the status of the BLF presence entity, as configured through BLF presence groups.

Cisco Unified Communications Manager handles all 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 directly if the phone and BLF presence entity are colocated.

If the device exists outside of the cluster, Cisco 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.

For non-Cisco Unified Communications Manager watchers that send BLF presence requests through a Cisco Unified Communications Manager trunk, Cisco Unified Communications Manager responds with BLF presence status if Cisco Unified Communications Manager supports the BLF presence entity. If Cisco Unified Communications Manager does not support the BLF presence entity, the request gets rejected.

The following examples demonstrate how BLF presence works for phones and trunks when the phones and trunks have permission to send and receive presence requests.

A Cisco Unified Communications Manager User Queries the BLF Status of Another Cisco Unified Communications Manager User

A Cisco Unified Communications Manager user calls another Cisco Unified Communications Manager user only to find that the called party is not available. When available, the called party checks the missed call list, and the phone contacts Cisco Unified Communications Manager. Cisco Unified Communications Manager validates that the called party is a valid watcher and determines that the caller represents a Cisco Unified Communications Manager presence entity. The BLF status for the caller gets updated on the phone of the called party.

A Cisco Unified Communications Manager User Queries the BLF Status of a Non-Cisco Unified Communications Manager User

A non-Cisco Unified Communications Manager user calls a Cisco Unified Communications Manager user only to find that the Cisco Unified Communications Manager user is unavailable. When available, the Cisco Unified Communications Manager user checks the missed call list, and the phone contacts Cisco Unified Communications Manager. Cisco Unified Communications Manager confirms that the Cisco Unified Communications Manager user is a valid watcher and determines that the non-Cisco Unified Communications Manager user represents a presence entity. A SIP trunk interacts with the non-Cisco Unified Communications Manager network and Cisco Unified Communications Manager, and status for the non-Cisco Unified Communications Manager user gets updated on the phone of the Cisco Unified Communications Manager user.

A Non-Cisco Unified Communications Manager User Queries the BLF Presence Status of a Cisco Unified Communications Manager User

A non-Cisco Unified Communications Manager user queries the state of a Cisco Unified Communications Manager user. The request comes through a Cisco Unified Communications Manager SIP trunk. Cisco Unified Communications Manager verifies that the non-Cisco Unified Communications Manager user is a valid watcher and determines that the Cisco Unified Communications Manager user represents a Cisco Unified Communications Manager presence entity. Cisco Unified Communications Manager sends the status to phone of the non-Cisco Unified Communications Manager user.

A Cisco Unified Communications Manager Accesses the Corporate Directory to Get BLF Status

A Cisco Unified Communications Manager user accesses the corporate directory on the phone. For each directory entry, BLF status displays.

A Phone Monitors a BLF/SpeedDial

After an administrator configures the BLF presence feature and the BLF/SpeedDial buttons, a user can immediately begin to monitor the real-time status of a BLF presence entity.

BLF Presence with Route Lists

Tip Use the information in this section with the BLF Presence with Phones and Trunks, on page 20, the BLF Presence Groups, on page 22, the BLF Presence Authorization, on page 24, and the SUBSCRIBE Calling Search Space, on page 26.

Cisco Unified Communications Manager receives BLF presence requests from watchers and status responses from BLF presence entities. Watchers and BLF presence entities can exist inside the cluster or outside of the cluster.

Cisco Unified Communications Manager supports external incoming and outgoing BLF presence requests through the SIP trunk. SIP trunks can be members of route groups, which are members of route lists. When Cisco Unified Communications Manager receives a BLF presence request or notification status that is associated with an outbound SIP trunk or route group, Cisco forwards the request or status to a SIP trunk.

Note 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/H323 trunk devices.

When a request gets forwarded to a route group or list, any SIP trunk in the group or list can carry the request. Cisco Unified Communications Manager forwards the request to the next available or idle outbound SIP trunk in the group or list. This process repeats until Cisco Unified Communications Manager receives a successful response or the operation fails.

After the BLF presence request to an external presentity is successful, the SIP trunk receives notification messages based on status changes for the presentity and sends the status to the route list/group to notify the watcher. When different watchers send BLF presence requests to the same presentity that is reached through the route list/group and SIP trunk, Cisco Unified Communications Manager sends the cached status for the presentity to the subscriber instead of creating another subscription.

The presentity can terminate the subscription at any time due to time-out or other reasons. When the SIP trunk receives a termination status, the termination status gets passed to the route list or group to notify the watcher.

See the SUBSCRIBE Calling Search Space, on page 26 chapter in the Cisco Unified Communications Manager Administration Guide for more information about configuring route lists.

BLF Presence Groups

Tip The Default Inter-Presence Group Subscription service parameter for the Cisco CallManager service sets the clusterwide permissions parameter for BLF presence groups to Allow Subscription or Disallow Subscription. This enables administrators to set a system default and configure BLF presence group relationships by using the default setting for the cluster. For information on configuring this service parameter, see the Configure Presence Service Parameters and Enterprise Parameters, on page 28.

Cisco Unified Communications Manager allows you to configure 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.

Note The system always allows BLF presence requests within the same BLF presence group.

You must also specify the relationships to other BLF presence groups by using one of the following permissions from the drop-down list in the BLF Presence Group Configuration window:

- Use System Default - To use the Default Inter-Presence Group Subscription service parameter (Allow Subscription or Disallow Subscription) setting for the permission setting, select the group(s) and configure the Subscription Permission to Use System Default.
- Allow Subscription - To allow a watcher in this group to monitor members in another group, select the group(s) and configure the Subscription Permission setting to Allow Subscription.
- Disallow Subscription - To block a watcher in this group from monitoring members in another group, select the group(s) and configure the Subscription Permission setting to Disallow Subscription.

Tip Whenever you add a new BLF presence group, Cisco Unified Communications Manager defines all group relationships for the new group with the default cluster setting as the initial permission setting.To apply different permissions, you configure new permissions between the new group and existing groups for each permission that you want to change.

The permissions that are configured for a BLF presence group display in the BLF Presence Group Relationship pane. Permissions that use the system default permission setting for the group-to-group relationship do not display.

Example: Configuring BLF Presence Group Permissions

Assume the clusterwide setting for Default Inter-Presence Group Subscription is set to Disallow Subscription. You create two BLF presence groups: Group A (workers) and Group B (managers). If you want to allow Group B members to monitor Group A members but to block group A members from monitoring Group B members, you would configure Allow Subscription for Group B to Group A. (Because the system default is Disallow Subscription, Group A already disallows subscriptions to Group B, unless you change the Default Inter-Presence Group Subscription service setting.)

Cisco Unified Communications Manager automatically creates the Standard BLF Presence Group at installation, which serves as the default group for BLF presence users. All BLF presence users (except application user) initially get assigned to the Standard BLF Presence group. You cannot delete this group.

Note Because not all application users use the SIP trunk or initiate BLF presence requests, the default setting for application user specifies None. To assign an application user to the Standard BLF Presence Group, administrators must configure this option.

For each BLF presence group that you create, you apply the BLF presence group to one or more of following items in Cisco Unified Communications Manager Administration (see the following table).

Table 2: Applying BLF Presence Groups

Apply BLF Presence Groups to	Presence Entity or Watcher	Comments
Directory number	Presence entity	For phones that are running either SIP or SCCP
Trunk	Watcher and Presence Entity	For external BLF presence servers that send presence requests via SIP trunk or a proxy server that is connected on SIP trunk (serving as watcher) For outgoing BLF presence requests to the SIP trunk (serving as presence entity)
Phone	Watcher	For phones that are running either SIP or SCCP
Application User	Watcher	For external applications that send BLF presence requests via SIP trunk or home on a proxy server that is connected on SIP trunk (for example Web Dial, IPPM, Meeting Place, conference servers, and presence servers)
End User	Watcher	For user directories and call lists and to configure extension mobility settings.

Apply BLF Presence Groups to	Presence Entity or Watcher	Comments
Note 1: A phone serves as a watcher; a line on a phone cannot serve as a watcher. Note 2: You do not need to provision BLF presence groups for BLF/SpeedDials.		

Tip See the BLF Presence Authorization, on page 24, for additional requirements for BLF presence requests through the SIP trunk.

The following examples describe how a phone or trunk obtains the destination status by using different BLF presence groups and permissions.

A Phone Wants Status About a Directory Number That Is Assigned to BLF/SpeedDial

Phone A, which is colocated with Phone B, has directory number 1111 (Phone B) that is configured as a BLF/SpeedDial button to monitor BLF presence status for Phone B. Phone A receives real-time status for directory number 1111 and displays the status icon next to the BLF/SpeedDial button. The system does not invoke BLF presence group authorization.

A Phone Wants Status About a Directory Number in a Call List

Phone A, which has the BLF presence group, User Group, that is configured for it, has directory number 1111 in the Missed Calls call list. Directory number 1111, which exists for Phone B, has the BLF presence group, Executive Group, that is configured for it. The BLF Presence Group Configuration window indicates that the relationship between the User Group and Executive Group is Disallow Subscription, as specified in the BLF Presence Group Relationship pane. Phone A cannot receive real-time status for directory number 1111, and Phone A does not display the real-status icon next to the Missed Call list entry.

A SIP Proxy Server That Is Connected to a SIP Trunk Wants Status About a Cisco Unified Communications Manager Directory Number

The following example describes how a SIP trunk obtains the status of a directory number when different BLF presence groups are configured for the SIP trunk and directory number. SIP proxy server D uses SIP trunk C to contact Cisco Unified Communications Manager for the status of directory number 5555 because directory number 5555 exists as a BLF/SpeedDial button on phone E that is running SIP, which connects to the proxy server. The SIP trunk indicates that it has BLF presence group, Administrator Group, that is configured for it, and directory number 5555 is assigned to the Engineering Group. The BLF Presence Group Configuration window indicates that the relationship between the Administrator Group and Engineering Group is allowed, as specified in the BLF Presence Group Relationship pane. Cisco Unified Communications Manager sends the status of the directory number to the trunk, which passes the status to the SIP proxy server D. Phone E that is running SIP receives real-time status for directory number 5555, and the phone displays the real-time status icon next to the BLF/SpeedDial button.

BLF Presence Authorization

Tip Use the information in this section with the “BLF presence with phones and trunks”, “BLF presence groups”, and “SUBSCRIBE Calling Search Space” topics.

To view the status of a presence entity, watchers send presence requests to Cisco Unified Communications Manager. The system requires watchers to be authorized to initiate status requests for a presence entity by using these mechanisms:

- The watcher BLF presence group must possess authorization to obtain the status for the presence entity presence group, whether inside or outside of the cluster.
- Unified CM must possess authorization to accept BLF presence requests from an external presence server or application.

Note The authorization process remains independent of calling search space routing for BLF presence requests.

To initiate BLF presence group authorization, you must configure one or more BLF presence groups and assign the appropriate permissions. Administrators configure permission settings for BLF presence groups, which specify when a BLF presence group for a watcher can monitor the status of members in other groups. To validate a BLF presence request, Unified CM performs a database lookup by using the permissions that are assigned to the BLF presence groups that are configured.

If you choose not to use BLF presence group authorization, leave all presence users assigned to the default BLF presence group and do not configure additional groups or permissions. You will still need to configure authorization for a SIP trunk or application if you want to authorize Unified CM to accept incoming BLF presence requests from an external presence server or application.

Tip When an administrator decides to add or change a BLF/SpeedDial button, the administrator ensures that the watcher is authorized to monitor that destination.

Administrators configure the Unified CM system to accept BLF presence requests that come via the SIP trunk by configuring parameters for the SIP trunk and application user.

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 SIP trunk BLF presence requests are allowed, 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.

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.

To authorize the Unified CM system to accept BLF presence requests from an external application that connects on the SIP trunk, check the Enable Application Level Authorization check box in the SIP Trunk Security Profile Configuration window and the Accept BLF Presence Subscription check box in the Applications User Configuration window for the application. When you configure the Unified CM system to accept BLF presence requests from an application user, Unified CM validates each presence request that is received on the SIP trunk before accepting it.

Tip To use presence group authorization with incoming presence requests from a SIP trunk application, configure a presence group for the application, such as Presence_User, 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 application authorization can occur, Unified CM must first authenticate the external application by using digest authentication. Enable Application Level Authorization cannot be checked unless Enable Digest Authentication is checked.

Note The authorization could pass for the trunk but fail for the application. See the “BLF Presence group and Presence authorization tips” topic for additional considerations when configuring presence authorization.

See the *Cisco Unified Communications Manager Security Guide* for more information about authentication and authorization.

Related Topics

BLF Presence with Phones and Trunks, on page 20
BLF Presence Groups, on page 22
SUBSCRIBE Calling Search Space, on page 26
BLF Presence Group and Presence Authorization Tips, on page 34

SUBSCRIBE Calling Search Space

The SUBSCRIBE Calling Search Space determines how Cisco Unified Communications Manager routes BLF presence requests that come from the trunk or the phone. The SUBSCRIBE calling search space, which is associated with a watcher, specifies the list of partitions to search for routing information to a presence entity for BLF presence requests.

To configure a calling search space specifically for this purpose, you configure a calling search space as you do all calling search spaces (**Call Routing** > **Class of Control** > **Calling Search Space**). For information on how to configure a calling search space, see the *Cisco Unified Communications Manager Administration Guide*.

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. If you do not select a different calling search space for presence requests, the SUBSCRIBE Calling Search Space defaults to None.

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 gets used for extension mobility calls.

BLF Presence with Extension Mobility

Tip Use the information in this section in conjunction with the BLF Presence Groups, on page 22, the BLF Presence Authorization, on page 24, and the SUBSCRIBE Calling Search Space, on page 26.

When you configure BLF/SpeedDial buttons in a user device profile in Cisco Unified Communications Manager Administration, a phone that supports Cisco Extension Mobility can display BLF presence status on the BLF/SpeedDial buttons after you log in to the device. The SUBSCRIBE calling search space and presence group that are configured for the user apply.

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 log-out profile that is configured. When a user device profile is configured for the logout profile, the SUBSCRIBE calling search space and BLF presence group that are configured for the user apply.

Tip See the *Cisco Unified Communications Manager Administration Guide* for more information about configuring device profiles.

System Requirements

The following system requirements exist for the Busy Lamp Field (BLF) Presence feature in Cisco Unified Communications Manager:

- Cisco Unified Communications Manager 8.0(2) (or higher) on each server in the cluster
- To identify the Cisco Unified IP Phone models that support BLF Presence, generate the Unified CM Phone Features List report in Cisco Unified Reporting. To generate the report, choose BLF Speed Dial, BLF Speed Dial with URI, or BLF Presence Subscription.

Interactions and Restrictions

The following interactions and restrictions apply to the BLF presence feature:

- Cisco Unified Communications Manager Assistant does not support SIP presence.
- Cisco Unified Communications Manager supports an inbound BLF presence request to a directory number that is associated with a hunt list.
- Cisco Unified Communications Manager rejects BLF presence requests to a directory number that is associated with a hunt pilot.
- The BLF on call list feature is not supported on the Cisco Unified IP Phone 7940 and Cisco Unified IP Phone 7960.

- Because the administrator ensures that the watcher is authorized to monitor the destination when configuring a BLF/SpeedDial, BLF presence group authorization does not apply to BLF/SpeedDials. 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/Speed Dial that appears in a call list.
- 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/SpeedDial buttons on Cisco Unified IP Phones with multiple lines, the phone uses the first available line as the subscriber.
- 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 presentity 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 presentity.
- You can configure BLF in the BAT phone template.

The following restrictions apply to Presence BLF interaction with DNs on H.323 phones when the H.323 phone device serves as presentity:

- When the H.323 phone is in the RING IN state, the BLF status gets reported as Busy. (For phone presentities of phones that are running either SCCP or SIP and that are in the RING IN state, the BLF status gets reported as Idle.)
- 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 presentities 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.)

Presence Configuration

This section contains information to configure Presence.

Tip Before you configure Presence, review the configuration summary task for this feature.

Related Topics

Configure BLF Presence, on page 17

Configure Presence Service Parameters and Enterprise Parameters

To configure presence enterprise parameters, for example, the BLF for Call List parameter, in Cisco Unified Communications Manager Administration, choose **System** > **Enterprise Parameters**. For information on the parameter, click the question mark that displays in the Enterprise Parameter Configuration window or click the link for the parameter name.

To configure presence service parameters, for example, the Default Inter-Presence Group Subscription parameter, perform the following procedure:

Tip The Default Inter-Presence Group Subscription parameter does not apply to BLF/SpeedDials.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **System** > **Service Parameters**.

Step 2 From the Server drop-down list box, choose the server where you want to configure the parameter.

Step 3 From the Service drop-down list box, choose the Cisco CallManager (Active) service.

If the service does not display as active, ensure that the service is activated in Cisco Unified Serviceability.

Step 4 Locate the clusterwide service parameters for the Presence feature.

Tip For information on the parameters, click the parameter name or click the question mark that displays in the Service Parameter Configuration window.

Step 5 Update the parameter values.

Step 6 Click **Save.**

Configure and Apply the SUBSCRIBE Calling Search Space

All calling search spaces that you configure in Cisco Unified Communications Manager Administration display in the SUBSCRIBE Calling Search Space drop-down list box in the Trunk Configuration or Phone Configuration window.

The SUBSCRIBE Calling Search Space determines how Cisco Unified Communications Manager routes presence requests that come from the trunk or the phone. If you do not select a different calling search space for presence requests, the SUBSCRIBE Calling Search Space defaults to None.

To configure a calling search space specifically for this purpose, you configure a calling search space as you do all calling search spaces (**Call Routing** > **Class of Control** > **Calling Search Space**). For information on how to configure a calling search space, see the *Cisco Unified Communications Manager Administration Guide*.

To apply a SUBSCRIBE Calling Search Space to the SIP trunk, phone, or end user, perform the following procedure:

Procedure

Step 1 Perform one of the following tasks:

a) Find a phone, as described in the *Cisco Unified Communications Manager Administration Guide*.
b) Find a SIP trunk, as described in the *Cisco Unified Communications Manager Administration Guide*.
c) Find an end user, as described in the *Cisco Unified Communications Manager Administration Guide*.

Step 2 After the configuration window displays, choose the calling search space from the SUBSCRIBE Calling Search Space drop-down list box.

Step 3 Click **Save.**

Step 4 Click **Reset.**

Find BLF Presence Groups

The Find and List window for presence groups allows you to search for BLF presence groups, which are used with the BLF presence feature for authorization. To find a BLF presence group, perform the following procedure:

Procedure

Step 1 Choose **System** > **BLF Presence Group**.

The Find and List BLF Presence Groups window appears. Records from an active (prior) query may also display in the window.

Step 2 To filter or search records

a) From the first drop-down list box, choose a search parameter.
b) From the second drop-down list box, choose a search pattern.
c) Specify the appropriate search text, if applicable.

Note To add additional search criteria, click the **+** button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the **–** button to remove the last added criterion or click the **Clear Filter** button to remove all added search criteria.

Step 3 To find all records in the database, ensure the dialog box is empty, click **Find**.

All matching records appear. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

Note You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking **Delete Selected**. You can delete all configurable records for this selection by clicking **Select All** and then clicking **Delete Selected**.

Step 4 From the list of records that appear, click the link for the record that you want to view.

Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Configure BLF Presence Groups

To add, update, or copy BLF presence groups, perform the following procedure:

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **System** > **BLF Presence Group**.

Step 2 Perform one of the following tasks:

a) To add a new BLF presence group, click the **Add New** button.

b) To copy an existing BLF presence group, locate the appropriate group as described in “Find BLF Presence groups”, click the **Copy** button or **Copy** icon next to the presence group that you want to copy.

c) To update an existing presence group, locate the appropriate group as described in “Find BLF Presence groups”.

d) To rename a presence group, locate the group as described in “Find BLF Presence groups”, click the Name link for group on the list, enter the new name when the window displays.

Step 3 Enter the appropriate settings as described in “BLF Presence group configuration”.

Step 4 Click **Save**.

What to do next

After you configure the BLF presence groups, apply the BLF presence group configuration to the phone that is running either SIP or SCCP, SIP trunk, directory number, application user (for application users sending presence requests over the SIP trunk), or end user in Cisco Unified Communications Manager Administration. See the “Apply a BLF Presence group” topic.

Related Topics

Find BLF Presence Groups, on page 30
BLF Presence Group Configuration, on page 31
Apply a BLF Presence Group, on page 33

BLF Presence Group Configuration

Presence authorization works with BLF presence groups. The following table describes the BLF presence group configuration settings. Before you configure these settings, review the “BLF Presence and Presence authorization tips” topic.

Table 3: BLF Presence Group Configuration Settings

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 settings for the named group to the selected group(s).

Field	Description
Subscription Permission	For the selected BLF presence groups, choose one of the following options from the drop-down list box: • Use System Default - Set the permissions setting to the Default Inter-Presence Group Subscription clusterwide service parameter setting (Allow Subscription or Disallow Subscription). • Allow Subscription - Allow members in the named group to view the real-time status of members in the selected group(s). • Disallow Subscription - Block members in the named group from viewing the real-time status of members in the selected group(s). The permissions that you configure display in the BLF Presence Group relationship pane when you click Save. All groups that use system default permission setting do not display.

Related Topics

BLF Presence Group and Presence Authorization Tips, on page 34

Delete a BLF Presence Group

This section describes how to delete a BLF presence group from the Cisco Unified Communications Manager database.

Before you begin

Before you can delete a BLF presence group from Cisco Unified Communications Manager Administration, you must apply another group to the devices/user or delete all devices/users that use the BLF presence group.

To find out which devices/users use the BLF presence group, click the Name link for the BLF presence group in the Find and List window; then, choose Dependency Records from the Related Links drop-down list box when the BLF Presence Group Configuration window appears; click **Go.**

If the dependency records feature is not enabled for the system, enable dependency records in the **System** > **Enterprise Parameters** window. For more information about dependency records, see the *Cisco Unified Communications Manager System Guide*.

Procedure

Step 1 Find the BLF presence group by using the procedure in the Find BLF Presence Groups, on page 30.

Step 2 To delete multiple BLF presence groups, check the check boxes next to the appropriate BLF presence group in the Find and List window; then, click the **Delete Selected** icon or the **Delete Selected** button.

Step 3 To delete a single BLF presence group, perform one of the following tasks:

a) In the Find and List window, check the check box next to the appropriate BLF presence group; then, click the **Delete Selected** icon or the **Delete Selected** button.

b) In the Find and List window, click the Name link for the BLF presence group. After the specific BLF Presence Group Configuration window appears, click the **Delete** icon or the **Delete** button.

Step 4 When prompted to confirm the delete operation, click **OK** to delete or **Cancel** to cancel the delete operation.

Apply a BLF Presence Group

For information on configuring BLF presence groups in Cisco Unified Communications Manager Administration, see the "BLF presence groups" topic. For information about configuring permission settings for presence authorization, see the "BLF presence authorization" topic. The system always allows presence requests between members in the same BLF presence group.

To apply a BLF presence group to the 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, perform the following procedure:

Procedure

Step 1 Perform one of the following tasks:

a) Find a SIP trunk, as described in the *Cisco Unified Communications Manager Administration Guide*.
b) Find an application user, as described in the *Cisco Unified Communications Manager Administration Guide*.
c) Find an end user, as described in the *Cisco Unified Communications Manager Administration Guide*.
d) Find a phone that is running either SCCP or SIP, as described in the *Cisco Unified Communications Manager Administration Guide*.

Tip After the Phone Configuration window appears, you can access the Directory Number Configuration window by clicking the Line link in the Association Information pane. In the Directory Number Configuration window, you specify the BLF presence group for the directory number.

Tip When an administrator decides to add or change a BLF/SpeedDial button, the administrator ensures that the watcher is authorized to monitor that destination.

Step 2 After the configuration page appear, choose the group from the BLF Presence Group drop-down list box. See the "BLF Presence group and Presence authorization tips" topic for provisioning tips.

Step 3 Click **Save**.

Step 4 For devices, you must click **Reset**.

Step 5 Repeat the procedure for all items that are listed.

Related Topics

BLF Presence Groups, on page 22
BLF Presence Authorization, on page 24
BLF Presence Group and Presence Authorization Tips, on page 34

BLF Presence Group and Presence Authorization Tips

Presence authorization works with BLF presence groups. This section lists tips to use when you set up BLF presence groups for presence authorization.

- To allow a watcher to monitor a destination, make sure that the BLF presence group that is applied to the watcher that is originating the request, including application users, has permission to monitor the group that is applied to the BLF presence entity. End users for supported applications, for example, Cisco Unified Communications Manager Assistant end users, also serve as watchers because the user requests status about a BLF presence entity that is configured on the application.
- To allow Cisco Unified Communications Manager to receive and route BLF presence requests from the SIP trunk application, make sure that the Accept Presence Subscription check box is checked in the Application User Configuration window to authorize incoming SUBSCRIBE requests. If no BLF presence group is applied to the application user, Unified CM uses the BLF presence group that is applied to the trunk.
- If you check the Accept Presence Subscription check box for an application user, but do not check the Accept Presence Subscription check box (in the SIP Trunk Security Profile Configuration window) that is applied to the trunk, a 403 error message gets sent to the SIP user agent that is connected to the trunk.
- If you check the Accept Presence Subscription check box for an application user, but do not check the Enable Application Level Authorization check box (in the SIP Trunk Security Profile Configuration window) that is applied to the trunk, a 403 error message gets sent to the SIP user agent that is connected to the 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 will accept all incoming requests before performing group authorization.
- If the SIP trunk uses digest authentication, as configured in the SIP Trunk Security Profile Configuration window, incoming BLF presence requests require authentication of the credentials from the sending device. 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.
- After authorization and authentication is successful for a SIP trunk application, Unified CM performs group authorization to verify the group permissions that are associated with the SUBSCRIBE request before accepting the request.
- When an administrator decides to add or change a BLF/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.
- When configuring a SIP URI as BLF/SpeedDial button, make sure the routing patterns are appropriately configured. See the *Cisco Unified Communications Manager Administration Guide* for more information.

Configure a Customized Phone Button Template for BLF/SpeedDial Buttons

Administrators can configure BLF/SpeedDial buttons for a phone, or user device profile. The Add a new BLF SD link does not display in the Association Information pane unless you configure a customized phone button template for BLF/SpeedDial buttons and apply the template to the 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 displays in the Association Information pane.

Tip If the template does not support BLF/SpeedDials, the Add a new BLF SD link displays in the Unassigned Associated Items pane.

To configure a customized phone button template for BLF/SpeedDial buttons, perform the following procedure:

Procedure

Step 1 Find the phone button template for the device, as described in the *Cisco Unified Communications Manager Administration Guide*.

Step 2 After the Find/List window displays, click the **Copy** button or **Copy** icon for the phone button template.

Step 3 In the Button Template Name field, enter a new name for the template; for example, BLF SIP 7970.

Step 4 Click **Save.**

Step 5 After the Phone Button Template Configuration window displays, choose Speed Dial BLF from the Feature drop-down list box(es); that is, if you want the line to be configured as a BLF/SpeedDial button.

Step 6 Click **Save.**

Step 7 If you are updating an existing customized phone button template that you already applied to phones, click **Reset.**

Configure BLF/SpeedDial Buttons

To configure BLF/SpeedDial buttons, perform the following procedure:

Procedure

Step 1 To configure the BLF/SpeedDial button in the Phone Configuration window, find a phone, as described in the *Cisco Unified Communications Manager Administration Guide*.

Step 2 To configure the BLF/SpeedDial button for user device profiles, find the user device profile as described in the*Cisco Unified Communications Manager Administration Guide*.

Step 3 After the configuration window displays, click the **Add a New BLF SD** link in the Association Information pane.

Tip 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/SpeedDials. The link displays in the Unassigned Associated Items pane if the phone button template does not support BLF/SpeedDials.

Step 4 Configure the settings, as described in BLF/SpeedDial Configuration, on page 36. Administrators must ensure that the watcher is authorized to monitor a destination that is configured as a BLF/SpeedDial button.

Step 5 After you complete the configuration, click **Save** and close the window.

The destination(s) and/or directory number(s) display in the pane.

BLF/SpeedDial Configuration

With the presence feature, a watcher can monitor the status of the presence entity (also called presentity). When you configure BLF/SpeedDial buttons, the presence entity displays as a speed dial on the device of the watcher.

The following table describes the settings that you configure for BLF/SpeedDial buttons.

Table 4: BLF/SpeedDial Button Configuration Settings

Field	Description
Destination	Perform one of the following tasks to configure a SIP URI or a directory number as a BLF/SpeedDial button: • Only for phones that are running SIP, enter the SIP URI. For phones that are running SCCP, you cannot configure SIP URI as BLF/SpeedDial buttons. • For phones that are running either SCCP or SIP, enter a directory number in this field or go to the Directory Number drop-down list box. If you want to configure non-Unified Communications Manager directory numbers as BLF/SpeedDial buttons, enter the directory number in this field. For this field, enter only numerals, asterisks (*), and pound signs (#). If you configure the Destination field, do not choose an option from the Directory Number drop-down list box. If you choose an option from the Directory Number drop-down list box after you configure the Destination, Unified Communications Manager deletes the Destination configuration.
Directory Number	The Directory Number drop-down list box displays a list of directory numbers that exist in the Unified Communications Manager database. Configure this setting only if you did not configure the Destination field. For phones that are running either SCCP or SIP, choose the number (and corresponding partition, if it displays) that you want the system to dial when the user presses the speed-dial button; for example, 6002-Partition 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/SpeedDial button. This field supports internationalization. If your phone does not support internationalization, the system uses the text that displays in the Label ASCII field.

Field	Description
Label ASCII	Enter the text that you want to display for the speed-dial 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. **Tip** 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.

CHAPTER 3

Call Back

This chapter provides information about the Call Back feature.

Configure Call Back

The Call Back feature allows you to receive call-back notification on your Cisco Unified IP Phone when a called party line becomes available. You can activate call back for a destination phone that is within the same Cisco Unified Communications Manager cluster as your phone or on a remote PINX over QSIG trunks or QSIG-enabled intercluster trunks.

To receive call-back notification, a user presses the CallBack softkey or feature button while receiving a busy or ringback tone. A user can also activate call back during reorder tone, which is triggered when the no answer timer expires.

Perform the following steps to configure the Call Back feature.

Procedure

Step 1 If phone users want the softkeys and 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 installed the locale installer.

For more information, see the *Cisco Unified Communications Operating System Administration Guide*

Step 2 In Cisco Unified Communications Manager Administration, create a copy of the Standard User softkey template and add the CallBack softkey to the following states:

- On Hook call state
- Ring Out call state
- Connected Transfer call state

If the phone supports Call Back as a feature button, create a copy of the applicable phone button template and add the CallBack feature button.

Step 3 In Cisco Unified Communications Manager Administration, add the new softkey template to the Common Device Configuration.

Step 4 In the Phone Configuration window, perform one of the following tasks:

a) Choose the common device configuration that contains the new softkey or phone button template.
b) Choose the new softkey template from the Softkey Template drop-down list box, or choose the new phone button template from the Phone Button Template drop-down list box.

Step 5 In the Phone Configuration window, verify that the correct user locale is configured for the Cisco Unified IP Phone(s).

For more information, see topics related to changing an end user password, as well as configuring Speed-Dial Buttons and abbreviated dialing in the *Cisco Unified Communications Manager Administration Guide*. Also see the *Cisco Unified Communications Operating System Administration Guide*

Step 6 If you do not want to use the default settings, configure the Call Back service parameters.

Step 7 Verify that the Cisco CallManager service is activated in Cisco Unified Serviceability.

For more information, see the *Cisco Unified Serviceability Administration Guide*

Related Topics

Add Softkey Template, on page 48
Call Back, on page 39
Call Back Feature, on page 40
Configure Softkey Template, on page 48
Create a Softkey Template, on page 47
Set Call Back Service Parameters, on page 50

Call Back Feature

The Call Back feature allows you to receive call-back notification on your Cisco Unified IP Phone when a called party line becomes available. You can activate call back for a destination phone that is within the same Cisco Unified Communications Manager cluster as your phone or on a remote PINX over QSIG trunks or QSIG-enabled intercluster trunks.

To receive call-back notification, a user presses the CallBack softkey or feature button while receiving a busy or ringback tone. A user can also activate call back during reorder tone, which is triggered when the no answer timer expires.

The following sections provide information about the Call Back feature:

- Call Back Examples, on page 41
- System Requirements for Call Back, on page 44
- Interactions and Restrictions, on page 44

- Install and Activate Call Back, on page 46

Call Back Examples

The following examples describe how Call Back works after an unavailable phone becomes available.

Note The calling phone only supports one active call back request. The called phone can support multiple call back requests.

Call Back only supports spaces and digits 0 through 9 for the name or number of the calling or called party. To work with Call Back, the name or number of the calling or called party cannot contain # or * (pound sign or asterisk).

Note If the originating side (User A) gets reset after Call Back has been activated, then Call Back gets automatically cancelled. User A does not receive an audio alert, and the Callback notification screen does not display. If the terminating side (User B) gets reset, Call Back does not get cancelled. User A will receive an audio alert, and the Callback notification screen displays after User B becomes available.

Example: User A Calls User B, Who Is Not Available

User A calls User B, who exists either in the same Cisco Unified Communications Manager cluster as User A or in a different cluster.

Because User B is busy or does not reply, User A activates the Call Back feature by using the CallBack softkey. The following call back activation message displays on the phone of User A:

```
CallBack is activated on <DN of User B>Press Cancel to deactivate
Press Exit to quit this screen
```

User A presses the Exit softkey.

After User B becomes available (phone becomes on hook after busy or completes an off-hook and on-hook cycle from idle), User A receives an audio alert, and the following message displays on the phone of User A:

```
<DN of User B> has become availableTime HH:MM MM/DD/YYYY
Press Dial to call
Press Cancel to deactivate
Press Exit to quit this screen
```

User A presses the Exit softkey and then goes off hook and dials the DN of User B. User B answers the call. Users A and B go on hook.

When User A presses the CallBack softkey, the following message displays on the phone of User A:

```
<DN of User B> has become availableTime HH:MM MM/DD/YYYY
Press Dial to call
Press Cancel to deactivate
Press Exit to quit this screen
```

Note Manually dialing a DN that has been activated with Call Back notification does not affect the Call Back status.

Example: User A Activates the Call Back Feature for User B but Is Busy When User B Becomes Available

User A calls User B. User B does not answer. User A activates the Call Back feature by using the CallBack softkey. The following call back activation message displays on the phone of User A:

```
CallBack is activated on <DN of User B>Press Cancel to deactivate
Press Exit to quit this screen
```

User A presses the Exit softkey.

User C then calls User A, and users A and C go on hook in an active call. User B becomes available (phone becomes on hook after busy or completes an off-hook and on-hook cycle from idle) while User A is still on an active call. User A receives an audio alert, and the following message displays on the phone of User A:

```
<DN of User B> has become availableTime HH:MM MM/DD/YYYY
Press Dial to call
Press Cancel to deactivate
Press Exit to quit this screen
```

User A can interrupt the active call to contact User B in either of two ways:

- Select Dial from the notification screen. The active call automatically gets put on hold while User A calls User B.
- Press the Exit softkey to exit the notification screen and then park (or otherwise handle) the active call. After the active call is handled, User A can press the CallBack softkey and select Dial to call User B).

Example: User A Calls User B, Who Configured Call Forward No Answer (CFNA) to User C Before Call-Back Activation Occurs

The following scenario applies to Call Forward No Answer.

The call from User A gets forwarded to User C because Call Forward No Answer is configured for User B. User A uses call back to contact User C if User C is not busy; if User C is busy, User A contacts User B.

When User B or User C becomes available (on hook), User A receives an audio alert, and a message displays on User A phone that states that the user is available.

Example: User A Calls User B, Who Configures Call Forwarding to User C After User A Activates Call Back

The following scenarios support Call Forward All, Call Forward Busy, and Call Forward No Answer.

- User A calls User B, who exists in the same Cisco Unified Communications Manager cluster as User A. User A activates call back because User B is not available. Before User B becomes available to User A, User B sets up call forwarding to User C. User A may call back User B or User C, depending on the call-forwarding settings for User B.
- User A calls User B, who exists in a different cluster. The call connects by using a QSIG trunk. User A activates call back because User B is not available. Before User B becomes available to User A, User B sets up call-forwarding to User C. One of the following events occurs:

- If the Callback Recall Timer (T3) has not expired, User A always calls back User B.
- After the Callback Recall Timer (T3) expires, User A may call back User B or User C, depending on the call-forwarding settings of User B.

Tip The timer starts when the system notifies User A that User B is available. If User A does not complete the call back call during the allotted time, the system cancels call back. On the phone of User A, a message states that User B is available, even after the call back cancellation. User A can dial User B.

Example: User A and User C Call User B at the Same Time

User A and User C call User B at the same time, and User A and User C activate call back because User B is unavailable. A call-back activation message displays on the phones of User A and User C.

When User B becomes available, both User A and User C receive an audio alert, and a message displays on both phones that states that User B is available. The User, that is, User A or User C, that presses the Dial softkey first connects to User B.

Suspend/Resume Feature

Call Back provides the ability of the system to suspend the call completion service if the user, who originated Call Back, is currently busy and receives call-back notification when the called party becomes available. When the originating user then becomes available, the call completion service resumes for that user.

After the originating user (User A) activates the Call Back feature, and then becomes busy when the called party (User B) becomes available, the originating PINX sends out a Suspend Callback APDU message that indicates to the peer to suspend monitoring of User B until User A becomes available again. When User A becomes available, the originating PINX sends the Resume APDU message for the terminating side to start monitoring User B again.

Note Call Back supports the originating Suspend/Resume call-back notification for both intracluster and intercluster QSIG trunks or QSIG-enabled intercluster trunks.

The following example describes how the Suspend/Resume feature works:

Example: User A Is Busy When User B Becomes Available

User A calls User B, who exists either in the same Cisco Unified Communications Manager cluster as User A or in a different cluster. Because User B is busy or does not reply, User A activates the Call Back feature by using the CallBack softkey. The following call back activation message displays on the phone of User A:

```
CallBack is activated on <DN of User B>Press Cancel to deactivate
Press Exit to quit this screen
```

User A presses the Exit softkey.

User A has a busy trigger set to 1.

User A becomes busy. User B then becomes available.

User A does not receive an audio alert and does not receive a call-back notification screen on the display.

The originating side (User A) sends a Suspend Callback APDU message to the terminating side (User B).

User A becomes available. The originating side sends a Resume Callback APDU message to the terminating side. This causes monitoring of User B to resume.

When User B becomes available, User A receives an audio alert, and a Callback notification screen displays.

System Requirements for Call Back

Call Back requires the following software components:

- Cisco Unified Communications Manager 5.0 or later
- Cisco CallManager service that is running on at least one server in the cluster
- Cisco Database Layer Monitor service that is running on the same server as the Cisco CallManager service
- Cisco RIS Data Collector service that is running on the same server as the Cisco CallManager service
- Cisco Unified Communications Manager Locale Installer, that is, if you want to use non-English phone locales or country-specific tones
- Microsoft Internet Explorer 7 or Microsoft Internet Explorer 8 or Firefox 3.x or Safari 4.x

Interactions and Restrictions

Note If users want the CallBack softkeys, feature buttons, and messages on the phone to display in any language other than English, or if you want the user to receive country-specific tones for calls, install the locale installer, as described in the *Cisco Unified Communications Operating System Administration Guide*.

Table 5: Cisco Unified IP Phone That Use Call Back Softkeys and Buttons

Cisco Unified IP Phone Model	CallBack Softkey	Call Back Button
Cisco Unified IP Phone 6900 Series (except 6901 and 6911)	X	X
Cisco Unified IP Phone 7900 Series	X	
Cisco Unified IP Phone 8900 Series	X	X
Cisco Unified IP Phone 9900 Series	X	X
Cisco IP Communicator	X	

You can use the Call Back feature with some Cisco-provided applications, such as Cisco Unified Communications Manager Assistant.

You can call the following devices and can have call back activated on them:

- Cisco Unified IP Phones 6900, 7900, 8900, and 9900 Series (except 6901 and 6911)
- Cisco VGC Phone (uses the Cisco VG248 Gateway)
- Cisco Analog Telephone Adapter (ATA) 186 and 188
- Cisco Unified Communications Manager Release 8.0 and earlier supported Call Back only on busy subscriber for Cisco VG224 endpoints. Cisco Unified Communications Manager Release 8.5 and later supports Call Back on no answer for Cisco VG224 endpoints.
- CTI route point forwarding calls to preceding phones

Tip When a Cisco Extension Mobility user logs in or logs out, any active call completion that is associated with call back automatically gets canceled. If a called phone is removed from the system after call back is activated on the phone, the caller receives reorder tone after pressing the Dial softkey. The user may cancel or reactivate call back.

Tip If you forward all calls to voice-messaging system, you cannot activate call back.

Note Call Back is not supported over SIP trunks; however, Call Back is supported over QSIG-enabled SIP trunks.

To find more information about Cisco Unified IP Phones and the Call Back feature, see the user documentation for your phone model.

Call Back Notification with Phones Running SIP

The way that call back notification works on the Cisco Unified IP Phones 7960 and 7940 that are running SIP differs from the phones that are running SCCP. The Cisco Unified IP Phones 7960 and 7940 that run SIP do not support call-back notification for on-hook/off-hook states. The only way that Cisco Unified Communications Manager would know when a line on a SIP 7960 or 7940 phone becomes available is by monitoring an incoming SIP INVITE message that Cisco Unified Communications Manager receives from the phone. After the phone sends SIP INVITE to Cisco Unified Communications Manager and the phone goes on hook, Cisco Unified Communications Manager can send an audio and call back notification screen to the Cisco Unified IP Phone 7960 and 7940 (SIP) user.

Interactions with Call Forward IDivert and Voice-Messaging Features

The following call states describe the expected behaviors, for the calling party, that occur when Unified Communications Manager Call Back interacts with the Call Forward, iDivert, and voice-messaging system features.

Note The Cisco Unified IP Phones 6900, 8900, and 9900 use the Divert feature and softkey, which behaves the same as Immediate Divert (iDivert).

Note The iDivert feature does not work if it has been initiated via CTI and the redirect signal must traverse a QSIG link.

When a called party (Phone B) either forwards an incoming call by using Forward All, Forward Busy, or Forward No Answer; or diverts a call by using iDivert; to a voice-messaging system, the calling party (Phone A) can enter one of the following states with respect to the call back feature:

- VM-Connected state: The call gets connected to voice-messaging system. The CallBack softkey remains inactive on the calling party (Phone A) phone.
- Ring-Out state with the original called party: The voice-mail profile of the called party does not have a voice-mail pilot. The called party (Phone B) will see “Key Is Not Active” after pressing the iDivert softkey. The calling party (Phone A) should be able to activate call back against the original called party (Phone B).
- Ring-Out state with voice-messaging system feature and voice-mail pilot number as the new called party: The call encounters either voice-messaging system failure or network failure. The called party (Phone B) will see “Temp Failure” after pressing iDivert softkey. The calling party (Phone A) cannot activate call back against the original called party (Phone B) because the call context has the voice mail pilot number as the “new” called party.
- Ring-Out state with busy voice-mail port and voice-mail pilot number as the new called party: The call encounters busy voice-mail port. The called party (Phone B) will see “Busy” after pressing iDivert softkey. The calling party (Phone A) cannot activate call back against the original called party (Phone B) because the call context has the voice mail pilot number as the “new” called party.

For more information, see the following sections:

- See topics related to phone features in the isco Unified Communications Manager System Guide.
- Immediate Divert, on page 663

Call Back with Call Forward All Over QSIG ICT and Nortel ECMA PBX

Call Back does not interoperate with Call Forward All when there is a transit node and a Nortel Meridian Option 11C Release 4.0 PBX configured in ECMA mode in the call flow.

Install and Activate Call Back

Call Back automatically installs when you install Cisco Unified Communications Manager. After you install Cisco Unified Communications Manager, you must configure Call Back in Cisco Unified Communications Manager Administration, so phone users can use the Call Back feature.

The Call Back feature relies on the Cisco CallManager services, so make sure that you activate the Cisco CallManager service in Cisco Unified Serviceability.

Call Back Softkey Configuration

This section provides detailed configuration information for Call Back. You can create and configure Softkey templates, add a Softkey template to the phone user, and set Call Back service parameters.

Tip Before you configure the Call Back feature, review the configuration summary task for this feature.

Related Topics

Configure Call Back, on page 39

Create a Softkey Template

Perform the following procedure to create a new softkey template with the CallBack softkey.

Procedure

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

The Softkey Template Configuration window displays.

Step 2 From the Find and List Softkey Template window, choose the Standard User softkey template.

Step 3 Click the **Copy** icon.

The Softkey Template Configuration window displays with new information.

Step 4 In the Softkey Template Name field, enter a new name for the template; for example, Standard User for Call Back.

Step 5 Click the **Save** button.

The Softkey Template Configuration redisplays with new information.

Step 6 To add the CallBack softkey to the template, choose **Configure Softkey Layout** from the Related Links drop-down list box in the upper, right corner and click **Go.**

The Softkey Layout Configuration window displays. You must add the CallBack softkey to the On Hook, Ring Out, and Connected Transfer call states.

Step 7 To add the CallBack softkey to the On Hook call state, choose On Hook from the Select a Call State to Configure drop-down list box.

The Softkey Layout Configuration window redisplays with the Unselected Softkeys and Selected Softkeys lists.

Step 8 From the Unselected Softkeys list, choose the CallBack softkey and click the right arrow to move the softkey to the Selected Softkeys list.

Step 9 To save and continue, click the Save button.

Step 10 To add the CallBack softkey to the Ring Out call state, choose Ring Out from the Select a Call State to Configure drop-down list box.

The Softkey Layout Configuration window redisplays with the Unselected Softkeys and Selected Softkeys lists.

Step 11 From the Unselected Softkeys list, choose the CallBack softkey and click the right arrow to move the softkey to the Selected Softkeys list.

Step 12 To save and continue, click the **Save** button.

Step 13 To add the CallBack softkey to the Connected Transfer call state, choose Connected Transfer from the Select a Call State to Configure drop-down list box.

Step 14 The Softkey Layout Configuration window redisplays with the Unselected Softkeys and Selected Softkeys lists.

Step 15 From the Unselected Softkeys list, choose the CallBack softkey and click the right arrow to move the softkey to the Selected Softkeys list.

Step 16 Click the **Save** button.

Configure Softkey Template

Perform the following procedure to add the CallBack softkey template to the common device configuration. You create customized common device configurations for Call Back feature users.

Procedure

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

The Find and List Common Device Configuration window displays.

Step 2 Choose any previously created common device configuration that is in the Common Device Configuration list.

Step 3 In the Softkey Template field, choose the softkey template that contains the CallBack softkey from the drop-down list box. (If you have not created this template, see the Create a Softkey Template, on page 47.)

Step 4 Click the **Save** button.

Add Softkey Template

Perform the following procedure to add the CallBack softkey template to each user phone.

Procedure

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

The Find and List Phones window displays.

Step 2 Find the phone to which you want to add the softkey template. See topics related to Cisco Unified IP Phone configuration in the *Cisco Unified Communications Manager Administration Guide*.

Step 3 Perform one of the following tasks:

a) From the Common Device Configuration drop-down list box, choose the common device configuration that contains the new softkey template.
b) In the Softkey Template drop-down list box, choose the new softkey template that contains the CallBack softkey.

Step 4 Click the **Save** button.

A dialog box displays with a message to press Reset to update the phone settings.

Configure Call Back Button

This section provides detailed information to configure a Call Back button template.

Tip Before you configure the Call Back feature, review the task to configure Call Back.

Related Topics

Configure Call Back, on page 39

Create a Phone Button Template

Perform the following procedure to create a new phone button template with the CallBack feature button.

Procedure

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

The Phone Button Template Configuration window displays.

Step 2 From the Find and List Phone Button Template window, choose the phone button template for the IP phone that needs the Call Back feature button; for example, Standard 6961 SCCP.

Step 3 Click the **Copy** icon.

The Phone Button Template Configuration window displays with new information.

Step 4 In the Phone Button Template Name field, enter a new name for the template; for example, Standard 6961 SCCP for Call Back.

Step 5 Click the **Save** button.

The Phone Button Template Configuration redisplays with new information.

Step 6 To add the CallBack feature button to the template, choose any line button drop-down list box and choose CallBack.

Step 7 Click the **Save** button.

Add Phone Button Template

Perform the following procedure to add the CallBack phone button template to each user phone.

Procedure

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

The Find and List Phones window displays.

Step 2 Find the phone to which you want to add the phone button template. See topics related to Cisco Unified IP Phone configuration in the *Cisco Unified Communications Manager Administration Guide*.

Step 3 In the Phone Button Template drop-down list box, choose the new phone button template that contains the CallBack feature button.

Step 4 Click the **Save** button.

A dialog box displays with a message to press Reset to update the phone settings.

Set Call Back Service Parameters

You configure Call Back service parameters by accessing **System** > **Service Parameters** in Cisco Unified Communications Manager Administration; choose the server where the Cisco CallManager service runs and then choose the Cisco CallManager service.

Unless instructed otherwise by the Cisco Technical Assistance Center, Cisco recommends that you use the default service parameters settings. Call Back includes service parameters such as Callback Enabled Flag, Callback Audio Notification File Name, Connection Proposal Type, Connection Response Type, Call Back Request Protection T1 Timer, Callback Recall T3 Timer, Callback Calling Search Space, No Path Preservation, and Set Private Numbering Plan for Callback. For information on these parameters, click the question mark button that displays in the upper corner of the Service Parameter Configuration window.

Provide Call Back Information to Users

The Cisco Unified IP Phone user guides that are available on the web provide procedures for how to use the Call Back feature on the Cisco Unified IP Phone. Use these guides in conjunction with the question mark button help provided on the Cisco Unified IP Phone 7900 Series.

Troubleshooting Call Back

Use the Cisco Unified Serviceability Trace Configuration and Real Time Monitoring Tool to help troubleshoot call back problems. See the Cisco Unified Serviceability Administration Guide and the Cisco Unified Real Time Monitoring Tool Administration Guide.

CHAPTER 4

Call Control Discovery

This chapter provides information about the call control discovery feature. This feature leverages the Service Advertisement Framework (SAF) network service, a proprietary Cisco service, to facilitate dynamic provisioning of inter-call agent information. By adopting the SAF network service, the call control discovery feature allows Cisco Unified Communications Manager to advertise itself along with other key attributes, such as directory number patterns that are configured in Cisco Unified Communications Manager Administration, so other call control entities that also use SAF network can use the advertised information to dynamically configure and adapt their routing behaviors; likewise, all entities that use SAF advertise the directory number patterns that they own along with other key information, so other remote call-control entities can learn the information and adapt the routing behavior of the call.

Configure Call Control Discovery

The call control discovery feature leverages the Service Advertisement Framework (SAF) network service, a proprietary Cisco service, to facilitate dynamic provisioning of inter-call agent information. By adopting the SAF network service, the call control discovery feature allows Cisco Unified Communications Manager to advertise itself along with other key attributes, such as directory number patterns that are configured in Cisco Unified Communications Manager Administration, so other call control entities that also use SAF network can use the advertised information to dynamically configure and adapt their routing behaviors; likewise, all entities that use SAF advertise the directory number patterns that they own along with other key information, so other remote call-control entities can learn the information and adapt the routing behavior of the call. The following procedure configures the call control discovery feature in your network.

Procedure

Step 1 If you have not already done so, configure the Cisco IOS router as the SAF forwarder.

See the documentation that supports your Cisco IOS router; for example, see the Cisco IOS Service Advertisement Framework Configuration Guide or the Cisco IOS Service Advertisement Framework Command Reference. 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://www.cisco.com/go/cfn`.

Step 2 Configure the SAF security profile for the SAF forwarder (**Advanced Features** > **SAF** > **SAF Security Profile**).

You can configure more than one SAF security profile in Cisco Unified Communications Manager Administration. A SAF forwarder, which is a Cisco IOS router that you configured for SAF, handles the publishing requests for the local Cisco Unified Communications Manager cluster and the service advertisements from remote call-control entities.

Step 3 Configure the SAF forwarders in Cisco Unified Communications Manager Administration (**Advanced Features** > **SAF** > **SAF Forwarder**).

Cisco recommends that you configure a primary and backup SAF forwarder for failover support.

Step 4 Configure SAF-enabled SIP and/or H.323 intercluster (non-gatekeeper controlled) trunks (**Device** > **Trunk**).

The local Cisco Unified Communications Manager cluster uses SAF-enabled trunks that are assigned to the CCD requesting service to route outbound calls to remote call-control entities that use the SAF network. The Cisco Unified Communications Manager cluster advertises the SAF-enabled trunks that are assigned to the CCD advertising service along with the range of hosted DNs; therefore, when a user from a remote call-control entity makes an inbound call to a learned pattern on this Cisco Unified Communications Manager, this Cisco Unified Communications Manager receives the inbound call from this SAF-enabled trunk and routes the call to the correct DN.

Step 5 Configure the Hosted DN groups. Cisco recommends that you group the hosted DN patterns by location; for example, hosted DN patterns that represent different zip codes for a city may get grouped together. (**Call Routing** > **Call Control Discovery** > **Hosted DN Group**).

Hosted DN groups are a collection of hosted DN patterns that you group together in Cisco Unified Communications Manager Administration. You assign a hosted DN group to a CCD advertising service in Cisco Unified Communications Manager Administration, and the CCD advertising service publishes all the hosted DN patterns that are a part of the hosted DN group. You can only assign one Hosted DN group to one call control discovery advertising service.

Step 6 Configure the Hosted DN patterns. (**Call Routing** > **Call Control Discovery** > **Hosted DN Pattern**).

Hosted directory number (DN) patterns are patterns that represent directory numbers that belong to a call-control entity; for example, hosted DN patterns that you configure in Cisco Unified Communications Manager Administration are a range of directory numbers that belong to the local Cisco Unified Communications Manager cluster that you want to advertise to remote call-control entities. The CCD advertising service publishes the hosted DN patterns to the active SAF forwarder.

Step 7 To publish the hosted DNs for the local Cisco Unified Communications Manager cluster, configure the Call Control Discovery Advertising service. (**Call Routing** > **Call Control Discovery** > **Advertising Service**).

You can configure as many CCD advertising services as you want. The call control discovery advertising service, which resides in Cisco Unified Communications Manager, allows the local Cisco Unified Communications Manager cluster to advertise its hosted DNs and the PSTN failover configuration to the remote call-control entities that use the SAF network.

Step 8 Configure a partition that is used specifically for call control discovery. (**Call Routing** > **Call Control Discovery** > **Partition**).

This route partition gets used exclusively by the CCD requesting service to ensure that all learned patterns get placed in digit analysis under the route partition. You assign the partition to the CCD Requesting Service in Cisco Unified Communications Manager Administration.

Tip The partition that you assign to the CCD requesting service must belong to a calling search space that the devices can use for calling the learned patterns, so assign the partition to the calling search space that you want the devices to use. If you do not assign a calling search space that contains the partition to the device, the device cannot call the learned patterns.

Step 9 To ensure that the local Cisco Unified Communications Manager cluster can listen for advertisements from the SAF network, configure one call control discovery requesting service. (**Call Routing** > **Call Control Discovery** > **Requesting Service**).

You can only configure one CCD requesting service. The call control discovery requesting service, which resides in the local Cisco Unified Communications Manager, allows the local Cisco Unified Communications Manager to listen for hosted DN advertisements from remote call-control entities that use the SAF network.

Step 10 If you have not already done so, configure your remote call-control entity to use the SAF network; for example, configure Cisco Unified Communications Manager Express or other Cisco Unified Communications Manager clusters for the SAF network.

See the documentation that supports your remote call-control entity; for example, the Cisco Unified Communications Manager Express documentation.

Step 11 After you configure call control discovery, you may block learned patterns that remote call-control entities send to the local Cisco Unified Communications Manager. (**Call Routing** > **Call Control Discovery** > **Blocked Learned Patterns**).

Related Topics

Advertising Service, on page 59
Advertising Service Configuration, on page 88
Advertising Service and Hosted DN Patterns, on page 60
Blocked Learned Pattern Configuration, on page 94
Call Control Discovery, on page 53
Configure a SAF-Enabled Trunk, on page 100
Delete Configuration Records for Call Control Discovery, on page 100
Hosted DN Pattern Configuration, on page 86
Identify Hosted DN Patterns in a Hosted DN Group, on page 100
Install and Activate Call Control Discovery, on page 69
Learned Patterns and the Requesting Service, on page 61
Partition Configuration for Call Control Discovery, on page 89
Requesting Service, on page 61
Requesting Service Configuration, on page 91
SAF Forwarders, on page 64
SAF Forwarder Configuration, on page 81
SAF Security Profile Configuration, on page 79

Call Control Discovery Feature

This section contains information about Call Control Discovery.

Overview of Call Control Discovery

The call control discovery feature leverages the Service Advertisement Framework (SAF) network service, a proprietary Cisco service, to facilitate dynamic provisioning of inter-call agent information. By adopting the SAF network service, the call control discovery feature allows the local Cisco Unified Communications Manager to advertise itself along with other key attributes, such as directory number patterns that are configured in Cisco Unified Communications Manager Administration, so other call control entities that also use SAF network can use the advertised information to dynamically configure and adapt their routing behaviors; likewise, all entities that use SAF advertise the directory number patterns that they own along with other key information, so other remote call-control entities can learn the information and adapt the routing behavior of the call. Additionally, the call control discovery feature enables the network to facilitate communication between SAF-supported entities, instead of relying on additional servers to enable intercall agent communications.

Tip The call control discovery feature eliminates the need for redundant SIP proxies or complex gatekeeper configurations, which provide dial plan resolution and reachability status of remote call-control entities in the network.

With the call control discovery feature, each local Cisco Unified Communications Manager cluster can perform the following tasks:

- Establish an authenticated connection with the SAF network
- Advertise the cluster to the SAF network by providing the IPv4 address or hostname of the node, the signaling protocol and port numbers that the SAF network uses to contact the cluster, and the directory number patterns that are configured in Cisco Unified Communications Manager Administration for the cluster
- Register with the SAF network to listen for requests that are coming from other remote call-control entities that also use the SAF-related network
- Use the information that is learned from the advertisements to dynamically add patterns to its master routing table, which allows Cisco Unified Communications Manager to route and set up calls to these destinations by using the associated IP address and signaling protocol information.
- When connectivity to a remote call-control entity gets lost, the SAF network notifies Cisco Unified Communications Manager to mark the learned information as IP unreachable. The call then goes through the PSTN.
- Provide redundancy to advertise and listen for information, so if a node loses connectivity to its primary SAF forwarder for any reason, another backup SAF router can be selected to advertise and listen for information.

Components of Call Control Discovery

This section contains detailed information about the following topics:

- Call Control Discovery terminology
- Advertising service, SAF-enabled trunks, and hosted DN patterns
- Learned patterns and the CCD requesting service
- CCD requesting service and SAF-enabled trunks
- Network withdrawal support
- SAF forwarders

Tip All components for the call control discovery feature work together, so review all sections to understand how the feature works.

Call Control Discovery Terminology

The following table provides a brief overview of terminology that is associated with the call control discovery feature. For detailed information on each concept, click the links in the Description column in the table.

Table 6: Call Control Discovery Terminology

Terminology	Description
Call control discovery (CCD) advertising service	• Resides in Cisco Unified Communications Manager • Advertises the PSTN failover configuration and hosted DN patterns along with the SAF trunk access information for the local Cisco Unified Communications Manager cluster to the remote call-control entities that use the SAF network. • Configured under **Call Routing** > **Call Control Discovery** > **Advertising Service** in Cisco Unified Communications Manager Administration • Related Topics - Advertising Service, on page 59

Terminology	Description
Call control discovery (CCD) requesting service	- Resides in Cisco Unified Communications Manager - Allows the local Cisco Unified Communications Manager to listen for advertisements from remote call-control entities that use the SAF network. - Ensures that learned patterns (hosted DN patterns from remote call-control entities) get inserted into digit analysis on the local Cisco Unified Communications Manager - Performs load balancing for calls to learned patterns - Handles withdrawals for Cisco Unified Communications Manager from the SAF network - Configured under **Call Routing** > **Call Control Discovery** > **Requesting Service** in Cisco Unified Communications Manager Administration. - Related Topics - Requesting Service, on page 61
Hosted DN patterns	- Directory number patterns that belong to the local call-control entity **Tip** For example, hosted DN patterns that you configure in Cisco Unified Communications Manager Administration under **Call Routing** > **Call Control Discovery** > **Hosted DN Pattern** are directory numbers pattern ranges for the local Cisco Unified Communications Manager cluster that you want to advertise to remote call-control entities. - For the local Cisco Unified Communications Manager, published by the CCD advertising service to the SAF forwarder. - Related Topics - Advertising Service and Hosted DN Patterns, on page 60
Learned patterns	- Patterns that are inserted into digit analysis by the CCD requesting service - Can be manually purged or blocked on the local Cisco Unified Communications Manager - Viewed in RTMT - Related Topics - Learned Patterns and the Requesting Service, on page 61

Terminology	Description
SAF forwarder	• Cisco IOS router • Notifies the local Cisco Unified Communications Manager when remote call-control entities advertise their hosted DNs patterns. • Receives publish requests from the local Cisco Unified Communications Manager cluster so that Cisco Unified Communications Manager can advertise the hosted DN patterns for the cluster. • Related Topics - SAF Forwarders, on page 64
SAF-enabled trunks	• SAF-enabled trunks that are assigned to the CCD advertising service handle inbound calls from remote call-control entities that use the SAF network • SAF-enabled trunks that are assigned to the CCD requesting service handle outgoing calls to learned patterns • Related Topics - Advertising Service and SAF-Enabled Trunks, on page 59 and Learned Patterns and the Requesting Service, on page 61

Advertising Service

The call control discovery advertising service, which resides in Cisco Unified Communications Manager, allows the local Cisco Unified Communications Manager cluster to advertise the PSTN failover configuration, the hosted DN patterns, and the SAF-enabled trunk access information for its cluster to the remote call-control entities that use the SAF network. In Cisco Unified Communications Manager Administration under **Call Routing** > **Call Control Discovery** > **Advertising Service**, you can configure as many CCD advertising services as you want.

Advertising Service and SAF-Enabled Trunks

Consider the following information, which relates to how SAF-enabled trunks work with the CCD advertising service.

- After you configure SAF-enabled trunks in Cisco Unified Communications Manager Administration, you can choose one SIP trunk and one H.323 (non-gatekeeper controlled) trunk to associate with the CCD advertising service in the CCD Advertising Service window. The CCD advertising service advertises the hosted DN patterns, the PSTN failover configuration for the hosted DN patterns, the IP address for the node, the dynamic port number for the H.323 trunk, the QSIG configuration for the H.323 trunk, standard port 5060 for the SIP trunk, and the SIP route header information. It advertises the information for each trunk that is assigned to the CCD advertising service.
- SAF-enabled trunks do not have preconfigured destinations. For inbound calls from remote call-control entities, the local Cisco Unified Communications Manager uses the advertised dynamic trunk port number and/or SIP route header to find the proper dynamic trunk to process the call.
- The CCD advertising service, which runs on the same nodes as its assigned/selected trunks, advertises the same set of hosted DN pattern ranges for each type of trunk.

- For inbound calls from remote call-control entities to the local Cisco Unified Communications Manager, the call gets routed to the appropriate SAF-enabled trunk that is advertised by the CCD advertising service. For H.323 trunks, the incoming called party prefixes get applied to the called party number before the call gets routed.
- H.323 trunks support different features than SIP trunks; for example, H.323 supports QSIG, and SIP supports presence. If your feature support requires that you assign both a H.323 and SIP trunk to the CCD advertising service, assign both trunk types. If your feature support allows you to assign one trunk type, Cisco recommends that you assign one trunk to the CCD advertising service that best serves the cluster.
- If you assigned both a SAF-enabled SIP trunk and SAF-enabled H.323 (non-gatekeeper controlled) intercluster trunk to the CCD advertising service, load sharing of inbound calls occurs for the two trunks.
- The QSIG Variant and ASN.1 ROSE OID Encoding settings in the H.323 Configuration window get advertised by the CCD advertising service. These settings impact decoding of QSIG messages for inbound tunneled calls; for call control discovery, they do not impact outgoing calls.

Advertising Service and Hosted DN Patterns

Hosted directory numbers (DNs) patterns are a range of directory number patterns that belong to the call-control entity; for example, hosted DN patterns that you configure in Cisco Unified Communications Manager Administration under **Call Routing** > **Call Control Discovery** > **Hosted DNs Pattern** are directory numbers patterns for the local Cisco Unified Communications Manager that you want to advertise to remote call-control entities. The CCD advertising service publishes the hosted DN patterns for the local cluster to the active SAF forwarder.

- The CCD advertising service on the local Cisco Unified Communications Manager sends an advertising publish request on behalf of the hosted DN service in Cisco Unified Communications Manager to the primary SAF forwarder.
- Each hosted DN pattern belongs to a hosted DN group, which you assign to the CCD advertising service. Placing hosted DN patterns into a hosted DN group ensures that a CCD advertising service can advertise multiple patterns.
- When you update configured hosted DN patterns in the Hosted DN Patterns window in Cisco Unified Communications Manager Administration, the CCD advertising service resends a publishing request with the updated patterns to the active SAF forwarder. A publishing request gets sent for each trunk that is assigned to the CCD advertising service.
- If a Hosted DN pattern gets added or deleted in Cisco Unified Communications Manager Administration, the CCD advertising service sends a new publish request with a higher service version number to the SAF network.
- If you change the hosted DN group that is assigned to the CCD advertising service, the CCD advertising service publishes the patterns from the newly-updated hosted DN group along with a higher version number for each assigned SAF-enabled trunk.
- The CCD advertising service attempts to send many hosted DN patterns in a single publishing request. If there are more hosted DN patterns than can be sent in a single request, the local Cisco Unified Communications Manager sends multiple requests, each with a unique service identifier.
- For some clusters, the same hosted DN pattern may be published multiple times based on the SAF-trunk selection in the CCD advertising service configuration window. For example, hosted DN pattern 8902XXXX gets published twice for each node and each SAF-enabled trunk if the CCD advertising

service configuration contains both a SAF-enabled SIP and H.323 (non-gatekeeper controlled) trunk. If the Cisco Unified Communications Manager group for the trunk contains two nodes, four publishing requests for 8902XXX get sent. This approach ensures that the receiving entity performs load sharing.

- When you choose a different hosted DN group in the CCD Advertising Service window in Cisco Unified Communications Manager Administration, the service sends a request to the SAF forwarder to unpublish the hosted DN group and then publishes the updated configuration.

Tip If a hosted DN group association changes, a SAF trunk association changes, a SAF trunk is reset in Cisco Unified Communications Manager Administration, or the CCD advertising service is reset, the CCD advertising service will unpublish the previous request and publish it again with a new service ID; in addition, other clusters receive a withdrawal service notification from the SAF network, followed by a new notification from the SAF network.

Requesting Service

The call control discovery requesting service which resides in Cisco Unified Communications Manager, allows the local Cisco Unified Communications Manager to listen for advertisements from remote call-control entities that use the SAF network. The CCD requesting service is also responsible for inserting learned patterns from the remote call-control entities into digit analysis and the local cache. In Cisco Unified Communications Manager Administration under **Call Routing** > **Call Control Discovery** > **Requesting Service**, you can configure only one CCD requesting service.

After the SAF forwarder notifies the local Cisco Unified Communications Manager that remote call-control entities are advertising information, the CCD requesting service inserts the learned patterns along with a configured partition into digit analysis on the local Cisco Unified Communications Manager, and locally caches the learned patterns and the associated PSTN failover configuration from the remote call-control entity.

Learned Patterns and the Requesting Service

Remote call-control entities, such as other Cisco Unified Communications Manager clusters or Cisco Unified Communications Manager Express, request that their hosted DN patterns get advertised to other remote call-control entities. For Cisco Unified Communications Manager, after the CCD requesting service inserts the advertised DN patterns into digit analysis on the local Cisco Unified Communications Manager, Cisco Unified Communications Manager considers the pattern to be a learned pattern.

Consider the following information about learned patterns and the CCD requesting service:

- The CCD requesting service on the local Cisco Unified Communications Manager subscribes its primary SAF forwarder to the hosted DN service in order to learn about the hosted DN patterns that are advertised by the remote call-control entities. For the CCD requesting service to subscribe to the hosted DN service, you must assign a SAF-enabled trunk to the service and you must activate the service in the CCD Requesting Service Configuration window.
- If the local Cisco Unified Communications Manager receives overlapping DN patterns from remote call-control entities in single or multiple advertisements, Cisco Unified Communications Manager performs a best match for routing the call. For example, Cisco Unified Communications Manager receives patterns 813XXXX and 8135XXX. If a user dials 8135233, Cisco Unified Communications Manager routes the call to the trunk that is associated with pattern 8135XXX.
- When a learned pattern from a remote call-control entity such as Cisco Unified Communications Manager Express is the same as a locally configured static pattern, the local Cisco Unified Communications

Manager uses the calling search space configuration for the calling device to determine whether to route the call to the local or learned pattern.

- The CCD requesting service can identify duplicate learned patterns from remote call-control entities, such as other Cisco Unified Communications Manager clusters or Cisco Unified Communications Manager Express. How the CCD requesting service handles the patterns depends on your feature parameter configuration for call control discovery in Cisco Unified Communications Manager Administration. If the Issue Alarm for Duplicate Learned Pattern feature parameter is set to True, the CCD requesting service issues an alarm and stores the duplicate learned patterns; calls that use those patterns get load balanced among different call-control entities.

- If a call to a learned pattern cannot go over IP, the CCD requesting service routes the call via the PSTN. Be aware that the CCD requesting service redirects a call to the DID number based on the PSTN failover configuration for the learned pattern. If configured, the AAR calling search space for the calling device gets used to redirect the call during PSTN failover.

- If the CCD requesting service receives a learned pattern that is advertised by its own cluster, Cisco Unified Communications Manager ignores the patterns; for example, if a node in the same cluster as the requesting service advertises the learned patterns, Cisco Unified Communications Manager discards the patterns.

- The CCD requesting service performs regular expression checking for all learned patterns and converts lowercase wildcards to uppercase wildcards.

- If you want to do so, you can purge learned patterns that you no longer want to use, and you can block the learned patterns so that the local Cisco Unified Communications Manager ignores the patterns when they are advertised by remote call-control entities. For example, if you want to block a learned pattern with prefix 235 from a remote call-control entity with IP address of 111.11.11.11, you can block the pattern specifically for this call-control entity by entering the relevant information in the Block Learned Patterns window; in this example, after you save the configuration, the CCD requesting service searches the local cache and purges the learned patterns with 235 prefix from the remote call-control entity with IP address of 111.11.11.11. Any subsequent notifications with this information gets blocked and ignored by the local Cisco Unified Communications Manager. Be aware that blocking and purging of patterns is based on exact match; for example, configuring 235XX blocks 235XX, not any subsets of that pattern. Be aware that if you do not specify a remote call-control entity or remote IP address, Cisco Unified Communications Manager purges and blocks the pattern for all remote call-control entities that advertise the pattern.

  You can view purged and blocked learned patterns in the Find and List Blocked Learned Patterns window in Cisco Unified Communications Manager Administration. These purged or blocked patterns do not display in RTMT. If you delete a blocked pattern from Cisco Unified Communications Manager Administration, Cisco Unified Communications Manager can relearn those patterns if they are still available in the SAF network (and if the maximum number of learned patterns has not been reached for the cluster).

Requesting Service and SAF-Enabled Trunks

When you configure the CCD requesting service, you assign a SAF-enabled trunk to the service. Consider the following information on how the CCD requesting service works with SAF-enabled trunks:

- Cisco Unified Communications Manager routes outbound calls over SAF-enabled SIP or H.323 intercluster (non-gatekeeper controlled) trunks to remote call-control entities that use the SAF network; that is, the SAF-enabled trunks that you assign to the CCD requesting service manage outgoing calls to the learned DN patterns from the remote call-control entities.

- If the SAF-enabled trunk uses a Cisco Unified Communications Manager group with two Cisco Unified Communications Manager nodes. the CCD requesting service runs on each node after the SAF-enabled trunk registers with the Cisco Unified Communications Manager.
- When the device pool for a SAF-enabled trunk on a remote Cisco Unified Communications Manager contains three Cisco Unified Communications Manager nodes, the trunk runs on all three nodes and advertises the hosted DN service with the same DN patterns. The local Cisco Unified Communications Manager that subscribes to the Hosted DN service receives three advertisements with identical DN patterns but with different IP addresses for the 3 nodes. The CCD requesting service adds the DN patterns into its local cache and associates the patterns with the IP addresses of the three nodes. For an outbound call to a remote Cisco Unified Communications Manager, the CCD requesting service provides the dialed pattern and list of Cisco Unified Communications Managers that are associated with the DN to a SAF-enabled trunk that is assigned to the CCD requesting service. Load balancing occurs, as indicated in the following table. The trunk establishes the call in the order that is available to the trunk, and it goes to the next node in the list when a node is not available.
- The CCD requesting service provides the IP address and port number for the remote call-control entity to the SAF-enabled trunk.
- SAF-enabled trunks do not have preconfigured destinations. For outgoing calls to learned patterns, call control discovery provides the destination IP addresses to a dynamic trunk on a per call basis.
- The remote call-control entity determines whether QSIG tunneling is required for outgoing calls over H.323 trunks. If the remote call-control entity advertises that QSIG tunneling is required, the QSIG message is tunneled in the message of the outgoing call, even if the H.323 Configuration window in Cisco Unified Communications Manager Administration indicates that QSIG support is not required.
- The CCD requesting service performs round-robin load balancing for calls to learned patterns by considering learned pattern protocols, its local trunks, and IP addresses of the remote call-control entity that advertised the patterns. The following table shows how the CCD requesting service load balances calls to learned patterns by using SAF-enabled SIP and H.323 intercluster trunks.

Call	How it works
For the first call to 8408XXXX	The CCD requesting service selects the SIP trunk, and the call gets routed to the SIP trunk with the learned SIP trunk IP addresses of 10.1.1.1/5060, 10.1.1.2/5060.
For the second call to 8408XXXX	The CCD requesting service selects the H323 intercluster trunk with learned H323 trunk IP addresses of 10.1.1.1/3456, 10.1.1.2/7890.
For the third call to 8408XXXX	The CCD requesting service select the SIP trunk, and the call gets routed to the SIP trunk with the learned SIP trunk IP addresses of 10.1.1.2/5060, 10.1.1.1/5060.
For the fourth call to 8408XXXX	The CCD requesting service selects the H.323 intercluster trunk with the learned H.323 trunk IP addresses of 10.1.1.2/7890, 10.1.1.1/3456.

Network Withdrawal Support

The CCD requesting service handles withdrawals from the SAF network, as described in the following bullets:

- When the remote call-control entity unpublishes specific learned patterns, the CCD requesting service purges those learned patterns from the local cache and digit analysis when it receives a source withdrawal request from the SAF network; in this case, no calls can occur to those learned patterns.
- When the SAF forwarder loses network connection with its call-control entity, the SAF forwarder withdraws those learned patterns that were published by the call control entity. In this case, CCD requesting service marks those learned patterns as unreachable via IP, and the calls gets routed through the PSTN gateway.

  When a broken connection cannot be restored and if no new notification requests come in before the PSTN failover timer times out, the CCD requesting service unregisters all unreachable learned patterns from digit analysis and purges them from its local cache. In this case, no calls to these learned patterns occur.
- When the local Cisco Unified Communications Manager loses the TCP connection to both the primary and secondary SAF forwarder, the CCD requesting service marks all learned patterns as IP unreachable after the timer for the CCD Learned Pattern IP Reachable Duration feature parameter expires; in this case, all calls to learned patterns get routed through the PSTN gateway. If a connection to the SAF network does not get restored before the timer for the CCD PSTN Failover Duration parameter expires, the CCD requesting service unregisters all unreachable learned patterns from digit analysis and purges them from its local cache. Calls to the purged learned patterns fail.
- When the local Cisco Unified Communications Manager loses the TCP connection to the SAF forwarder, that SAF forwarder contacts all other SAF forwarders. In this case, the other SAF forwarders notify their call control entities, and the call control entities mark their patterns as unreachable via IP after their unreachable pattern duration timer expires (for Cisco Unified Communications Manager, this is the CCD Learned Pattern IP Reachable Duration feature parameter). For Cisco Unified Communications Manager, if a connection to the SAF network does not get restored before the timer for the CCD PSTN Failover Duration parameter expires, the CCD requesting service unregisters all unreachable learned patterns from digit analysis and purges them from its local cache. Calls to the purged learned patterns fail.

SAF Forwarders

A SAF forwarder, which is a Cisco IOS router configured for SAF, notifies the local Cisco Unified Communications Manager cluster when remote call-control entities advertise their hosted DNs patterns. In addition, the SAF forwarder receives publishing requests from the local Cisco Unified Communications Manager cluster for each configured and registered trunk that is configured in the CCD Advertising Service window; the publishing request contains the Hosted DN patterns for the Cisco Unified Communications Manager, the PSTN failover configuration, the listening port for the trunk, and, for SIP trunks, the SIP route header field, which contains a URI for the trunk.

The following table describes the SAF deployment models that Cisco Unified Communications Manager supports.

Table 7: SAF Deployment Models

Deployment Models	Description	Notes
Clusterwide	All nodes in the cluster can connect to all SAF forwarders.	The clusterwide deployment model can support primary and backup SAF forwarders.

Deployment Models	Description	Notes
Node-specific	Particular nodes in the cluster are assigned to the SAF forwarders, and those nodes prioritize these SAF forwarders over other configured SAF forwarders in the network; this means that the particular nodes always contact the assigned SAF forwarders first over other configured SAF forwarders.	The node-specific deployment model can support primary and backup SAF forwarders. This deployment model is recommended for cluster over WAN deployments where each node in the cluster is separated geographically and you route local traffic through local nodes; for COW deployments, you can configure multiple sets of primary and backup SAF forwarders to support different geophysical locations. You can assign up to two SAF forwarders to a particular node.

You can configure a single SAF forwarder, which provides no failover support, or you configure a primary and backup SAF forwarder to provide failover support. With primary and backup SAF forwarders, the Cisco Unified Communications Manager advertises to and subscribes to the backup SAF forwarder when the primary SAF forwarder is unavailable.

The SAF forwarder contains the IPv4 address and port that Cisco Unified Communications Manager uses to communicate with the SAF network. At start-up time, the SAF client control, which is a nonconfigurable, inherent component of Cisco Unified Communications Manager, marks the first SAF forwarder that registers with Cisco Unified Communications Manager as the primary SAF forwarder. Be aware that the primary SAF forwarder subscribes to the hosted DN services; the backup does not perform this task. The backup SAF forwarder immediately gets promoted to the primary SAF forwarder if/when the primary SAF forwarder becomes unavailable for any reason.

The SAF client control component in Cisco Unified Communications Manager maintains the connection to the SAF forwarder by sending keepalive messages to the SAF forwarder at regular intervals. The SAF client control component experiences keepalive response timeouts with network errors, TCP connection failures, or SAF forwarder failures. When the primary SAF forwarder becomes unreachable, the backup SAF forwarder automatically becomes the primary SAF forwarder, and the SAF client component in Cisco Unified Communications Manager tries to establish a connection with the failed SAF forwarder. When the connection is successfully established, the SAF forwarder gets designated again as the backup SAF forwarder. Under these circumstances, the SAF client control component uses the newly (currently) promoted primary SAF forwarder and notifies the CCD advertising and requesting services that the current primary SAF forwarder is being used. The CCD services send all publishing and subscription requests to the current primary SAF forwarder, and the current primary SAF forwarder sends notifications for all the Hosted DNs service advertisements that it receives to the SAF client control component, which forwards the advertisements to the CCD requesting service. The CCD requesting service compares the notifications that it received from the backup SAF forwarder with its cached information and updates, deletes or adds new information, as appropriate. The SAF client control component attempts to reconnect to the failed SAF forwarder at regular intervals. When the connection attempt is successful, the SAF client control component registers again with the previously failed SAF forwarder and redesignates the other SAF forwarder as the backup.

Tip Cisco Unified Communications Manager always advertises to and subscribes to the primary SAF forwarder, even when you have more than 2 SAF forwarders configured in the database. If the primary SAF forwarder gets deleted from the database, then the backup SAF forwarder automatically becomes the primary SAF forwarder, and Cisco Unified Communications Manager promotes another configured SAF forwarder to the backup SAF forwarder.

Tip For clusterwide deployments, you cannot designate the primary and backup SAF forwarders. The Cisco Unified Communications Manager database sends an ordered list of SAF forwarders to the Cisco Unified Communications Manager.

Tip If one or both of the SAF forwarders do not work, Cisco Unified Communications Manager does not attempt to connect to a third SAF forwarder, even if a third SAF forwarder is configured. If the connection is lost for the primary and backup SAF forwarder, the Cisco Unified Communications Manager does not connect to the third SAF forwarder, even if a third SAF forwarder is configured.

If the CCD advertising or requesting service loses connection with SAF network, the SAF forwarder informs all other call control discovery services about the service interruption. The client continually attempts to register to the SAF forwarder. After the CCD service reconnects with the SAF network, the SAF forwarder immediately informs all CCD services about the service restoration.

When the SAF forwarder detects a TCP connection failure with other SAF forwarders or one of its external clients, such as Cisco Unified Communications Manager or Cisco Unified Communications Manager Express, Cisco Unified Communications Manager marks learned patterns as unreachable after it receives a network withdrawal notification from the SAF forwarder. All subsequent calls to these learned patterns get routed over the PSTN by using the PSTN failover configuration for the unreachable learned patterns. The timer for the CCD PSTN Failover Duration feature parameter starts as soon as the network withdrawal notification is received. If Cisco Unified Communications Manager receives another network withdrawal notification when the timer is going, Cisco Unified Communications Manager restarts the timer.

Tip Cisco Unified Communications Manager uses digest authentication (SHA1) to communicate with the SAF forwarder. You configure a SAF Forwarder security profile, which includes the username and password in requests that Cisco Unified Communications Manager sends to the SAF forwarder; the requests must include the MESSAGE INTEGRITY attribute to include the username and password.

When a connection loss occurs between the SAF forwarder and the Cisco Unified Communications Manager, for example, a cable for the server or router gets unplugged, the registration status may look correct, even when it is not. In this case, patterns may appear to be reachable until the SAF keepalive timer (on the SAF forwarder) or the TCP timer expires. After the timer for the TCP timer expires, the patterns are marked as unreachable.

System Requirements for Call Control Discovery

The following system requirements exist for Cisco Unified Communications Manager:

- Local Cisco Unified Communications Manager 8.0(2) (or higher) cluster
- SAF-enabled SIP or H.323 intercluster (non-gatekeeper controlled) trunks
- Remote call-control entities that support and use the SAF network; for example, other Cisco Unified Communications Manager 8.0(2) (or higher) clusters or Cisco Unified Communications Manager Express servers
- Cisco IOS router(s) that are configured as SAF forwarders

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://www.cisco.com/go/cfn`.

Interactions and Restrictions

Autonomous System

All Cisco Unified Communications Manager clusters are limited to advertised or learned routes within the same autonomous system (AS).

BLF Subscriptions

If a user wants to subscribe BLF status of a SAF learned pattern, Cisco Unified Communications Manager sends a SIP subscribe message over a SIP trunk to the remote cluster.

This functionality is supported with SAF-enabled SIP trunks only (not with SAF-enabled H.323 trunks).

Bulk Administration Tool

In the Bulk Administration Tool, you can import and export the configuration for SAF security profiles, SAF forwarder, CCD advertising service, CCD requesting service, hosted DN groups, and hosted DN patterns, and so on. For information on how to import and export the configuration, see the Cisco Unified Communications Manager Bulk Administration Guide.

Call Detail Records

Cisco Unified Communications Manager supports redirecting onBehalfOf as SAFCCDRequestingService with a redirection reason as SS_RFR_SAF_CCD_PSTNFAILOVER, which indicates that the call is redirected to a PSTN failover number.

For more information on call detail records, see the Cisco Unified Communications Manager Call Detail Records Administration Guide.

Incoming Called Party Settings

The H.323 protocol does not support the international escape character +. To ensure that the correct DN patterns get used with SAF/call control discovery for inbound calls over H.323 gateways/trunks, you must configure the incoming called party settings in the service parameter, device pool, H.323 gateway, or H.323 trunk windows; that is, configuring the incoming called party settings ensures that when a inbound call comes from a H.323 gateway or trunk, Cisco Unified Communications Manager transforms the called party number back to the value that was originally sent over the trunk/gateway. See the following example for more information.

- For example, a caller places a call to +19721230000 to Cisco Unified Communications Manager A.
- Cisco Unified Communications Manager A receives +19721230000 and transforms the number to 55519721230000 before sending the call to the H.323 trunk. In this case, your configuration indicates that the international escape character + should be stripped and 555 should be prepended for calls of International type.
- For this inbound call from the trunk, Cisco Unified Communications Manager B receives 55519721230000 and transforms the number back to +19721230000 so that digit analysis can use the value as it was sent by the caller. In this case, your configuration for the incoming called party settings indicates that you want 555 to be stripped and +1 to be prepended to called party numbers of International type.

Cisco Unified Serviceability

Cisco Unified Serviceability provides alarms to support the call control discovery feature. For information on how to configure alarms, see the Cisco Unified Serviceability Administration Guide. For alarm definitions that are associated with the call control discovery feature, see the Troubleshooting Call Control Discovery, on page 101.

Dialed Number Analyzer

Dialed Number Analyzer allows you to add learned patterns so that you can analyze them for your dialing plan. For more information on how to perform this task, see the Cisco Unified Communications Manager Dialed Number Analyzer Guide.

Digest Authentication

Cisco Unified Communications Manager uses digest authentication (without TLS) to authenticate to the SAF forwarder. When Cisco Unified Communications Manager sends a message to the SAF forwarder, Cisco Unified Communications Manager computes the SHA1 checksum and includes it in the MESSAGE-INTEGRITY field in the message.

You must configure a SAF security profile. For more information, see the SAF Security Profile Configuration, on page 79.

QSIG

The QSIG Variant and ASN.1 ROSE OID Encoding settings in the H.323 Configuration window get advertised by the CCD advertising service. These settings impact decoding of QSIG messages for inbound tunneled calls; for call control discovery, they do not impact outgoing calls.

The remote call-control entity determines whether QSIG tunneling is required for outgoing calls over H.323 trunks. If the remote call-control entity advertises that QSIG tunneling is required, the QSIG message is tunneled in the message of the outgoing call, even if the H.323 Configuration window in Cisco Unified Communications Manager Administration indicates that QSIG support is not required.

Real Time Monitoring Tool

The Real Time Monitoring Tool displays perfmon counters that support the call control discovery features. For information on these perfmon counters, see the Cisco Unified Real Time Monitoring Tool Administration Guide.

The Real Time Monitoring Tool allows you to view reports for learned patterns and SAF forwarders.

Learned Pattern reports include such information as learned pattern name, time stamp, reachability status for the pattern, remote call-control entity that hosts the pattern, the PSTN failover configuration, and the destination IP address and port. RTMT allows you to search based on different criteria; for example, if you specify a search for the remote call-control entity, all the learned patterns display for the remote call-control entity.

SAF Forwarder reports display information such as authentication status, registration status of SAF forwarders, and so on.

For more information on these reports, see the Cisco Unified Real Time Monitoring Tool Administration Guide.

SAF Network Issues

When the Cisco Unified Communications Manager cannot connect to the SAF forwarder, Cisco recommends that you do not update the configuration for the CCD requesting service or CCD advertising service, unless these services are inactive; that is, the Activated Feature check box is unchecked in Cisco Unified Communications Manager Administration. If you update the services when Cisco Unified Communications Manager cannot connect to the SAF network and these services are active, problems may occur; for example, patterns may not be classified correctly as unreachable or reachable, duplicate or stale patterns may exist, and so on.

In addition, Cisco recommends that you do not update the SAF forwarder configuration when the Cisco Unified Communications Manager cannot connect to the SAF forwarder.

Install and Activate Call Control Discovery

After you install Cisco Unified Communications Manager, your network can support the call control discovery feature if you perform the necessary configuration tasks. For information on configuration tasks that you must perform, see the Configure Call Control Discovery, on page 53.

Configuring Call Control Discovery

Tip Before you configure the call control discovery feature, review the Configure Call Control Discovery, on page 53.

This section contains information on the following topics:

- Considerations for Call Control Discovery Configuration, on page 70
- Call Control Discovery Feature Parameters, on page 75
- SAF Security Profile Configuration, on page 79
- SAF Forwarder Configuration, on page 81
- Hosted DN Group Configuration, on page 84
- Hosted DN Pattern Configuration, on page 86
- Advertising Service Configuration, on page 88
- Partition Configuration for Call Control Discovery, on page 89
- Requesting Service Configuration, on page 91
- Blocked Learned Pattern Configuration, on page 94
- Configuration Records for Call Control Discovery, on page 96 (provides information on how to run searches for the configuration that is related to call control discovery; provides information on how to work in the Find and List windows)
- SAF Security Profile Configuration, on page 79 (provides procedure for working in the Call Control Discovery windows; section does not provide descriptions for configuration settings)
- Configure a SAF-Enabled Trunk, on page 100
- Advertising Service Configuration, on page 88
- Delete Configuration Records for Call Control Discovery, on page 100

Considerations for Call Control Discovery Configuration

Review the following considerations before you configure the call control discovery feature:

- SAF Forwarders, on page 71
- Hosted DN Patterns and Groups, on page 71
- Advertising and Requesting Services, on page 72
- SAF-Enabled Trunks , on page 73

Tip This section does not describe all configuration considerations. This section provides high-level considerations that you should review before you configure the CCD configuration settings. Use this section in conjunction with the sections that are highlighted under the Considerations for Call Control Discovery Configuration, on page 70.

SAF Forwarders

- Cisco recommends that you configure a primary and backup SAF forwarder for redundancy.
- When you configure a SAF forwarder or SAF security profile, some configuration in Cisco Unified Communications Manager Administration must match the configuration that you entered on the Cisco IOS router.
- Cisco Unified Communications Manager supports the following deployment models for SAF forwarders: clusterwide or node-specific. Before you configure SAF forwarders, review SAF Forwarders, on page 64, which describes these deployment models.
- You can only configure IPv4 for SAF forwarders.
- Each SAF forwarder must have a unique IP address.
- Cisco recommends that you do not update the SAF forwarder configuration when the Cisco Unified Communications Manager cannot connect to the SAF forwarder.
- For information on SAF forwarder field descriptions, see SAF Security Profile Configuration, on page 79.

Hosted DN Patterns and Groups

- Be aware that the PSTN Failover Strip Digits, PSTN Failover Prepend Digits, and Use HostedDN as PSTN Failover settings display in both the Hosted DN Group and Hosted DN Patterns Configuration windows. If you do not configure these settings in the Hosted DN Patterns Configuration window, the Hosted DN Group configuration applies to the hosted DN patterns.
- Each hosted DN group covers one geophysical location advertising DN range.
- In the Find and List window for Hosted DN Patterns, you can download a .cvs file so that you can add or update multiple hosted DN patterns for the call control discovery feature at the same time. Then, you can upload the patterns in the same window. (You can also add or update multiple hosted DN patterns in BAT.)

  If you choose to replace the patterns when you upload the patterns, you lose all hosted DN patterns.

  If invalid or bad data exists in the .csv file, the data gets ignored by Cisco Unified Communications Manager.
- Cisco Unified Communications Manager allows you to configure up to 10,000 hosted DN patterns per cluster.
- Each hosted DN pattern must be unique. Each hosted DN pattern can only exist in one hosted DN group.

- The Find and List Hosted DN Patterns window allows you to identify which hosted DN patterns belong to a Hosted DN group. For more information on how to perform this task, see the Identify Hosted DN Patterns in a Hosted DN Group, on page 100.
- For information on field descriptions for hosted DN groups and hosted DN patterns, see the Hosted DN Group Configuration, on page 84 and Hosted DN Pattern Configuration, on page 86.

Advertising and Requesting Services

- You cannot name any CCD advertising service and the CCD requesting service the same name in Cisco Unified Communications Manager Administration.
- You must enable SAF on the trunk in Cisco Unified Communications Manager Administration and assign SAF-enabled trunks to the CCD advertising and requesting services in Cisco Unified Communications Manager Administration. Be aware that SAF-enabled SIP trunks only support UDP or TCP. If you want to do so, you can use the same SAF-enabled trunks for the CCD advertising service and CCD requesting service. For information on enabling SAF on the trunks, see the Configure a SAF-Enabled Trunk, on page 100.
- You can configure one CCD requesting service. You can configure as many CCD advertising services as you want.
- Only one hosted DN group can be associated with one CCD advertising service.
- The call control discovery feature relies on a route partition, which you configure in the CCD Partition window (**Call Routing** > **Call Control Discovery** > **Partition**). This route partition gets used exclusively by the call control discovery to ensure that all learned patterns get placed in digit analysis under the route partition. You assign this partition to the CCD requesting service.

  Be aware that the CCD partition does not display under **Call Routing** > **Class of Control** > **Partition** in Cisco Unified Communications Manager Administration.

  For field descriptions for the CCD partition, see the Partition Configuration for Call Control Discovery, on page 89.

Tip Updating the Learned Pattern Prefix field or Route Partition field in the CCD Requesting Service Configuration window may impact system performance because the digit-analysis master routing table automatically gets updated when these fields are changed. To avoid system performance issues, Cisco recommends that you update these fields during off-peak hours.

- After you make changes to the configuration for the CCD advertising and requesting services, click **Save**. You do not need to click the **Reset** button in these windows unless you want the following events to occur:
  - For the CCD Advertising Service-The **Reset** button in the CCD Advertising Service Configuration window triggers the call control discovery advertising service to withdraw existing publishing requests and to publish all the related information again.
  - For the CCD Requesting Service-The **Reset** button in the CCD Requesting Service Configuration window causes the requesting service to remove the learned patterns from the local cache and for the requesting service to subscribe to the SAF network again. By clicking the **Reset** button in the CCD Requesting Service Configuration window, Cisco Unified Communications Manager can learn patterns again.

To minimize the impact to your network, Cisco recommends that you click the **Reset** button in the CCD Advertising Configuration window or the CCD Requesting Configuration window during off-peak hours.

Be aware that clicking **Reset** in the CCD Advertising and Requesting Service Configuration windows does not reset the trunk. You reset the trunk in the Trunk Configuration window.

- When you delete a CCD advertising service, all hosted DN patterns that are advertised with each assigned trunk get unpublished.
- When you delete the CCD requesting service, all learned patterns get unregistered from the local cache and digit analysis.
- If you want a user to make outbound calls to learned patterns that are advertised by remote call-control entities, ensure that the calling search space that you assign to the device contains the route partition that is assigned to the CCD requesting service.
- When the Cisco Unified Communications Manager cannot connect to the SAF forwarder, Cisco recommends that you do not update the configuration for the CCD requesting service or CCD advertising service, unless these services are inactive; that is, the Activated Feature check box is unchecked in Cisco Unified Communications Manager Administration. If you update the services when Cisco Unified Communications Manager cannot connect to the SAF network and these services are active, problems may occur; for example, patterns may not be classified correctly as unreachable or reachable, duplicate or stale patterns may exist, and so on.
- Make sure that the call-control entities do not advertise the same hosted DN patterns.

  If the call-control entities advertise the same hosted DN patterns, problems may occur; for example, a call routing loop may occur between advertising clusters when these clusters make calls to learned patterns by using a calling search space where the learned pattern partition is in front of the locally configured static partition.
- For information on field descriptions for the CCD advertising service and for the CCD requesting service, see the Advertising Service Configuration, on page 88 and the Requesting Service Configuration, on page 91.

SAF-Enabled Trunks

- One configured SAF-enabled H.323 trunk and one configured SAF-enabled SIP trunk can serve all SIP and H.323 calls to learned patterns for one cluster.
- Make sure that you apply the configuration to the SAF-enabled trunk before you assign the trunk to the CCD advertising or requesting service. You apply the configuration in the Trunk Configuration window.
- If you do not select/assign a SAF-enabled trunk when you configure the CCD requesting service, the CCD requesting service does not get created and patterns do not get learned.
- If you assign both a H.323 and a SIP SAF-enabled trunk to the CCD requesting service, make sure that the same Cisco Unified Communications Manager group exists in the device pool that is assigned to the trunk.
- To support clustering over WAN deployments, configure different Cisco Unified Communications Manager groups to associate with sets of SAF-enabled trunks.

- To ensure redundancy and reduce call-processing traffic, Cisco recommends that no more than two nodes exist in the Cisco Unified Communications Manager group for the device pool that you assign to the SAF-enabled trunk.
- If a trunk is assigned to a route group or associated with a route pattern, you cannot enable SAF on the trunk. Likewise, if you enable SAF on the trunk, you cannot assign the trunk to a route group or associate the trunk with a route pattern.
- Verify that the SIP trunk has a security profile of Nonsecure before you enable SAF on the trunk. You cannot enable SAF on SIP trunks that use authenticated or encrypted security profiles.
- Resetting a SAF-enabled trunk that is assigned to the CCD advertising service causes the CCD advertising service to unpublish the hosted DN patterns and republish with a different service ID for that trunk.
- If different SAF-enabled trunks are configured to use different Cisco Unified Communications Manager groups, the inbound and outbound SAF-related call traffic gets distributed among different Cisco Unified Communications Manager nodes.
- If a Cisco Unified Communications Manager group changes for the SAF-enabled trunk, the CCD advertising service sends unpublish requests to the SAF network; in addition, the CCD requesting service removes the learned patterns from the local cache and digit analysis because no trunk runs on this Cisco Unified Communications Manager node. After the CCD advertising service and/or requesting service start on the new nodes, the advertising service sends a publish request to the SAF network, and the requesting service sends a subscribe request to the SAF network.
- If you change the device pool of the SAF-enabled trunk, the CCD advertising service sends unpublish requests to the SAF network; in addition, the CCD requesting service removes the learned patterns from the local cache and digit analysis because no trunk runs on this Cisco Unified Communications Manager node. After the CCD advertising service and/or requesting service start on the new nodes, the advertising service sends a publish request to the SAF network, and the requesting service sends a subscribe request to the SAF network.
- If you want to delete a SAF-enabled trunk from Cisco Unified Communications Manager Administration, you must unassign the trunk from the CCD advertising service and/or CCD requesting service before you delete it from the Trunk Configuration window.
- Be aware that resetting a SAF-enabled trunk or changing the Cisco Unified Communications Manager group for the trunk impacts the CCD advertising and requesting services. For example, if you reset a trunk and the CCD requesting service cannot access the trunk after 10 seconds have passed, all learned patterns get purged from digit analysis and from the local cache, and the requesting process stops.

Miscellaneous Considerations

- To ensure PSTN failover, configure a route pattern and assign the route pattern to the gateway.
- If your cluster does not support E.164, you must configure translation patterns so that your users can dial E.164 numbers.
- You can view purged and blocked learned patterns in the Find and List Blocked Learned Patterns window in Cisco Unified Communications Manager Administration. If you delete a blocked pattern from Cisco Unified Communications Manager Administration, Cisco Unified Communications Manager can relearn those patterns if they are still available in the SAF network (and if the maximum number of learned patterns has not been reached for the cluster).
- Learned patterns are viewed in RTMT.

Call Control Discovery Feature Parameters

To access the feature parameters that support the call control discovery feature, choose **Call Routing** > **Call Control Discovery** > **Feature Configuration**. The following table describes the feature parameters for the call control discovery feature. For additional information, you can click the question mark help in the Feature Configuration window.

Table 8: Call Control Discovery Feature Parameters

Feature Parameter	Description
CCD Maximum Number of Learned Patterns	This parameter specifies the number of patterns that this Cisco Unified Communications Manager cluster can learn from the SAF network. The higher the number of allowed learned patterns, the more memory and CPU processing power is required for your server. When Cisco Unified Communications Manager attempts to learn more patterns than is specified in the parameter configuration, the alarm, CCDLearnedPatternLimitReached, gets issued.
CCD Learned Pattern IP Reachable Duration	This parameter specifies the number of seconds that learned patterns stay active (reachable) before Cisco Unified Communications Manager marks those patterns as unreachable. For example, you configure 20 seconds for this parameter; when Cisco Unified Communications Manager cannot communicate with the SAF forwarder after 20 seconds, all calls to learned patterns fail over to the PSTN until IP connectivity to the SAF forwarder gets restored. During the PSTN failover, Cisco Unified Communications Manager cannot learn new patterns. After the time that you specified for this parameter elapses, Cisco Unified Communications Manager marks the learned patterns as unreachable. Use this parameter with the CCD PSTN Failover Duration parameter, which allows patterns that have been marked as unreachable to be reached through PSTN failover. You can enter a number (seconds) from 0 to 300; the default equals 60 seconds.

Feature Parameter	Description
CCD PSTN Failover Duration	This parameter specifies the number of minutes that calls to unreachable/inactive learned patterns are routed through the PSTN gateway and then purged from the system. The configuration for this parameter does not take effect until after the timer expires for the CCD Learned Pattern IP Reachable Duration parameter. The expiration of the CCD Learned Pattern IP Reachable Duration parameter indicates that IP connectivity fails between the SAF forwarder and Cisco Unified Communications Manager, and all learned patterns get marked as unreachable. Then, when the duration expires for CCD PSTN Failover Duration parameter, all learned patterns get purged from the system and calls to purged patterns are rejected (caller hears reorder tone or “number is unavailable” announcement). Setting this parameter to 0 means that PSTN failover cannot occur; that is, if the SAF forwarder cannot be reached for the number of seconds that you defined in the CCD Learned Pattern IP Reachable Duration parameter, no failover option is provided over the PSTN, and calls to learned patterns immediately fail. Setting this parameter to 525600 means that PSTN failover never expires and learned patterns never get purged because of IP connectivity issues. You can enter a number (minutes) from 0 to 525600; the default equals 2880.
Issue Alarm for Duplicate Learned Patterns	This parameter determines whether Cisco Unified Communications Manager issues the alarm, DuplicateLearnedPattern, when it learns duplicate patterns from different remote call-control entities on the SAF network. The default equals False.

Feature Parameter	Description
CCD Stop Routing On Unallocated Unassigned Number	This parameter determines whether Cisco Unified Communications Manager continues to route calls to a remote call-control entity, such as a Cisco Unified Communications Manager cluster or Cisco Unified Communications Manager Express, when the remote call-control entity rejects the call with the cause code for Unallocated/Unassigned Number. Be aware that an unallocated number represents a hosted DN that does not exist in the current call control entity. The default equals True. If the parameter is set to True, the call is released as soon as Cisco Unified Communications Manager receives the cause code from the remote call-control entity. If the parameter is set to False, when Cisco Unified Communications Manager extends the call to the learned pattern and the remote call-control entity sends the unallocated number cause value, Cisco Unified Communications Manager attempts to find another reachable IP address for the remote cluster for this learned pattern. If any reachable remote destination is available, Cisco Unified Communications Manager tries to extend the call to the IP address of the available reachable remote cluster.

Feature Parameter	Description
Set Urgent Priority for Fixed-Length CCD Learned Patterns	This parameter determines whether Cisco Unified Communications Manager waits for interdigit timer before routing the call to the destination that is associated with the fixed-length learned pattern (when the fixed-length learned pattern is a better match for the sequence of digits dialed as compared to the overlapping route pattern configured). If the parameter is set to True, Cisco Unified Communications Manager does not wait for the interdigit timer before routing the call to the destination that is associated with the fixed-length learned pattern. If the parameter is set to False, Cisco Unified Communications Manager waits for interdigit timer before routing the call to the destination that is associated with the fixed-length learned pattern. The default equals False. Example: Cisco Unified Communications Manager learns the pattern +44987XXX for routing the calls to another Cisco Unified Communications Manager and there is also a route pattern configured as \+44! for routing the calls to the PSTN destination. If this parameter is set to False and +44987127 is dialed, Cisco Unified Communications Manager waits for interdigit timer before routing the call to another Cisco Unified Communications Manager (this interdigit timer allows user to dial more digits after +44987127 to reach the PSTN destination). If this parameter is set to True and +44987127 is dialed, then Cisco Unified Communications Manager immediately routes the call to another Cisco Unified Communications Manager.

Feature Parameter	Description
Set Urgent Priority for Variable-Length CCD Learned Patterns	This parameter determines whether Cisco Unified Communications Manager waits for interdigit timer before routing the call to the destination that is associated with the variable-length learned pattern. If the parameter is set to True, Cisco Unified Communications Manager does not wait for interdigit timer before routing the call to the destination that is associated with the variable-length learned pattern. If the parameter is set to False, Cisco Unified Communications Manager waits for interdigit timer before routing the call to the destination that is associated with the variable-length learned pattern. The default equals False. Example: Cisco Unified Communications Manager has translation pattern 9011.!# configured. This translation pattern strips predot digits and the trailing # character and adds the prefix +55 to the dialed digits. Cisco Unified Communications Manager also learns pattern \+55.! for routing the calls to another Cisco Unified Communications Manager. If this parameter is set to False and 9011234567# (resultant digits = +55234567) is dialed, Cisco Unified Communications Manager waits for interdigit timer before routing the call to another Cisco Unified Communications Manager. If this parameter is set to True and 9011234567# (resultant digits = +55234567) is dialed, then Cisco Unified Communications Manager immediately routes the call to another Cisco Unified Communications Manager.

SAF Security Profile Configuration

Configuration Path-**Advanced Features** > **SAF** > **SAF Security Profile**

In the SAF Security Profile Configuration window, you configure a SAF security profile so that a secure connection occurs between the SAF forwarder and the Cisco Unified Communications Manager. When you configure a SAF forwarder in the SAF Forwarder Configuration window, you must choose a SAF security profile to apply to the SAF forwarder.

The call control discovery feature leverages the Service Advertisement Framework (SAF) network service, a proprietary Cisco service, to facilitate dynamic provisioning of inter-call agent information. For more information on the call control discovery feature, see the Call Control Discovery, on page 53.

Cisco Unified Communications Manager uses digest authentication (SHA1) to communicate with the SAF forwarder.

Before You Begin

Be aware that some of the information that you configure in this window must also be configured on the SAF forwarder.

Before you configure the SAF security profile, see the Configure Call Control Discovery, on page 53 and Considerations for Call Control Discovery Configuration, on page 70.

Table 9: SAF Security Profile Configuration Settings

Field	Description
Name	Enter the name of the SAF security profile. The name that you enter displays in the Find and List SAF Security Profile window and in the SAF Security Profile drop-down list box in the SAF Forwarder Configuration window. Valid entries include alphanumeric characters, hyphen, period, underscore, and blank spaces. You can configure up to 50 characters.
Description	Enter a description for the SAF security profile. You can enter all characters except for \, “, < >, &, and %. You can configure up to 128 characters.
User Name	Enter a value that you want Cisco Unified Communications Manager to include in requests when it contacts the SAF forwarder. **Tip** To ensure that the Cisco Unified Communications Manager can register with the SAF forwarder, enter the same user name that you entered on the router (SAF forwarder). The user name is case sensitive, so enter the user name exactly as you entered it on the SAF forwarder. The value that you enter represents the shared secret for message integrity checks between Cisco Unified Communications Manager and the SAF forwarder. The user name gets included in any request from Cisco Unified Communications Manager that contains the MESSAGE-INTEGRITY attribute.

Field	Description
User Password	Enter a value that you want Cisco Unified Communications Manager to include in requests when it contacts the SAF forwarder. **Tip** To ensure that the Cisco Unified Communications Manager can register with the SAF forwarder, enter the same password that you entered on the router (SAF forwarder). The password is case sensitive, so enter the password exactly as you entered it on the SAF forwarder.

SAF Forwarder Configuration

Configuration Path-**Advanced Features** > **SAF** > **SAF Forwarder**

A SAF forwarder, a Cisco router that you configure for call control discovery/SAF, handles the publishing requests from Cisco Unified Communications Manager for the call control discovery feature. In addition, the SAF forwarder handles advertising requests from remote call-control entities for the call control discovery feature. For information on call control discovery, see the Call Control Discovery, on page 53.

Before You Begin

Before you configure the SAF forwarder, make sure that you have configured at least one SAF security profile.

Be aware that some of the information that you configure in this window must also be configured on the SAF forwarder.

Before you configure the SAF forwarder, see the Configure Call Control Discovery, on page 53 and Install and Activate Call Control Discovery, on page 69.

Table 10: SAF Forwarder Configuration Settings

Field	Description
Name	Enter the name of the SAF forwarder. Valid entries include alphanumeric characters, hyphen, period, and underscore. You can enter up to 50 characters. The value that you enter in this field gets used to classify SAF forwarder records in the database. The value that you enter displays in the Find and List SAF Forwarder window when you perform a search.
Description	Enter a description for the SAF forwarder. You can enter all characters except for \, “, < >, &, and %. You can enter up to 128 characters.

Field	Description
Client Label	The client label allows the SAF forwarder to identify the Cisco Unified Communications Manager node. Valid entries include alphanumeric characters, underscore, and @. You can enter up to 50 characters. Each Cisco Unified Communications Manager node that you select to interact with this SAF forwarder includes its unique client label in the registration message that it sends to the SAF forwarder. When the SAF forwarder receives the registration message, it verifies whether you configured the client label on the SAF forwarder. When you configure a single SAF forwarder for the entire cluster, all nodes in the cluster use the same SAF forwarder configuration and register to the same SAF forwarder. To create a unique client label for the nodes in the cluster, you can append @ to the client label value, which ensures that the registration message includes the basename followed by @<nodeid>. For example, you enter abcde_ny@ for the client label for a two-node cluster that connects to one SAF forwarder, so the registration message includes abcde_ny@1 for node 1 or abcde_ny@2 for node 2. If you do not append the @ to the client label value, you do not need to configure the basename parameter for the client label on the router, but you do need to configure the client label on the router. If you append the @ to the client label value, you must configure the basename parameter with the client label on the router. **Tip** If more than one Cisco Unified Communications Manager node displays in the Selected Cisco Unified Communications Managers pane under the Showed Advanced section, append @ to the client label value; otherwise, errors may occur because each node uses the same client label to register with the SAF forwarder.
SAF Security Profile	Choose the SAF security profile that you want to apply to this SAF forwarder. The username and password from the security profile get sent to the SAF forwarder, so choose a security profile that contains a username and password that the SAF forwarder will accept. (The SAF forwarder must be configured to use the same username and password.)

Field	Description
SAF Forwarder Address	Enter the IPv4 address of the SAF forwarder.
SAF Forwarder Port	Enter the port number that Cisco Unified Communications Manager uses to establish a connection with the SAF forwarder. The default setting is 5050. The port that you enter must match the port number that you configure on the SAF forwarder. The port range on the SAF forwarder is 1024 to 65535.
Enable TCP Keep Alive	Check the Enable TCP Keep Alive check box to ensure that Cisco Unified Communications Manager gets notified if the TCP connection between the SAF forwarder and Cisco Unified Communications Manager fails. If this check box is unchecked, the Cisco Unified Communications Manager does not get notified that the TCP connection fails until the SAF forwarder keepalive timer expires (configured on the SAF forwarder). Cisco recommends that this check box remains checked.
Show/Hide Advanced	
SAF Reconnect Interval	Enter the time (in seconds) that Cisco Unified Communications Manager allows to pass before it attempts to reconnect to the SAF forwarder after a connection failure. Enter a value between 0 and 500. The default value is 20.
SAF Notifications Window Size	Enter the number of outstanding Notify requests that the SAF forwarder can maintain at the same time to the Cisco Unified Communications Manager. The default value is 7. You can enter a number between 0 to 255. If you enter 0 in this field, the SAF forwarder does not send any notification to this Cisco Unified Communications Manager, but the Cisco Unified Communications Manager can still publish hosted DNs to the SAF network if the CCD advertising service is configured and active.

Field	Description
Available Cisco Unified Communications Managers	This setting works with the Selected Cisco Unified Communications Managers pane. Every node in the Available Cisco Unified Communications Managers pane can connect to the SAF forwarder that you configure in the SAF Forwarder Configuration window. If you want to do so, you can assign a particular node to this SAF forwarder so that the node prioritizes this SAF forwarder over other configured SAF forwarders. You assign the node to the SAF forwarder by moving the node to the Selected Cisco Unified Communications Managers pane. To move a node to or from the Available Cisco Unified Communications Managers pane, highlight the node and click the up or down arrow. If you have assigned a node to two SAF forwarders, the assigned node does not display in the pane because you can only assign a node to two SAF forwarders. For example, three SAF forwarders exist—forwarder1, forwarder2, and forwarder3. You assign node_2 to forwarder1 and forwarder3, which means that node_2 does not display in the Available Cisco Unified Communications Managers pane for forwarder2.
Selected Cisco Unified Communications Managers	Use this pane for cluster over WAN (COW) configurations. This pane displays the nodes that prioritize this SAF forwarder over other configured SAF forwarders. For example, if node_1 and node_2 display in this pane for forwarder1, then node_1 and node_2 always choose forwarder1 first, even though you may have configured other SAF forwarders. To move a node to or from the Selected Cisco Unified Communications Managers pane, highlight the node and click the up or down arrow below the Available Cisco Unified Communications Managers pane. To order the nodes in the pane, highlight the node and click the up or down arrow to the right of the pane.

Hosted DN Group Configuration

Configuration Path-**Call Routing** > **Call Control Discovery** > **Hosted DN Group**

Supported with the call control discovery feature, hosted DN groups are a collection of hosted DN patterns that you group together in Cisco Unified Communications Manager Administration. After you assign a hosted DN group to the CCD advertising service in Cisco Unified Communications Manager Administration, the

CCD advertising service advertises all the hosted DN patterns that are a part of the hosted DN group. You can assign only one hosted DN group per CCD Advertising Service.

For more information on the call control discovery feature, see the Call Control Discovery, on page 53.

Before You Begin

Before you configure the hosted DN groups, see the Configure Call Control Discovery, on page 53 and Install and Activate Call Control Discovery, on page 69.

Table 11: Hosted DN Group Configuration Settings

Field	Description
Name	Enter the name of the hosted DN group. Valid entries include alphanumeric characters, hyphen, period, underscore, and blank space. You can enter up to 50 characters. The value that you enter displays in the Find and List Hosted DN Group window, the Hosted DN Group Configuration window, the Hosted DN Pattern Configuration window, and the CCD Advertising Service Configuration window,
Description	Enter a description for the hosted DN group. You can enter all characters except for \, “, < >, &, and %. You can enter up to 128 characters.
PSTN Failover Strip Digits	Enter the number of digits that you want stripped from the hosted DN if the call fails over to the PSTN. You can enter a value between 0 and 16.
PSTN Failover Prepend Digits	Enter the international escape character, +, or digits (0-9) that you want to add to the beginning of the directory number if the call fails over to the PSTN. You can enter up to 16 characters. For example, enter an access or area code.
Use HostedDN as PSTN Failover	If you check this check box, Cisco Unified Communications Manager ignores the configuration that you entered in the PSTN Failover Strip Digits or PSTN Failover Prepend Digits. If you do not need to strip digits from or prepend digits to the hosted DN when the call fails over to the PSTN, check the Use Hosted DN as PSTN Failover check box. When you check the check box, the PSTN Failover Strip Digits or PSTN Failover Prepend Digits fields display as disabled. If you check the check box, the entity that makes the outbound call uses the original hosted DN range for PSTN failover.

Hosted DN Pattern Configuration

Configuration Path-**Call Routing** > **Call Control Discovery** > **Hosted DN Patterns**

Hosted DN Pattern Configuration window supports the call control discovery feature, which allows Cisco Unified Communications Manager to use the SAF network to learn information, such as directory number patterns, from other remote call-control entities that also advertise SAF.

Hosted DN patterns are directory number patterns that belong to Cisco Unified Communications Manager; the CCD advertising service advertises these patterns to other remote call-control entities that use the SAF network. You associate these patterns with Hosted DN groups, which allow you to easily associate multiple patterns to a CCD advertising service.

Table 12: Hosted DN Pattern Configuration Settings, on page 86 describes the configuration settings that display in the Hosted DN Pattern Configuration window; these same settings display in the .csv file where you can add or modify hosted DN patterns and then upload them into the Cisco Unified Communications Manager database.

Before You Begin

Before you configure the hosted DN patterns, see the Configure Call Control Discovery, on page 53 and Install and Activate Call Control Discovery, on page 69.

For more information on call control discovery, see the Call Control Discovery, on page 53.

Table 12: Hosted DN Pattern Configuration Settings

Field	Description
Hosted Pattern	Enter the value for the hosted DN pattern, which can contain a maximum of 50 characters. The value that you enter in this field gets advertised by the CCD advertising service to remote call-control entities. You can enter the international escape character + followed by pattern or dialable digits (0-9A-Da-d), pattern ([6-9]), wildcard character (X), or (^) with optional % or ! at the end of the entry.
Description	Enter a description for the hosted DN pattern. You can enter all characters except for \, “, < >, &, and %. You can enter up to 128 characters.

Field	Description
Hosted DN Group	Choose the Hosted DN group that you want to associate with this hosted DN pattern. If both of the following conditions are met, Cisco Unified Communications Manager applies the PSTN failover configuration for the hosted DN group to the hosted DN pattern: • In the Hosted DN Patterns window, you do not configure the PSTN Failover Strip Digits or PSTN Failover Prepend Digits fields (or you use the defaults). • In the Hosted DN Patterns window, you uncheck the Use HostedDN as PSTN Failover check box.
PSTN Failover Strip Digits	Enter the number of digits that you want to strip from the beginning of the directory number when an IP connection is not available and the call fails over to the PSTN. You can enter a value between 0 and 16. When all of the following conditions are met, the hosted DN group configuration applies: • When you enter 0 in this field (or leave it blank) • When you leave the PSTN Failover Prepend Digits field blank • When the Use Hosted DN as PSTN Failover check box is unchecked If the value that you enter in this field is longer than the hosted DN pattern, all digits in the pattern get stripped before any digits are prepended.
PSTN Failover Prepend Digits	Enter the international escape character, +, or the digits that you want to add to the beginning of the directory number if the call fails over to the PSTN. You can enter up to 16 characters. When all of the following conditions are met, the hosted DN group configuration applies: • When you enter 0 in this field (or leave it blank) • When you leave the PSTN Failover Strip Digits field blank • When the Use Hosted DN or PSTN Failover check box is unchecked

Field	Description
Use HostedDN as PSTN Failover	If you do not need to strip digits from or prepend digits to the hosted DN when the call fails over to the PSTN, check the Use Hosted DN as PSTN Failover check box. When you check the check box, the PSTN Failover Strip Digits or PSTN Failover Prepend Digits fields display as disabled. If you check the check box, the entity that makes the outbound call uses the original hosted DN range for PSTN failover. If you are modifying the .csv file for hosted DN patterns, enter TRUE, which indicates that you want to use the Hosted DN exactly as is during PSTN failover, or FALSE, which indicates that you plan to strip digits from and prepend digits to the directory number during PSTN failover.

Advertising Service Configuration

Configuration Path-**Call Routing** > **Call Control Discovery** > **Advertising Service**

The call control discovery advertising service, which supports the call control discovery feature, allows **Cisco Unified Communications Manager** to advertise the hosted DNs for the cluster and the PSTN failover configuration to remote call-control entities that use the SAF network. Advertising Service Configuration describes the CCD Advertising Service configurations settings.

Before You Begin

Before you configure the CCD advertising service, seeConfigure Call Control Discovery, on page 53 and Install and Activate Call Control Discovery, on page 69.

Table 13: CCD Advertising Service Configuration Settings

Field	Description
Name	Enter the name of the CCD advertising service. Valid entries include alphanumeric characters, hyphen, period, underscore, and blank space. You can enter up to 50 characters. You cannot name any CCD advertising service and the CCD requesting service the same name in Cisco Unified Communications Manager Administration, so ensure that the name is unique.
Description	Enter a description for the CCD advertising service. You can enter all characters except for \, “, < >, &, and %. You can enter up to 128 characters.

Field	Description
SAF SIP Trunk	Choose the SIP trunk that you want to use with this CCD advertising service. For inbound calls to the **Cisco Unified Communications Manager**, the call gets routed to the appropriate trunk that is advertised by the CCD advertising service. If a trunk does not display in the drop-down list box, you did not choose Call Control Discovery from the Trunk Service Type drop-down list box when you first configured the trunk.
SAF H323 Trunk	Choose the H.323 trunk that you want to use with the CCD advertising service. For inbound calls to the **Cisco Unified Communications Manager**, the call gets routed to the appropriate trunk that is advertised by the CCD advertising service. If a trunk does not display in the drop-down list box, verify that you checked the Enable SAF check box in the Trunk Configuration window for H.323 (non-gatekeeper controlled) trunks.
HostedDN Group	Choose the Hosted DN group that you want to associate with this CCD advertising service. The CCD advertising service advertises the hosted DN patterns that are a part of the hosted DN group. You can only assign the hosted DN group to one CCD advertising service, so only unassigned hosted DN groups display in this drop-down list box.
Activated Feature	Ensure the Activated Feature check box is checked. If the Activated Feature check box is not checked, the CCD advertising service does not work.

Partition Configuration for Call Control Discovery

Configuration Path-**Call Routing** > **Call Control Discovery** > **Partition**

The CCD requesting service, which supports the call control discovery feature, allows Cisco Unified Communications Manager to listen for hosted DN advertisements from remote call-control entities that use the SAF network. In addition, the CCD requesting service ensures that learned patterns get inserted into the digit analysis master routing table.

The partition under Call Routing > Call Control Discovery > Partition only supports the call control discovery feature; that is, all learned patterns automatically belong to the CCD partition that you assign to the CCD requesting service. The call control discovery partition ensures that the learned patterns get inserted into digit analysis under this partition for call control discovery.

Be aware that the CCD partition does not display under **Call Routing** > **Class of Control** > **Partition** in Cisco Unified Communications Manager Administration.

Before You Begin

Before you configure the CCD partition, see the Configure Call Control Discovery, on page 53 and Install and Activate Call Control Discovery, on page 69.

Next Steps

Assign the partition to the CCD requesting service.

The partition that you assign to the CCD requesting service must belong to a calling search space that the devices can use for calling the learned patterns, so assign the partition to the calling search space that you want the devices to use. If you do not assign a calling search space that contains the partition to the device, the device cannot call the learned patterns.

Table 14: Partition Configuration Settings for Call Control Discovery

Field	Description
Name	Enter the name of the partition that you plan to assign to the CCD requesting service. You can enter alphanumeric characters, underscore (_), hyphen (-), or space. You can enter up to 50 characters.
Description	Enter a description for the partition. You can enter all characters except for \, “, < >, &, and %. You can enter up to 128 characters.
Time Schedule	From the drop-down list box, choose a time schedule to associate with this CCD partition. The associated time schedule specifies when the partition is available to make outgoing calls to learned patterns for this cluster. The default value specifies None, which implies that time-of-day routing is not in effect and the partition remains active at all times. In combination with the Time Zone value in the following field, association of a partition with a time schedule configures the partition for time-of-day routing. The system checks outgoing calls to learned patterns under this partition against the specified time schedule.

Field	Description
Time Zone	Choose one of the following options to associate a CCD partition with a time zone: • Originating Device-If you choose this option, the system checks the partition against the associated time schedule with the time zone of the calling device. • Specific Time Zone-If you choose this option, choose a time zone from the drop-down list box. The system checks the partition against the associated time schedule at the time that is specified in this time zone. When an outgoing call to a CCD learned pattern occurs, the current time on the Cisco Unified Communications Manager gets converted into the specific time zone set when one option is chosen. The system validates this specific time against the value in the Time Schedule field.

Requesting Service Configuration

Configuration Path-**Call Routing** > **Call Control Discovery** > **Requesting Service**

The CCD requesting service, which supports the call control discovery feature, allows Cisco Unified Communications Manager to listen for advertisements from remote call-control entities that use the SAF network. In addition, the CCD requesting service ensures that learned patterns get inserted into the digit analysis.

In Cisco Unified Communications Manager Administration, you can configure only one call control discovery requesting service.

Before You Begin

Before you configure the CCD requesting service, see the Configure Call Control Discovery, on page 53 and Install and Activate Call Control Discovery, on page 69.

Table 15: CCD Requesting Service Configuration Settings

Field	Description
Name	Enter the name of the CCD requesting service. Valid entries include alphanumeric characters, hyphen, period, underscore, and blank space. You can enter up to 50 characters. You cannot name any CCD advertising service and the CCD requesting service the same name in Cisco Unified Communications Manager Administration, so ensure that the name is unique.

Field	Description
Description	Enter a description for the CCD requesting service. You can enter all characters except for \, “, < >, &, and %. You can enter up to 128 characters.
Route Partition	From the drop-down list box, choose the partition where you want the learned patterns to belong. The Route Partition field only supports the call control discovery feature; that is, all learned patterns automatically belong to the partition that you choose. This route partition gets used exclusively by the CCD requesting service to ensure that all learned patterns get placed in digit analysis under the route partition. If you choose a partition besides None from the drop-down list box, the partition that you choose must belong to a calling search space that the devices can use for calling the learned patterns. In this case, if you do not assign a calling search space that contains the partition to the device, the device cannot call the learned patterns. **Tip** Cisco strongly recommends that you configure a unique partition and assign it to the CCD requesting service. If you choose None from the Route Partition drop-down list box, all devices can call the learned patterns. **Tip** Updating the Learned Pattern Prefix field or Route Partition field may impact system performance because the digit-analysis master routing table automatically gets updated when these fields are changed. To avoid system performance issues, Cisco recommends that you update these fields during off-peak hours.

Field	Description
Learned Pattern Prefix	The learned pattern prefix gets applied to the hosted DN pattern before the CCD requesting service registers with digit analysis. For outgoing calls to learned patterns, the learned pattern prefix gets stripped. Enter the prefix that you want to apply to the hosted DN pattern before the hosted DN pattern registers with digit analysis. To make calls to the learned patterns, the phone user must dial the prefix followed by the learned pattern. You can enter numbers, *, #, or +. You can enter up to 24 characters. **Tip** Updating the Learned Pattern Prefix field or Route Partition field may impact system performance because the digit-analysis master routing table automatically gets updated when these fields are changed. To avoid system performance issues, Cisco recommends that you update these fields during off-peak hours.
PSTN Prefix	Enter the digits that will get prepended to the learned patterns when PSTN failover occurs. You can enter numbers, *, #, or +. You can enter up to 24 characters. When calls to learned patterns fail over to the PSTN, the PSTN prefix gets added to the learned pattern after the PSTN failover settings that are advertised by the remote call-control entity for that learned pattern get applied.
Available SAF Trunks	A list of SAF-enabled trunks that are not assigned to the CCD requesting service display in the Available SAF Trunks pane. To assign the trunk to the CCD requesting service, highlight the service and click the down arrow to move the trunk to the Selected SAF Trunks pane.

Field	Description
Selected SAF Trunks	Cisco Unified Communications Manager routes outbound calls over SAF-enabled SIP or H.323 intercluster (non-gatekeeper controlled) trunks to remote call-control entities that use the SAF network; that is, the SAF-enabled trunks that you assign to the CCD requesting service manage outgoing calls to the learned DN patterns. A list of SAF-enabled trunks that are assigned to the CCD requesting service display in the Selected SAF Trunks pane. You can assign as many SAF-enabled trunks as you want. Outbound calls get managed in a round-robin fashion; that is, if the learned pattern supports both SIP and H.323 protocol, then outbound calls alternate between the trunk types. To unassign the trunk from the CCD requesting service, highlight the service and click the up arrow to move the trunk to the Available SAF Trunks pane. To order the trunks in the pane, highlight the trunk and click the up and down arrows to the right of the pane. **Tip** At least one SAF-enabled trunk must exist in the Selected SAF Trunks pane; otherwise, the CCD requesting service does not get started for the local cluster, and patterns do not get learned.
Activated Feature	Ensure the Activated Feature check box is checked. If the Activated Feature check box is not checked, the CCD requesting service does not work.

Blocked Learned Pattern Configuration

Configuration Path-**Call Routing** > **Call Control Discovery** > **Blocked Learned Patterns**

The Blocked Learned Pattern Configuration window supports the call control discovery feature by allowing you to purge and block learned patterns, for example, learned patterns that you no longer want to use.

If you want to do so, you can purge learned patterns that you no longer want to use, and you can block the learned patterns so that Cisco Unified Communications Manager ignores the patterns when they are advertised by remote call-control entities. For example, if you want to block a learned pattern with prefix 235 from remote call-control entity, xyz with IP address of 111.11.11.11, you can block the pattern specifically for this call-control entity by entering the relevant information in the Block Learned Patterns window; in this example, after you save the configuration, the CCD requesting service searches the local cache and purges the learned patterns with 235 prefix from remote call-control entity xyz with IP address of 111.11.11.11. Any subsequent notifications with this information gets blocked and ignored by Cisco Unified Communications Manager. Be aware that blocking and purging of patterns is based on exact match; for example, configuring 235XX blocks 235XX, not any subsets of that pattern. Be aware that if you do not specify a remote call-control entity and

IP address for the entity, Cisco Unified Communications Manager purges and blocks the pattern for all remote call-control entities that use it.

Tip You can view purged and blocked learned patterns in the Find and List Blocked Learned Patterns window in Cisco Unified Communications Manager Administration. These purged or blocked patterns do not display in RTMT. If you delete a blocked pattern from Cisco Unified Communications Manager Administration, Cisco Unified Communications Manager can relearn those patterns if they are still available in the SAF network and if the maximum number of learned patterns has not been reached for the cluster. For a pattern to be relearned by Cisco Unified Communications Manager, you must delete the entire record for the blocked learned pattern from Cisco Unified Communications Manager Administration; that is, Cisco Unified Communications Manager does not relearn a pattern when you only delete part of the blocked learned pattern configuration; for example, if you only delete the Remote Call Control Identity or Remote IP configuration for the record.

Tip For Cisco Unified Communications Manager to block or purge a pattern, the learned pattern must match all data that you configure in the Blocked Learned Patterns window.

This table describes the blocked learned patterns configuration settings that display in the Blocked Learned Pattern Configuration window.

Table 16: Blocked Learned Pattern Configuration Settings

Field	Description
Learned Pattern	**Tip** If you want Cisco Unified Communications Manager to block all patterns based on a prefix that gets prepended to the directory number, do not configure this field; instead, configure the Learned Pattern Prefix field. **Tip** If you want to block all learned patterns from a particular remote call-control entity, do not configure this field; instead, configure the Remote Call Control Identity field or the Remote IP field. For this field, enter the exact learned pattern that you want to block. Cisco Unified Communications Manager blocks a pattern based on exact match, so you must enter the exact pattern that you want Cisco Unified Communications Manager to block. For example, if you enter 235XX, Cisco Unified Communications Manager blocks 235XX patterns.

Field	Description
Learned Pattern Prefix	**Tip** If you configured the Learned Pattern field, do not configure the Learned Pattern Prefix field. If you want to block a learned pattern based on the prefix that is prepended to the pattern, enter the prefix in this field. For example, if you want to block learned patterns that use +1, enter +1 in this field. If you configure the Remote Call Control Identity or Remote IP fields, Cisco Unified Communications Manager blocks the learned patterns that use the particular prefix from the remote call-control entity that you configure (not from all remote call-control entities that advertise patterns with the prefix). If you do not enter a remote call-control entity or remote IP address, then all patterns that use the prefix get blocked.
Remote Call Control Identity	Enter the name of the remote call-control entity that advertises the pattern that you want to block. For example, you may enter the name of a cluster or a site. If you leave this field and the Remote IP field blank, Cisco Unified Communications Manager blocks the learned pattern for all remote call-control entities that advertise the pattern.
Remote IP	Enter the IP address for the remote call-control entity where you want to block the learned pattern. If you want to block a particular learned pattern from all remote call-control entities, you do not need to configure this field. Configure this field when you want to block a particular learned pattern from a specific remote call-control entity.

Configuration Records for Call Control Discovery

The call control discovery feature leverages the Service Advertisement Framework (SAF) network service, a proprietary Cisco service, to facilitate dynamic provisioning of inter-call agent information. By adopting the SAF network service, the call control discovery feature allows Cisco Unified Communications Manager to advertise itself along with other key attributes, such as directory number patterns that are configured in Cisco Unified Communications Manager Administration, so other call control entities that also use SAF network server can use the advertised information to dynamically configure and adapt their routing behaviors; likewise, all entities that use SAF advertise the directory number patterns that they own along with other key information, so other remote call-control entities can learn the information and adapt the routing behavior of the call.

After you configure call control discovery, you can search for the configuration records in the related Find and List windows in Cisco Unified Communications Manager Administration. The Find and List windows allow you to search for records based on specific criteria.

Note During your work in a browser session, Cisco Unified Communications Manager Administration retains your search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your search preferences until you modify your search or close the browser.

Procedure

Step 1 To locate one of the Find and List windows for the call control discovery feature in Cisco Unified Communications Manager Administration, perform one of the following tasks:

a) Choose **Advanced Features** > **SAF** > **SAF Security Profile**.
b) Choose **Advanced Features** > **SAF** > **SAF Forwarder**.
c) Choose **Call Routing** > **Call Control Discovery** > **Hosted DN Group**.
d) Choose **Call Routing** > **Call Control Discovery** > **Hosted DN Patterns**.
e) Choose **Call Routing** > **Call Control Discovery** > **Advertising Service**.
f) Choose **Call Routing** > **Call Control Discovery** > **Partition**.
g) Choose **Call Routing** > **Call Control Discovery** > **Blocked Learned Pattern**.

Tip No Find and List window displays for the CCD requesting service because you can configure only one CCD requesting service in Cisco Unified Communications Manager Administration. When you choose **Call Routing** > **Call Control Discovery** > **Requesting Service**, the record, if configured, displays.

Tip In the Find and List window for Hosted DN Patterns, you can download a .cvs file so that you can add or update multiple hosted DN patterns for the call control discovery feature at the same time. To download a .csv file, click Download in the window. To upload a modified .csv file in the Find and List window for Hosted DN Patterns, click Upload File; browse to the file that you want to upload, check the Replace Existing Patterns check box if you want to overwrite the existing patterns, and then click **Upload File**.

Tip The Find and List Hosted DN Patterns window allows you to identify which hosted DN patterns belong to a Hosted DN group. For more information, see the Identify Hosted DN Patterns in a Hosted DN Group, on page 100.

The Find and List window displays. Records from an active (prior) query may also display in the window.

Step 2 To find all records in the database, ensure the dialog box is empty.

To filter or search records

a) From the first drop-down list box, select a search parameter.
b) From the second drop-down list box, select a search pattern.
c) Specify the appropriate search text, if applicable.

Note To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

Note If you search by the search parameter, Activated Feature, in the Find and List CCD Advertising Service window, you must enter t or f to indicate true or false if you specify search text. Do not enter true or false when you specify the search text.

Step 3 Click **Find**.

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

Note You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking Delete Selected. You can delete all configured records for this selection by clicking **Select All** and then clicking **Delete Selected**.

Step 4 From the list of records that display, click the link for the record that you want to view.

Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Configure Call Control Discovery

The call control discovery feature leverages the Service Advertisement Framework (SAF) network service, a proprietary Cisco service, to facilitate dynamic provisioning of inter-call agent information. By adopting the SAF network service, the call control discovery feature allows Cisco Unified Communications Manager to advertise itself along with other key attributes, such as directory number patterns that are configured in Cisco Unified Communications Manager Administration, so other call control entities that also use SAF network server can use the advertised information to dynamically configure and adapt their routing behaviors; likewise, all entities that use SAF advertise the directory number patterns that they own along with other key information, so other remote call-control entities can learn the information and adapt the routing behavior of the call.

This section describes how to add, copy, or update configuration for call control discovery in the Cisco Unified Communications Manager database. For call control discovery, you configure a SAF security profile, SAF forwarders, hosted DN groups and patterns, CCD advertising services, and the CCD requesting service. Before you configure call control discovery, see the Configure Call Control Discovery, on page 53.

Tip This section does not describe how to enable trunks for SAF. For information on how to enable a trunk for SAF, see the Hosted DN Group Configuration, on page 84.

Tip To identify which hosted DN patterns belong to a hosted DN group, see the Identify Hosted DN Patterns in a Hosted DN Group, on page 100.

Tip This section does not display how to access the CCD Feature Configuration window, which displays feature parameters for call control discovery. For more information on feature parameters, see the Call Control Discovery Feature Parameters, on page 75.

Procedure

Step 1 Perform one of the following tasks:

a) If you are configuring the CCD requesting service, choose **Call Routing** > **Call Control Discovery** > **Requesting Service**. The CCD Requesting Service Configuration window displays; go to Step 2, on page 99.
b) Choose **Advanced Features** > **SAF** > **SAF Security Profile**.
c) Choose **Advanced Features** > **SAF** > **SAF Forwarder**.
d) Choose **Call Routing** > **Call Control Discovery** > **Hosted DN Group**.
e) Choose **Call Routing** > **Call Control Discovery** > **Hosted DN Patterns**.
f) Choose **Call Routing** > **Call Control Discovery** > **Advertising Service**.
g) Choose **Call Routing** > **Call Control Discovery** > **Blocked Learned Pattern**.

The Find and List window displays for the SAF Security Profile, SAF Forwarder, Hosted DN Group, Hosted DN Patterns, Partition, and CCD Advertising Service windows.

Step 2 From the Find and List window, perform one of the following tasks:

a) To copy an existing record related to call control discovery, locate the record as described in the SAF Security Profile Configuration, on page 79, click the Copy button next to the record that you want to copy, and continue with Step 3, on page 99.
b) To add a new record related to call control discovery, click the Add New button and continue with Step 3, on page 99.
c) To update an existing record, locate the appropriate record as described in the SAF Security Profile Configuration, on page 79 and continue with Step 3, on page 99.
d) In the Find and List window for Hosted DN Patterns, you can download a .cvs file so that you can add or update multiple patterns for the call control discovery feature at the same time. To download a .csv file, click Download in the window.

Step 3 Configure the appropriate fields as described in the following sections:

a) SAF Security Profile Configuration, on page 79
b) SAF Forwarder Configuration, on page 81
c) Hosted DN Group Configuration, on page 84
d) Hosted DN Pattern Configuration, on page 86
e) Partition Configuration for Call Control Discovery, on page 89
f) Advertising Service Configuration, on page 88
g) Requesting Service Configuration, on page 91
h) Blocked Learned Pattern Configuration, on page 94

Step 4 To upload a modified .csv file in the Find and List window for Hosted DN Patterns, click Upload File; browse to the file that you want to upload, check the Replace Existing Patterns check box if you want to overwrite the existing patterns, and then click **Upload File**.

Step 5 To save the configuration information to the database, click **Save.**

Tip The Reset button in the CCD Advertising Service Configuration window triggers the call control discovery advertising service to withdraw existing publishing requests and to publish all the related information again. The Reset button in the CCD Requesting Service Configuration window triggers the requesting service to remove the learned patterns from the local cache, resubscribe to the SAF network, and to learn patterns again. To ensure that your network is not impacted, Cisco recommends that you click the Reset button during off-peak hours.

Configure a SAF-Enabled Trunk

You can configure a SIP or H.323 (non-gatekeeper controlled) trunk so that it supports SAF. For SIP trunks, you choose Call Control Discovery from the Trunk Service Type drop-down list box, which displays in the same window where you assign the trunk type and trunk protocol. Be aware that you cannot change the trunk service type after you choose it from the drop-down list box.

For H.323 (non-gatekeeper controlled) trunks, you check the Enable SAF check box in the Trunk Configuration window when you configure the trunk (after you choose the trunk type and trunk protocol). If you want to disable SAF on the H.323 trunk after you enable it, uncheck the Enable SAF check box.

For trunk configuration considerations, see the Install and Activate Call Control Discovery, on page 69.

Identify Hosted DN Patterns in a Hosted DN Group

The Find and List Hosted DN Patterns window allows you to identify which hosted DN patterns belong to a Hosted DN group. In the Find and List Hosted DN Patterns window, you can perform one of the following tasks:

- You can search for all hosted DN patterns, which displays the hosted DN group in the Hosted DN Group when the results display. (The GUI groups the hosted DN groups together in the results.)
- You can search specifically for a particular hosted DN group by choosing Hosted DN Group from the Find drop-down list box and then entering a hosted DN group in the search criteria.

Delete Configuration Records for Call Control Discovery

This section describes how to delete a configured call control discovery record in Cisco Unified Communications Manager Administration.

Before you begin

If you delete a blocked pattern from Cisco Unified Communications Manager Administration, Cisco Unified Communications Manager can relearn those patterns if they are still available in the SAF network (and if the maximum number of learned patterns has not been reached for the cluster).

When you delete a CCD advertising service, all hosted DN patterns that are advertised with each assigned trunk get unpublished.

When you delete the CCD requesting service, all learned patterns get unregistered from the local cache and digit analysis.

Note You can delete multiple records from the Find and List window by checking the check boxes next to the appropriate records and clicking Delete Selected. You can delete all records in the window by clicking Select All and then clicking Delete Selected.

Procedure

Step 1 If you want to delete the record from the Find and List window, perform the following tasks:

a) Find the record that you want to delete.
b) Click the record that you want to delete.
c) Click **Delete Selected**.

You receive a message that asks you to confirm the deletion.

d) Click **OK.**

The window refreshes, and the record gets deleted from the database.

Step 2 If you want to delete the record from the configuration window, perform the following tasks:

a) Find the record that you want to delete.
b) Access the configuration window; click **Delete** in the configuration window.

You receive a message that asks you to confirm the deletion.

c) Click **OK.**

The window refreshes, and the record gets deleted from the database.

Related Topics

Configuration Records for Call Control Discovery, on page 96

Provide Information to Users

The call control discovery feature does not impact end users; for example, it does not impact phone users.

Troubleshooting Call Control Discovery

For information on troubleshooting call control discovery, see the Troubleshooting Guide for Cisco Unified Communications Manager.

CHAPTER 5

Call Display Restrictions

This chapter provides information about the Call Display Restrictions feature which allows you to choose the information that will display for calling and/or connected lines, depending on the parties who are involved in the call. By using specific configuration settings in Cisco Unified Communications Manager Administration, you can choose to present or restrict the display information for each call.

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 would not want the call information to display on either phone. The Call Display Restrictions feature enables this functionality.

Configure Call Display Restrictions

The Call Display Restrictions feature allows you to choose the information that will display for calling and/or connected lines, depending on the parties who are involved in the call. By using specific configuration settings in Cisco Unified Communications Manager Administration, you can choose to present or restrict the display information for each call.

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 would not want the call information to display on either phone. The Call Display Restrictions feature enables this functionality.

Perform the following steps to configure Call Display Restrictions.

Procedure

Step 1 Configure partitions for rooms, front desk, club, and the PSTN.

For more information, see topics related to partitions and the *Cisco Unified Communications Manager Administration Guide*.

Step 2 Configure call park directory numbers or define a range of call park directory numbers. Configure translation patterns for each call park directory number for call park retrieval from rooms.

For more information, see topics related to Call Park and the *Cisco Unified Communications Manager Administration Guide*

Step 3 Configure a partition for call park directory numbers to make the partition available only to users who have the partition in their calling search space.

For more information, see topics related to partitions and Call Park, as well as the *Cisco Unified Communications Manager Administration Guide*.

Step 4 Configure calling search spaces for rooms, front desk, club, the PSTN, and room park range (for Call Park).

For more information, see topics related to calling search spaces and the *Cisco Unified Communications Manager Administration Guide*.

Step 5 Configure the phones for the rooms, front desk, club, and the gateway for the PSTN.

For more information, see topics related to devices and gateways, as well as the *Cisco Unified Communications Manager Administration Guide*.

Step 6 Configure translation patterns and route patterns.

For more information, see topics related to translation patterns, as well as the *Cisco Unified Communications Manager Administration Guide* and the *Cisco Unified Communications Manager System Guide*.

Related Topics

Call Display Restrictions, on page 103
Call Display Restrictions Feature, on page 104
Call Park, on page 115
Calling Search Spaces, on page 111
Devices and Gateways, on page 112
Partitions, on page 111
Translation Patterns, on page 112

Call Display Restrictions Feature

The Call Display Restrictions feature works within a Cisco Unified Communications Manager cluster that is running Cisco Unified Communications Manager 5.0 or a later version or a Cisco Unified Communications Manager server that is running Cisco Unified Communications Manager 6.0 or a later version. To enable Call Display Restrictions, you must configure the following parameters:

Service Parameter:

- Always Display Original Dialed Number

  Translation Pattern Parameters

- Name Display for Original Dialed Number When Translated
- Calling Line ID Presentation
- Connected Line ID Presentation

  Phone Configuration/User Device Profile Parameter:

- Ignore Presentation Indicators (internal calls only)

The combination of these settings allows you to determine whether the display information for each call is allowed or restricted and how to display the connected number.

Overview of Call Display Restrictions

Call Display Restrictions allow you to selectively display or restrict calling and/or connected line display information. A hotel environment, which might have the following needs, frequently requires this functionality:

- For calls between a guest room and the front desk, both the room and the front desk should see the call information display of each other.
- For calls between guest rooms, the rooms should not see the call information display of each other.
- For calls between guest rooms and other hotel extensions (such as the club house), only the rooms should see the call information display.
- For external calls from the public switched telephone network (PSTN) to the front desk or guest rooms, the call information of the caller should not display if the display settings are restricted.
- For all calls to the front desk, the call information of internal calls should display.
- When the front desk transfers a call from a guest room to security, the room phone shows only the dialed number for the front desk.

Call Display Restrictions Enablement

The basis for the functionality of the Call Display Restrictions feature is calls being routed through different translation patterns before the calls are extended to the actual device. Users then dial the appropriate translation pattern numbers to achieve the display restrictions.

Translation Pattern Configuration

To enable Call Display Restrictions, configure translation patterns with different levels of display restrictions by choosing the appropriate option for the calling line ID presentation and the connected line ID presentation parameters.

Tip You must configure partitions and calling search spaces, along with translation patterns. For more information about these configurations, see topics related to translation pattern configuration and the *Cisco Unified Communications Manager Administration Guide*.

Phone Configuration/User Device Profile Configuration

Next, enable the “Ignore Presentation Indicators (internal calls only)” parameter to ignore any presentation restriction that is received for internal calls and to ensure that the device will display the call information of the remote party.

For users who log in to phones that are enabled for Extension Mobility, configure this setting from the Cisco Unified Communications Manager Administration Device Profile Configuration window as well.

Connected Number Display

When a call routes through a translation or route pattern, routes to a Call Forward All or Call Forward Busy destination, or gets redirected through a call transfer or CTI application, the connected number display updates to show the modified number or redirected number.

To turn off phone display updates so that the phone displays only the dialed digits, set the Cisco CallManager service parameter "Always Display Original Dialed Number" to true. When this service parameter specifies true, the originating phone displays only the dialed digits for the duration of the call.

You can choose if the name for the original dialed number or the number after translation is displayed using the Cisco CallManager service parameter called "Name Display for Original Dialed Number When Translated". The default setting displays the name for the original dialed number before translation. This parameter is not applicable if the "Always Display Original Dialed Number" service parameter is set to false.

Related Topics

Configure the Phone, on page 110
Configure Translation Pattern Parameters, on page 109
Extension Mobility, on page 108

System Requirements for Call Display Restrictions

The following software components support Call Display Restrictions:

- Cisco Unified Communications Manager

The following devices support Call Display Restrictions:

- Cisco Unified IP Phone 6900 Series (except 6901 and 6911)
- Cisco Unified IP Phone 7900 Series
- Cisco Unified IP Phone 8900 Series
- Cisco Unified IP Phone 9900 Series
- H.323 clients
- CTI ports
- Cisco IP Communicator

Call Display Restrictions Examples

The following scenarios provide examples for using Call Display Restrictions:

- Front Desk calls Room-1 - Both phones display the call information of each other.
- Front Desk calls Room-1, and Front Desk transfers the call to Room-2 - The final connected parties, Room-1 and Room-2, cannot see the call information display of each other.
- External (PSTN) calls the Front Desk - The Front Desk honors the display settings of the external caller.

- External (PSTN) calls Room-1 - Room-1 honors the presentation of the external caller; the external caller cannot see the call information display of Room-1.
- Room-1 calls Front Desk - Both phones display the call information of each other.
- Room-1 calls Room-2 - Neither phone can see the call information display of the other.
- Room-1 calls Front Desk, and Front Desk transfers the call to Room-2 - The final connected parties, Room-1 and Room-2, cannot see the call information display of each other.
- Room-1 calls Front Desk-1, and Front Desk-1 transfers the call to Front Desk-2 - The final connected parties, Room-1 and Front Desk-2, can see the call information display of each other.
- Room-1 calls Room-2, and Room-2 transfers the call to Front Desk - Room-1 and Front Desk see the call information display of each other.
- Club House calls Room-1 - Club House cannot display the call information; Room-1 can see the call information display.
- All parties in a conference call - All phones see "To Conference" for the call information display.
- Room-1 calls Club House, and Club House manager has all calls forwarded to his mobile - Room-1 sees the Club House number only.

Interactions

This section describes how the Call Display Restrictions feature interacts with Cisco Unified Communications Manager applications and call processing features.

The connected number display restriction applies to all calls that originate in the system. When set to true, this setting interacts transparently with existing Cisco Unified Communications Manager applications, features, and call processing. The setting applies to all calls that terminate inside or outside the system.

Call Park

When the Call Display Restrictions feature is used 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 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 settings 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 the Call Park and Directed Call Park, on page 119 for additional information about using the Call Park feature.

Conference List

When you use Call Display Restrictions, you restrict the display information for the list of participants in a conference. For more information about conference lists, see the Cisco Unified Communications Manager System Guide.

Conference and Voice Mail

When Call Display Restrictions are used 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. That is, 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).

Configure Call Display Restrictions

To use Call Display Restrictions, make sure that you perform the following Cisco Unified Communications Manager configurations:

- Configure partitions and calling search spaces before you add a translation pattern.
- Configure translation patterns with different levels of display restrictions.
- From the Phone Configuration window, check the “Ignore Presentation Restriction (internal calls only)” check box to ensure that the call information display for internal calls is always visible.
- Configure individual, associated translation patterns for each individual Call Park directory number, to work with the Call Park feature.
- Set the “Always Display Original Dial Number” service parameter to True to ensure privacy and to block connected number updates for redirected calls.

Tip Before you configure call display restrictions, review the task to configure Call Display restrictions.

Related Topics

Configure Call Display Restrictions, on page 103

Configure Translation Pattern Parameters

Configure the following parameters from the Cisco Unified Communications Manager Administration Translation Pattern Configuration window.

Tip For outgoing calls, the translation pattern setting at the terminating end can override the originating Cisco Unified Communications Manager settings.

Calling Line ID Presentation

Cisco Unified Communications Manager uses calling line ID presentation as a supplementary service to allow or restrict the originating caller phone number on a call-by-call basis. Choose one of the following options to allow or restrict the display of the calling party phone number on the called party phone display for this translation pattern:

- Default - This option does not change the calling line ID presentation.
- Allowed - Cisco Unified Communications Manager allows the display of the calling number.
- Restricted - Cisco Unified Communications Manager blocks the display of the calling number.

Note If the incoming call goes through a translation pattern or route pattern and the calling line ID presentation setting is allowed or restricted, the system modifies the calling line presentation with the translation or route pattern setting.

Connected Line ID Presentation

Cisco Unified Communications Manager uses connected line ID presentation as a supplementary service to allow or restrict the called party phone number on a per-call basis. Choose one of the following options to allow or restrict the display of the connected party phone number on the calling party phone display for this translation pattern:

- Default - This option does not change the connected line ID presentation.
- Allowed - This option displays the connected party phone number.
- Restricted - Cisco Unified Communications Manager blocks the display of the connected party phone number.

Note If the incoming call goes through a translation or route pattern and the connected line ID presentation field is set to allowed or restricted, the system modifies the connected line presentation indicator with the translation or route pattern setting.

Note If the connected number display restriction is enabled, the connected number display does not update for modified numbers or redirected calls.

Examples

- For calls that are made from one guest room to another, configure the calling line ID presentation and the connected line ID presentation to restricted to ensure that the call information does not display.
- For calls that are made from the front desk to a guest room, configure the calling line ID presentation to allowed and the connected line ID presentation to restricted to ensure both parties can see the call information.

Tip For more information about calling party transformations and connected party transformations, see the Configure Call Display Restrictions, on page 103 chapter in the Cisco Unified Communications Manager System Guide.

Configure the Phone

To complete the configuration of the Call Display Restrictions feature, check the “Ignore Presentation Indicators (internal calls only)” check box from the Cisco Unified Communications Manager Administration Phone Configuration window.

For use with Extension Mobility, also configure this setting from the Cisco Unified Communications Manager Administration Device Profile Configuration window.

When you set the “Ignore Presentation Indicators (internal calls only)” field,

- Cisco Unified Communications Manager always displays the remote party call information if the other party is internal.
- Cisco Unified Communications Manager does not display the remote party call information if the other party is external and the display presentation is restricted.

Note Ensure the calling line ID presentation and the connected line ID presentation are configured with the “Ignore Presentation Indicators (internal calls only)” parameter for Cisco Unified Communications Manager to ignore the presentation settings of internal callers. For incoming external calls, the system maintains the received presentation indicators even if the “Ignore Presentation Indicators (internal calls only)” parameter is set.

- For phones that are used at the hotel front desk, check the “Ignore Presentation Indicators (internal calls only)” check box, so the front desk can always see the call information display for internal calls.

Tip For information about phone configurations and device profile configurations, see the Cisco Unified Communications Manager Administration Guide.

Call Display Restrictions Configuration Examples

This section provides sample configurations to enable the Call Display Restrictions feature.

Partitions

From the Cisco Unified Communications Manager Administration Partition Configuration window, configure the following partitions:

- Insert a real partition P_Room
- Insert a real partition P_FrontDesk
- Insert a real partition P_Club
- Insert a real partition P_PSTN
- Insert a translation partition P_CallsFromRoomToRoom
- Insert a translation partition P_CallsFromRoomToFrontDesk
- Insert a translation partition P_CallsFromRoomToClub
- Insert a translation partition P_CallsFromRoomToPSTN
- Insert a translation partition P_CallsFromFrontDeskToRoom
- Insert a translation partition P_CallsFromFrontDeskToFrontDesk
- Insert a translation partition P_CallsFromFrontDeskToClub
- Insert a translation partition P_CallsFromFrontDeskToPSTN
- Insert a translation partition P_CallsFromPSTN
- Insert a translation partition P_CallsFromClubToRoom
- Insert a translation partition P_CallsFromClubToFrontDesk
- Insert a translation partition P_FrontDeskToParkNumber
- Insert a translation partition P_RoomToParkNumber
- Insert a translation partition P_ParkNumberRange

Calling Search Spaces

From the Cisco Unified Communications Manager Administration Calling Search Space Configuration window, configure the following calling search spaces:

- Insert a calling search space CSS_Room {P_Room}
- Insert a calling search space CSS_FrontDesk {P_FrontDesk}
- Insert a calling search space CSS_Club {P_Club}
- Insert a calling search space CSS_PSTN {P_PSTN}
- Insert a calling search space CSS_FromRoom

- { P_CallsFromRoomToFrontDesk, P_CallsFromRoomToRoom, P_CallsFromRoomToClub, P_CallsFromRoomToPSTN, P_RoomToParkNumber, P_ParkNumberRange}
- Insert a calling search space CSS_FromFrontDesk
- { P_CallsFromFrontDeskToRoom, P_CallsFromFrontDeskToClub, P_CallsFromFrontDeskToPSTN, P_CallsFromFrontDeskToFrontDesk }
- Insert a calling search space CSS_FromPSTN
- { P_CallsFromPSTN}
- Insert a calling search space CSS_FromClub
- { P_CallsFromClubToRoom, P_CallsFromClubToFrontDesk}
- Insert a calling search space CSS_ RoomParkRange
- {P_ParkNumberRange }

Devices and Gateways

From the Cisco Unified Communications Manager Administration Phone Configuration window and from the Cisco Unified Communications Manager Administration Gateway Configuration window, configure the following phones and configure the following gateway:

- 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 PSTN Gateway E with route pattern P_PSTN and calling search space CSS_FromPSTN
- {CSS_FromPSTN}, RoutePattern {P_PSTN}

Translation Patterns

From the Cisco Unified Communications Manager Administration Translation Pattern Configuration window, configure the following translation patterns:

- Insert a translation pattern TP1 as 1XX

- Partition: P_CallsFromRoomToFrontDesk
- CSS: CSS_FrontDesk
- Calling Line ID Presentation and Calling Name Presentation: Restricted
- Connected Line ID Presentation and Connected Name Presentation: Allowed
- {P_CallsFromRoomToFrontDesk, CSS_FrontDesk, Calling Line/Name - Restricted, Connected Line/Name - Allowed}
- Insert a translation pattern TP2 as 2XX
- Partition: P_CallsFromRoomToRoom
- CSS: CSS_Room
- Calling Line ID Presentation and Calling Name Presentation: Restricted
- Connected Line ID Presentation and Connected Name Presentation: Restricted
- {P_CallsFromRoomToRoom, CSS_Room, Calling Line/Name - Restricted, Connected Line/Name - Restricted}
- Insert a translation pattern TP3 as 3XX
- Partition: P_CallsFromRoomToClub
- CSS: CSS_Club
- Calling Line ID Presentation and Calling Name Presentation: Restricted
- Connected Line ID Presentation and Connected Name Presentation: Allowed
- {P_CallsFromRoomToClub, CSS_Club, Calling Line/Name - Restricted, Connected Line/Name - Allowed}
- Insert a translation pattern TP4 as 9XXXX with called party transform mask as XXX
- Partition: P_CallsFromRoomToPSTN
- CSS: CSS_PSTN
- Calling Line ID Presentation and Calling Name Presentation: Restricted
- Connected Line ID Presentation and Connected Name Presentation: Default
- {P_CallsFromRoomToPSTN, CSS_PSTN, Calling Line/Name - Restricted, Connected Line/Name - Default}
- Insert a route pattern RP5 as 9.XXXXXX with discard digits as predot
- (DDI : PreDot)
- Partition: P_CallsFromRoomToPSTN
- CSS: CSS_PSTN
- Calling Line ID Presentation and Calling Name Presentation: Restricted
- Connected Line ID Presentation and Connected Name Presentation: Default

- {P_CallsFromRoomToPSTN, CSS_PSTN, Calling Line/Name - Restricted, Connected Line/Name - Default}
- Insert a translation pattern TP6 as 2XX
- Partition: P_CallsFromFrontDeskToRoom
- CSS: CSS_Room
- Calling Line ID Presentation and Calling Name Presentation: Allowed
- Connected Line ID Presentation and Connected Name Presentation: Restricted
- {P_CallsFromFrontDeskToRoom, CSS_Room, Calling Line/Name - Allowed, Connected Line/Name - Restricted}
- Insert a translation pattern TP7 as 1XX
- Partition: P_CallsFromFrontDeskToFrontDesk
- CSS: CSS_FrontDesk
- Calling Line ID Presentation and Calling Name Presentation: Allowed
- Connected Line ID Presentation and Connected Name Presentation: Allowed
- {P_CallsFromFrontDeskToFrontDesk, CSS_FrontDesk, Calling Line/Name - Allowed, Connected Line/Name - Allowed}
- Insert a translation pattern TP8 as 3XX
- Partition: P_CallsFromFrontDeskToClub
- CSS: CSS_Club
- Calling Line ID Presentation and Calling Name Presentation: Allowed
- Connected Line ID Presentation and Connected Name Presentation: Allowed
- {P_CallsFromFrontDeskToClub, CSS_Club, Calling Line/Name - Allowed, Connected Line/Name - Allowed}
- Insert a translation pattern TP9 as 9XXXX
- Partition: P_CallsFromFrontDeskToPSTN
- CSS: CSS_PSTN
- Calling Line ID Presentation and Calling Name Presentation: Allowed
- Connected Line ID Presentation and Connected Name Presentation: Default
- {P_CallsFromFrontDeskToPSTN, CSS_PSTN, Calling Line/Name - Allowed, Connected Line/Name - Default}
- Insert a route pattern RP10 as 9.XXXX with discard digits as predot
- Partition: P_CallsFromFrontDeskToPSTN
- CSS: CSS_PSTN
- Calling Line ID Presentation and Calling Name Presentation: Restricted

- Connected Line ID Presentation and Connected Name Presentation: Default
- {P_CallsFromFrontDeskToPSTN, CSS_PSTN, Calling Line/Name - Restricted, Connected Line/Name - Default}
- Insert a translation pattern TP11 as 1XX
- Partition: P_CallsFromClubToFrontDesk
- CSS: CSS_FrontDesk
- Calling Line ID Presentation and Calling Name Presentation: Allowed
- Connected Line ID Presentation and Connected Name Presentation: Allowed
- {P_CallsFromClubToFrontDesk, CSS_FrontDesk, Calling Line/Name - Allowed, Connected Line/Name - Allowed}
- Insert a translation pattern TP12 as 2XX
- Partition: P_CallsFromClubToRoom
- CSS: CSS_Room
- Calling Line ID Presentation and Calling Name Presentation: Allowed
- Connected Line ID Presentation and Connected Name Presentation: Restricted
- { P_CallsFromClubToRoom, CSS_Room, Calling Line/Name - Allowed, Connected Line/Name - Restricted}
- Insert a translation pattern TP13 as 1XX
- Partition: P_CallsFromPSTN
- CSS: CSS_FrontDesk
- Calling Line ID Presentation and Calling Name Presentation: Restricted
- Connected Line ID Presentation and Connected Name Presentation: Allowed
- { P_CallsFromPSTN, CSS_FrontDesk, Calling Line/Name - Restricted, Connected Line/Name - Allowed}

Call Park

From the Cisco Unified Communications Manager Administration Call Park Number Configuration window, configure the following items for the Call Park feature:

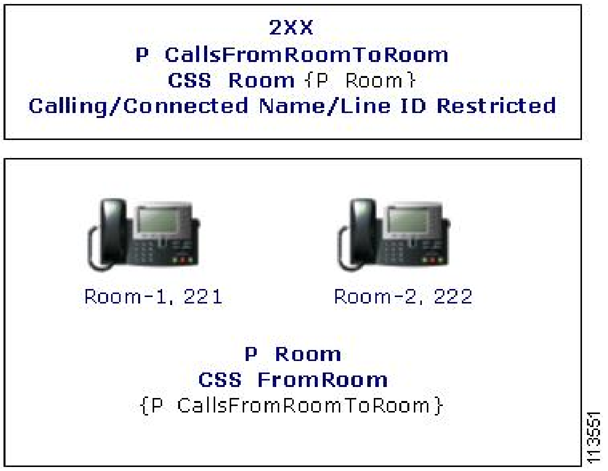
- Insert a Call Park directory number 888X
- Call Park Number Range: P_ParkNumberRange/888X
- Configure the translation patterns for the call park retrieval from
- room: TP (11-20): 8880 to 8889
- Partition: P_RoomToParkNumber
- CSS: CSS_RoomParkRange
- Calling Line ID Presentation and Calling Name Presentation: Restricted

- Connected Line ID Presentation and Connected Name Presentation: Restricted

Call Flow Example

The following figure shows a graphic representation of a sample call flow, with a description of how the Call Display Restrictions feature works in this scenario.

Figure 1: Sample Call Flow



1. Room-1 calls Room-2 (directory number 222).
2. Room-1 has CSS_FromRoom, so Room-1 can access only phones that are in the P_CallsFromRoomToRoom partition.
3. The P_CallsFromRoomToRoom partition contains 2XX, but it does not contain directory number 222 (Room-2).
4. The call routes to translation pattern TP:2XX, which is configured to restrict display information.
5. The TP:2XX translation pattern can access the P_Room partition because it is configured with the CSS_Room calling search space.
6. The CSS_Room calling search space contains directory number 222 (Room-2).
7. The call connects to Room-2, but theTP:2XX translation pattern restricts the display information.

Configure the Service Parameter for Connected Number Display Restriction

The connected number display restriction restricts the connected line ID presentation to dialed digits only. This option addresses customer privacy issues as well as connected number displays that are meaningless to phone users.

Procedure

Step 1 In Cisco Unified Communications Manager 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 setting is False.

Step 4 (Optional) Set the **Name Display for Original Dialed Number When Translated** service parameter.

The default setting displays the alerting name of the original dialed number before translation. You can change this parameter to display 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**.

CHAPTER 6

Call Park and Directed Call Park

This chapter provides information about the Call Park feature, which is a hold function, and the Directed Call Park feature, which is a transfer function. Cisco recommends that you treat these two features as mutually exclusive: enable one or the other, but not both. If you do enable both, ensure that the numbers that are assigned to each are exclusive and do not overlap.

Call Park Configuration

The Call Park feature allows you to place a call on hold, so it can be retrieved from another phone in the Cisco Unified Communications Manager system (for example, a phone in another office or in a conference room). If you are on an active call at your phone, you can park the call to a call park extension by pressing the Park softkey or the Call Park button. Someone on 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.

Procedure

Step 1 Configure a partition for call park extension numbers to make partition available only to users who have the partition in their calling search space.

For more information, see topics related to partition configuration settings and media termination point configuration in the *Cisco Unified Communications Manager Administration Guide*.

Step 2 Configure a unique call park number or define a range of call park extension numbers for each Cisco Unified Communications Manager.

Step 3 Add all servers that call park uses to the appropriate Cisco Unified Communications Manager group.

For more information, see topics related to Cisco Unified CM group configuration in the *Cisco Unified Communications Manager Administration Guide*.

Note Servers and Cisco Unified Communications Managers get configured during installation.

Step 4 Assign the Standard User softkey template to each device that has call park access. For phones that do not use the Call Park softkey, add the Call Park button in a copy of the applicable phone button template. Assign the phone button template, which includes the Call Park button, to the phone in Phone Configuration.

For more information, see topics related to configuring softkey templates, phone buttons, and Cisco Unified IP Phones in the *Cisco Unified Communications Manager Administration Guide*.

Step 5 In the User Group Configuration window, assign application and end users to the Standard CTI Allow Call Park Monitoring user group. This requirement applies only to users associated with CTI applications that require Call Park monitoring capability.

For more information, see topics related to adding users to a user group in the *Cisco Unified Communications Manager Administration Guide*.

Step 6 Notify users that the call park feature is available.

See the phone documentation for instructions on how users access Call Park features on their Cisco Unified IP Phone.

Related Topics

Call Park Feature, on page 121

Configure a Call Park Number, on page 130

Directed Call Park Configuration

Directed Call Park allows a user to transfer a call to an available user-selected directed call park number. Configure directed call park numbers in the Cisco Unified Communications Manager Directed Call Park Configuration window. Configured directed call park numbers exist clusterwide. You can configure phones that support the directed call park Busy Lamp Field (BLF) to monitor the busy/idle status of specific directed call park numbers. Users can also use the BLF to speed dial a directed call park number. See the System Requirements for Directed Call Park, on page 137 for a list of the phone models that support the BLF.

Cisco 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. Configure the retrieval prefix in the Directed Call Park Configuration window.

Perform the following steps to configure directed call park. For more information, see the Directed Call Park Feature, on page 136 and the **Directed Call Park Configuration** .

Procedure

Step 1 Configure a partition for directed call park numbers to make the partition available only to users who have the partition in their calling search space. To successfully retrieve a parked call, the calling search space from which the user is retrieving the call must contain the partition that includes the directed call park number.

Step 2 Configure a unique directed call park number or define a range of directed call park numbers. You must specify a range by using wildcards. For example, the range 40XX configures the range as 4000 to 4099.

Caution Do not enter a range by using dashes (such as 4000-4040).

Note You can monitor only individual directed call park numbers with the directed call park BLF. If you configure a range of numbers, the BLF cannot support monitoring of the busy/idle status of the range or of any number within the range.

Step 3 Assign the Standard User softkey template to each device that has directed call park access.

Step 4 For phone models that support the directed call park BLF, configure the phone button template to include one or more Call Park BLF buttons and configure the directed call park BLF settings.

Step 5 Notify users that the directed call park feature is available.

Call Park Feature

The Call Park feature allows you to place a call on hold, so it can be retrieved from another phone in the Cisco Unified Communications Manager system (for example, a phone in another office or in a conference room). If you are on an active call at your phone, you can park the call to a call park extension by pressing the Park softkey or the Call Park button. Someone on 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 Cisco Unified Communications Manager cluster, and each Cisco Unified Communications Manager in a cluster must have call park extension numbers defined. (For information about using call park across clusters, see the Use Call Park Across Clusters, on page 122.) 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.

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 within the Cisco Unified Communications Manager.

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, Cisco Unified Communications Manager chooses the next call park extension number that is available and displays that number on the phone.

Cisco Unified Communications Manager can park only one call at each call park extension number.

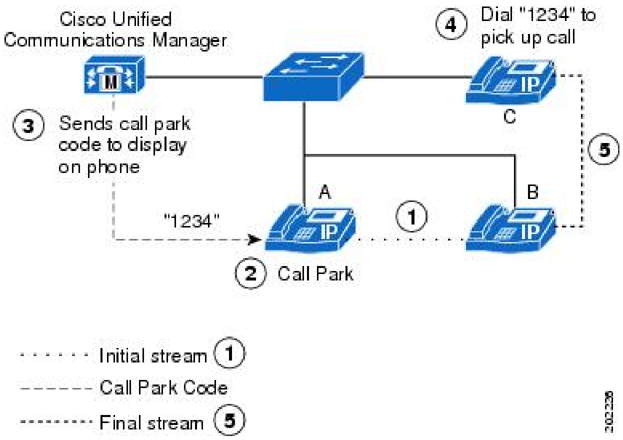
Note If users will use call park across servers in a cluster, ensure each Cisco Unified Communications Manager server in a cluster has call park extension numbers that are configured.See the Configure a Call Park Number, on page 130 for configuration details.

Use the Call Park Feature

The following figure illustrates the call park process.

1. User on phone A calls phone B.
2. User on phone A wants to take the call in a conference room for privacy. Phone A user presses the Park softkey or button.
3. The Cisco Unified Communications Manager server to which phone A is registered sends the first available call park directory, 1234, which displays on phone A. The user on phone A watches the display for the call park directory number (so he can dial that directory number on phone C).
4. The user on phone A leaves the office and walks to an available conference room where the phone is designated as phone C. The user goes off-hook on phone C and dials 1234 to retrieve the parked call.
5. The system establishes call between phones C and B.

Figure 2: Call Park Process



Use Call Park Across Clusters

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 Cisco Unified Communications Manager cluster. Additionally, you must ensure that calling search spaces and partitions are properly configured.

See the following example.

Example of Retrieving Parked Calls from Another Cluster

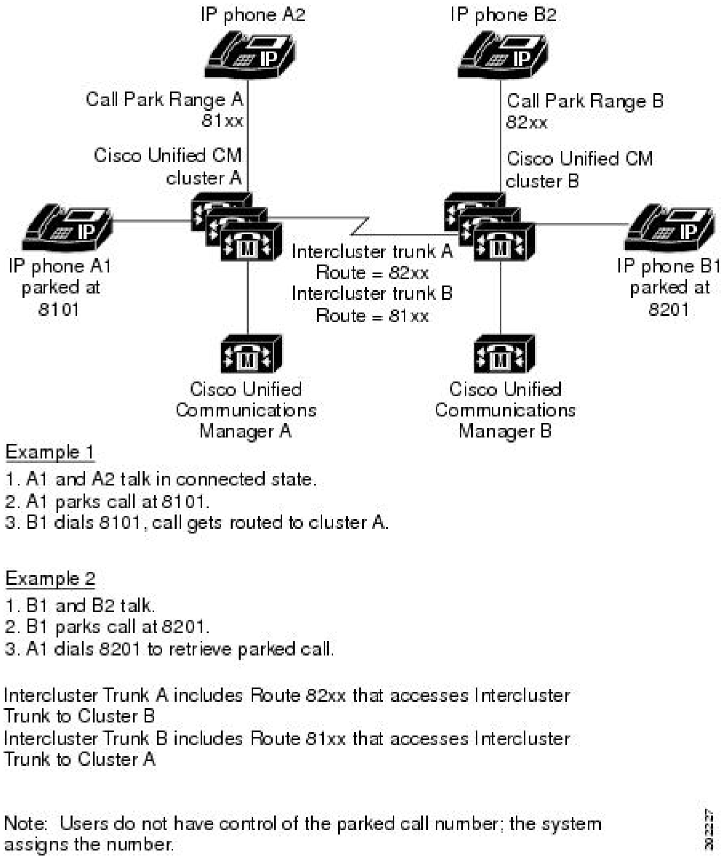
Two clusters exist in the network (cluster A and cluster B). Cluster A includes user A1 and user A2. Cluster B includes user B1 and user B2.

Cluster A includes call park numbers in the range of 81xx. Cluster B includes call park numbers in the range of 82xx, which the administrator configured.

Cluster A includes route patterns that are configured to other cluster park ranges as 82xx (routes to Cluster B). Cluster B includes route patterns that are configured to other cluster park ranges as 81xx (routes to Cluster A).

When user A1 parks a call at 8101, all users (which have correct partitions configured) in Cluster A and Cluster B can retrieve the parked call because of the route pattern configuration. When user B1 parks a call at 8202, all users (which have correct partitions configured) in Cluster A and Cluster B can retrieve the parked call because of the route pattern configuration. See the following figure.

Figure 3: Retrieving Parked Calls by Using Intercluster Trunks



Example 1

1. A1 and A2 talk in connected state.
2. A1 parks call at 8101.
3. B1 dials 8101, call gets routed to cluster A.

Example 2

1. B1 and B2 talk.
2. B1 parks call at 8201.
3. A1 dials 8201 to retrieve parked call.

Intercluster Trunk A includes Route 82xx that accesses Intercluster Trunk to Cluster B
Intercluster Trunk B includes Route 81xx that accesses Intercluster Trunk to Cluster A

Note: Users do not have control of the parked call number; the system assigns the number.

Cluster-Wide Call Park

Cisco Unified CM allows you to enable call parking for cluster-wide configurations. The feature consists of these functions:

- Park numbers for all nodes in a Cisco Unified CM cluster are now allocated from a single entity, the lowest active node in the cluster. Therefore, Cisco Unified CM ignores the field on the Call Park Number Configuration web page
- The single entity allocates park numbers from a pool of all configured park numbers, regardless of which Cisco Unified CM is assigned.
- Cisco Unified CM allocates park numbers through strict enforcement of the partition order in the Calling Search Space (CSS) of the parking party. This update provides a predictable behavior that is easy for administrators to understand.
- The parked calls limit is no longer 100 calls per cluster. Available park numbers and system resources determine the number of parked calls.

Cluster-Wide Call Park and Softkey

After the called party presses the CallPark softkey to park a call, Cisco Unified CM takes the following actions to allocate a park number:

- The lowest active node in the cluster manages the pool of all configured park numbers.
- Cisco Unified CM checks the partition list of the CSS of the parking party for available park numbers by searching each partition in order. If Cisco Unified CM finds a number, the system allocates the number and marks it as unavailable. If Cisco Unified CM does not find an available number in any of the partitions, the call park attempt fails.

Cluster-Wide Call Park Behavior

With Cluster-wide Call Park, centralized Cisco Unified CM deployments that host multiple locations on a single cluster (such as retail stores and bank branches) place the park numbers for each location into the partitions that are devoted to those locations. This placement prevents parties at one store from retrieving calls parked at another store. Also, the new Call Park behaviors reduce the difficulty of administering the feature, because administrators no longer need to place park numbers in the CSS of each inbound trunk or gateway.

Finally, this behavior follows the partition order of a CSS when searching for park numbers, which aligns with the search behaviors of other Cisco Unified CM features described in the SRND.

Enable Cluster-Wide Call Park

Procedure

Step 1 Select **System** > **Service Parameters**

Step 2 Select the desired node as "Server" and service as "Cisco CallManager (active)"

Step 3 Select the **Advanced** button

The advanced service parameters are displayed in the window

Step 4 Under the **Clusterwide Parameters (Feature - General)** section, set the Enable Clusterwide CallPark Number/Ranges service parameter to True.

Step 5 Restart all Cisco Unified CM services

CTI Support for Cluster-Wide Call Park

Cisco Unified Communications Manager provides CTI support for both legacy and cluster-wide call park.

For cluster-wide call park, if a cluster node becomes out of service while a call is parked, the monitored line generates a Call Disconnected event from that node. If all the nodes in the cluster become out of service, the monitored line generates a LineOutOfService event. The Parked line remains in service as long as there is one active node in the cluster.

System Requirements for Call Park

To operate, call park requires the following software component:

- Cisco Unified Communications Manager

The following IP phones (SCCP and SIP) support call park with the Park softkey in the Standard User and Standard Feature softkey templates:

- Cisco Unified IP Phones 6900 (except 6901 and 6911)
- Cisco Unified IP Phones 7900 (except 7921, 7925, 7935, 7936, 7937)
- Cisco Unified IP Phones 8900
- Cisco Unified IP Phones 9900

Note You can configure Call Park on any line (except line 1) or button by using the programmable line key feature.

The following IP phones (SCCP and SIP) support call park with the Call Park button in the phone button templates:

- Cisco Unified IP Phones 6900 (except 6901 and 6911)
- Cisco Unified IP Phones 7900 (except 7906, 7911, 7921, 7925, 7935, 7936, 7937)
- Cisco Unified IP Phones 8900
- Cisco Unified IP Phones 9900

Interactions and Restrictions

This section describes the interactions and restrictions for call park.

Interactions

This section provides information about how Call Park interacts with Cisco Unified Communications Manager applications and call processing.

CTI Applications

CTI applications access call park functionality, including monitoring activity on call park DNs. To monitor a call park DN, you must 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. 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.

Route Plan Report

The route plan report displays the patterns and directory numbers that are configured in Cisco Unified Communications Manager. Use the route plan report to look for overlapping patterns and directory numbers before assigning a directory number to call park. See theCisco Unified Communications Manager Administration Guide.

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. See the Cisco Unified Communications Manager Administration Guide.

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-messaging mailbox greeting of user B.

Barge

The following paragraphs describe the differences between Barge and cBarge with call park.

Barge with Call Park

The target phone (the phone that is being barged upon) controls the call. The barge initiator “piggy backs” 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 makes it behave similar to a MeetMe conference. Both phones (target and barge initiator) have full access to their features.

Directed Call Park

Cisco recommends 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.

Q.SIG 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.

Restrictions

The following restrictions apply to call park:

- Cisco Unified Communications Manager can park only one call at each call park extension number.
- Ensure each call park directory number, partition, and range is unique within the Cisco Unified Communications Manager.
- For shared line devices across nodes, the line will register 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.
- To achieve failover/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.
- Each Cisco Unified Communications Manager to which devices are registered needs 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 Cisco Unified Communications Manager Dialed Number Analyzer tool.
- If any call park numbers are configured for Cisco 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.
- If you entered a Call Park Reversion Timer value that is less than the Call Park Display Timer, call park numbers may not display on the phone.

- If directed call park (or call park) is initiated from a shared line and the call is not retrieved from any device, then the parked call does not always get reverted to the recipient in the shared line (parker). A conference call is set up between both the shared lines and the caller on park reversion or park reversion fails causing a two-party call (between the other shared line and caller). The reason being, on park reversion, Cisco 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 which hit the park). If the party already in the conference is attempted to be added first by Cisco Unified Communications Manager, then the park reversion fails. When park reversion fails, the shared line can still barge into the call as usual.

See the Configure a Call Park Number, on page 130 for configuration details.

Install and Activate Call Park

Call park, a system feature, comes standard with Cisco Unified Communications Manager software. It does not require special installation.

Configure Call Park

This section contains the following information:

Tip Before you configure Call Park, review the Call Park configuration information.

Related Topics

Call Park Configuration, on page 119

Set the Service Parameters for Call Park

Cisco Unified Communications Manager provides two clusterwide service parameters for call park: Call Park Display Timer and Call Park Reversion Timer. Each service parameter includes a default and requires no special configuration.

- Call Park Display Timer - Default specifies 10 seconds. This parameter determines how long a call park number displays on the phone that parked the call. Set this timer for each server in a cluster that has the Cisco CallManager service and call park configured.
- Call Park Reversion Timer - Default specifies 60 seconds. This parameter determines the time that a call remains parked. Set this timer for each server in a cluster that has the Cisco CallManager service and call park configured. 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 upon expiration of the Call Park Reversion Timer.

Procedure

Step 1 To set the timers, choose **System** > **Service Parameters**.

Step 2 Update the Call Park Display Timer.

Step 3 Update the Call Park Reversion Timer fields in the Clusterwide Parameters (Feature-General) pane.

Find a Call Park Number

Because you may have several call park numbers in your network, Cisco Unified Communications Manager lets you locate specific call park numbers on the basis of specific criteria. Use the following procedure to locate call park numbers.

Note During your work in a browser session, Cisco Unified Communications Manager Administration retains your call park number search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your call park number search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Call Routing** > **Call Park**.

The Find and List Call Park Numbers window displays.

Step 2 To find all records in the database, ensure the dialog box is empty.

To filter or search records:

a) From the first drop-down list box, select a search parameter.
b) From the second drop-down list box, select a search pattern.
c) Specify the appropriate search text, if applicable.

Note To add additional search criteria click the **+** button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the **–** button to remove the last added criteria or click the Clear Filter button to remove all added search criteria.

Step 3 Click **Find**.

All or matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

Note You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking Delete Selected. You can delete all configurable records for this selection by clicking Select All and then clicking Delete Selected.

Step 4 From the list of records that display, click the link for the record that you want to view.

Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Configure a Call Park Number

This section describes how to add, copy, and update a single call park extension number or range of extension numbers.

Procedure

Step 1 Choose **Call Routing** > **Call Park**.

Step 2 Perform one of the following tasks:

a) To add a new Call Park Number, click **Add New**.

b) To copy a Call Park Number, find the Call Park number or range of numbers and then click the **Copy** icon.

c) To update a Call Park Number, find the Call Park number or range of numbers.

The Call Park Number Configuration window displays.

Step 3 Enter or update the appropriate Call Park settings.

Step 4 To save the new or changed call park numbers in the database, click **Save.**

Related Topics

Call Park Configuration, on page 130

Find a Call Park Number, on page 129

Call Park Configuration

The Call Park feature allows you to place a call on hold, so it can be retrieved from another phone in the Cisco Unified Communications Manager system (for example, a phone in another office or in a conference room). If you are on an active call at your phone, you can park the call to a call park extension by pressing the Park softkey or the Call Park button. Someone on 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 following table describes the call park configuration settings.

Table 17: Call Park Configuration Settings

Field	Description
Call Park Number/Range	Enter the call park extension number. You can enter literal 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 Cisco Unified Communications Manager servers. Ensure that each Cisco 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 box. If you do not want to restrict access to the call park numbers, choose <None> for the partition. See topics related to searching for a partition in the *Cisco Unified Communications Manager Administration Guide* for instructions on finding a partition when there are a large number of them configured. **Note** Make sure that the combination of call park extension number and partition is unique within the Cisco Unified Communications Manager.
Cisco Unified Communications Manager	Using the drop-down list box, choose the Cisco Unified Communications Manager to which these call park numbers apply. **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 Cisco Unified Communications Manager servers. Ensure that each Cisco 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 comprised of phones and gateways talking to various nodes, where calls originating from any server may need to be parked, the phones require a CSS that contains call park ranges from all servers.

Delete a Call Park Number

This section describes how to delete call park numbers from the Cisco Unified Communications Manager database.

Procedure

Step 1 Using the procedure in the Find a Call Park Number, on page 129, locate the call park number or range of numbers.

Step 2 Click the call park number or range of numbers that you want to delete.

Step 3 Click **Delete.**

Note You can delete multiple call park numbers from the Find and List Call Park Numbers window by checking the check boxes next to the appropriate call park numbers and clicking **Delete Selected**. You can delete all call park numbers in the window by clicking **Select All** and then clicking **Delete Selected**.

Park Monitoring for Cisco Unified IP Phones 8961 9951 and 9971

Park monitoring is supported only when a Cisco Unified IP Phone 8961, 9951, or 9971 (SIP) parks a call. Park monitoring then monitors the status of a parked call. The park monitoring call bubble is not cleared until the parked call gets retrieved or is abandoned by the parkee. This parked call can be retrieved using the same call bubble on the parker’s phone.

Note Configuring call park numbers and settings are the same procedures as for other phone models.

Set the Service Parameters for Park Monitoring

Cisco Unified Communications Manager provides three clusterwide service timer parameters for park monitoring: Park Monitoring Reversion Timer, Park Monitoring Periodic Reversion Timer, and Park Monitoring Forward No Retrieve Timer. Each service parameter includes a default and requires no special configuration. These timer parameters apply to park monitoring only; the Call Park Display Timer and Call Park Reversion Timer are not used for park monitoring. Set these timers for each server in a cluster that has the Cisco CallManager service and call park configured.

See the following table for descriptions of these parameters.

Table 18: Service Parameters for Park Monitoring

Field	Description
Park Monitoring Reversion Timer	Default value specifies 60 seconds. This parameter determines the number of seconds that Cisco 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. You can override the value that this service parameter specifies on a per-line basis in the Directory Number Configuration window (Call Routing > Directory Number), in the Park Monitoring section. Specify a value of 0 to immediately utilize the periodic reversion interval that the Park Monitoring Periodic Reversion Timer service parameter specifies. For example, if this parameter is set to zero and the Park Monitoring Periodic Reversion Timer is set to 15, the user is prompted about the parked call immediately and every 15 seconds thereafter until the Park Monitoring Forward No Retrieve Timer expires.
Park Monitoring Periodic Reversion Timer	Default value specifies 30 seconds. This parameter determines the interval (in seconds) that Cisco Unified Communications Manager waits before prompting the user again that a call has been parked. To connect to the parked call, the user can simply go off-hook during one of these prompts. Cisco Unified Communications Manager continues to prompt the user about the parked call as long as the call remains parked and until the Park Monitoring Forward No Retrieve Timer expires. Specify a value of 0 to disable periodic prompts about the parked call.
Park Monitoring Forward No Retrieve Timer	Default value specifies 300 seconds. This parameter determines the number of seconds that park reminder notifications occur before the parked call forwards to the Park Monitoring Forward No Retrieve destination that is specified in the parker Directory Number Configuration window. (If no forward destination is provided in Cisco Unified Communications Manager Administration, the call returns to the line that parked the call.) This parameter starts when the Park Monitoring Reversion Timer expires. When the Park Monitoring Forward No Retrieve Timer expires, the call is removed from park and forwards to the specified destination or returned to the parker line.

Note To set the timers, choose **System** > **Service Parameters** and update the Park Monitoring Reversion Timer, Park Monitoring Periodic Reversion Timer, and Park Monitoring Forward No Retrieve Timer fields in the Clusterwide Parameters (Feature-General) pane.

Set Park Monitoring Parameters in Directory Number Configuration Window

The Directory Number Configuration window (**Call Routing** > **Directory Number**) contains an area called "Park Monitoring," where you can configure the three parameters shown in the following table.

Table 19: Park Monitoring Parameters in Directory Number Configuration Window

Field	Description
Park Monitoring Forward No Retrieve Destination External	When the parkee is an external party, the call forwards to the specified destination in the parker Park Monitoring Forward No Retrieve Destination External field. If the Forward No Retrieve Destination External field value is empty, the parkee gets redirected to the parker line.
Park Monitoring Forward No Retrieve Destination Internal	When the parkee is an internal party, the call forwards to the specified destination in the parker Park Monitoring Forward No Retrieve Destination Internal field. If the Park Monitoring Forward No Retrieve Destination Internal field is empty, the parkee gets redirected to the parker line.
Park Monitoring Reversion Timer	This parameter determines the number of seconds that Cisco 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. Default: 60 seconds **Note** If you configure a non-zero value, this value overrides the value of this parameter that is set in the Service Parameters window. However, if you configure a value of 0 here, the value in the Service Parameters window gets used.

Set Park Monitoring Parameter in Hunt Pilot Configuration Window

When a call that was routed via the hunt list is parked, the Hunt Pilot Park Monitoring Forward No Retrieve Destination parameter value is used (unless it is blank) when the Park Monitoring Forward No Retrieve Timer expires. This value is configured in the Hunt Pilot Configuration window (**Call Routing** > **Route/Hunt** >

Hunt Pilot). If the Hunt Pilot Park Monitoring Forward No Retrieve Destination parameter value is blank, then the call will be forwarded to the destination configured in the Directory Number Configuration window when the Park Monitoring Forward No Retrieve Timer expires.

Directed Call Park Feature

Directed Call Park allows a user to transfer a call to an available user-selected directed call park number. Configure directed call park numbers in the Cisco Unified Communications Manager Directed Call Park Configuration window. Configured directed call park numbers exist clusterwide. You can configure phones that support the directed call park Busy Lamp Field (BLF) to monitor the busy/idle status of specific directed call park numbers. Users can also use the BLF to speed dial a directed call park number. See Interactions and Restrictions, on page 137, for a list of the phone models that support the BLF.

Cisco 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. Configure the retrieval prefix in the Directed Call Park Configuration window.

Call Gets Retrieved Example

The following example illustrates the use of the directed call park feature and retrieval of the parked call on Cisco Unified IP Phones (SCCP) only.

1. Users A1 and A2 connect in a call.
2. To park the call, A1 presses the Transfer softkey (or Transfer button, if available) and dials directed call park number 80 (for example) or presses the BLF button for directed call park number 80 (if the phone model supports the BLF button).
3. A1 either presses the Transfer softkey (or Transfer button) again or goes on hook to complete the directed call park transfer. This action parks A2 on directed call park number 80.

Note The user 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. See the Cisco Unified Communications Manager System Guide.

4. From any phone with a correctly configured partition and calling search space, user B1 dials the directed call park prefix (21, for example) followed by the directed call park number 80 to retrieve the call. B1 connects to A2.

Call Does Not Get Retrieved Example

The following example illustrates the use of the directed call park feature when the parked call does not get retrieved and reverts to the reversion number. This example illustrates how the feature works on Cisco Unified IP Phones (SCCP) only.

1. Users A1 and A2 connect in a call.

2. To park the call, A1 presses the Transfer softkey (or Transfer button, if available) and dials directed call park number 80 (for example) or presses the BLF button for directed call park number 80 (if the phone model supports the BLF button).
3. A1 either presses the Transfer softkey (or Transfer button) again or goes on hook to complete the directed call park transfer. This action parks A2 on directed call park number 80.

Note The user 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. See the Cisco Unified Communications Manager System Guide.

4. The call does not get retrieved before the Call Park Reversion Timer (service parameter) expires.
5. A2 reverts to the configured reversion number.

System Requirements for Directed Call Park

To operate, Directed Call Park requires the following software component:

- Cisco Unified Communications Manager

A user can park and retrieve a call by using directed call park from any phone that can perform a transfer. Cisco VG248 Analog Phone Gateways also support directed call park.

The following IP phones (SCCP and SIP) support directed call park BLF:

- Cisco Unified IP Phone 6900 Series (except 6901 and 6911)
- Cisco Unified IP Phone 7900 Series (except 7906, 7911, 7936, 7937)
- Cisco Unified Wireless IP Phone 7925
- Cisco Unified IP Phone Expansion Module (7914, 7915, 7916)
- Cisco Unified IP Color Key Expansion Module
- Cisco Unified IP Phone 8900 Series
- Cisco Unified IP Phone 9900 Series

The following phones that are running SCCP support directed call park BLF:

- Cisco Unified IP Phones (7940, 7960)

Interactions and Restrictions

This section describes the interactions and restrictions for directed call park.

Interactions

This section describes how directed call park interacts with Cisco Unified Communications Manager applications and call processing features.

Music On Hold

Music on hold allows users to place calls on hold with music that is provided from a streaming source. 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 Call Manager service parameter, Default Network Hold MOH Audio Source, for the audio source.

Route Plan Report

The route plan report displays the patterns and directory numbers that are configured in Cisco Unified Communications Manager. Use the route plan report to look for overlapping patterns and directory numbers before assigning a directory number to directed call park. See the Cisco Unified Communications Manager Administration 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. See the Cisco Unified Communications Manager Administration Guide.

Related Topics

Call Park, on page 139

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 voice-messaging mailbox greeting of user B.

Barge

The following paragraphs describe the differences between Barge and cBarge with directed call park.

Barge with Directed Call Park

The target phone (the phone that is being barged upon) controls the call. The barge initiator “piggy backs” 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 similar to a meet-me conference. Both phones (target and barge initiator) retain full access to their features.

Call Park

Cisco recommends 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.

Restrictions

The following restrictions apply to directed call park:

- Cisco Unified Communications Manager can park only one call at each directed call park number.
- Ensure each directed call park directory number, partition, and range is unique within the Cisco Unified Communications Manager. If the Park softkey is also activated (not recommended), ensure that no overlap exists between call park numbers and directed call park numbers.
- A caller who has been parked (the parkee) by using the directed call park feature cannot, while parked, use the standard call park feature.
- 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.
- 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.
- If reversion number is not configured, the call reverts to the parker (parking party) after the call park reversion timer expires. Directed Call Park for phones that are running SIP is designed as busy lamp field (BLF) plus call transfer (to a park code). The transfer functionality remains the same as for phones that are running SCCP. 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.

Related Topics

Configure a Directed Call Park Number, on page 141

Install and Activate Directed Call Park

Directed call park system feature comes standard with Cisco Unified Communications Manager software. Any phone that can perform a transfer can use directed call park. It does not require special installation. Cisco recommends that you configure either call park or directed call park, but not both. If you do configure both, ensure that the directed call park and call park numbers do not overlap.

Configure Directed Call Park

This section provides instructions to configure Directed Call Park.

Tip Before you configure Directed Call Park, review the Directed Call Park configuration information.

Related Topics

Directed Call Park Configuration, on page 120

Set the Service Parameters for Directed Call Park

The Call Park Reversion Timer clusterwide service parameter affects directed call park. This parameter determines the time that a call remains parked. The default specifies 60 seconds. When the timer expires, the parked call returns to either the device that parked the call or to another specified number, depending on what you configure in the Directed Call Park Configuration window.

Find a Directed Call Park Number

Because you may have several directed call park numbers in your network, Cisco Unified Communications Manager lets you locate specific directed call park numbers on the basis of specific criteria. Use the following procedure to locate directed call park numbers.

Note During your work in a browser session, Cisco Unified Communications Manager Administration retains your directed call park number search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your directed call park number search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Call Routing** > **Directed Call Park**.

The Find and List Directed Call Parks window displays.

Step 2 To filter or search records:

a) From the first drop-down list box, select a search parameter.

b) From the second drop-down list box, select a search pattern.

c) Specify the appropriate search text, if applicable.

Note To add additional search criteria, click the **+** button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the **–** button to remove the last added criteria or click the **Clear Filter** button to remove all added search criteria.

Step 3 To find all records in the database, ensure the dialog box is empty, click **Find**.

All or matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

Note You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking **Delete Selected**. You can delete all configurable records for this selection by clicking **Select All** and then clicking **Delete Selected**.

Step 4 From the list of records that display, click the link for the record that you want to view.

Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Configure a Directed Call Park Number

This section describes how to add, copy, and update a single directed call park extension number or range of extension numbers.

Procedure

Step 1 Choose **Call Routing** > **Directed Call Park**.

Step 2 Perform one of the following tasks:

a) To add a new Directed Call Park Number, click **Add New**.

b) To copy a Directed Call Park Number, find the Directed Call Park number or range of numbers and then click the **Copy** icon.

c) To update a Directed Call Park Number, find the Directed Call Park number or range of numbers.

The Directed Call Park Number Configuration window displays.

Step 3 Enter or update the appropriate Directed Call Park settings.

Step 4 To save the new or changed call park numbers in the database, click **Save.**

Note If you update a directed call park number, Cisco Unified Communications Manager reverts any call that is parked on that number only after the Call Park Reversion Timer expires.

Note Whenever changes are made to directed call park numbers or ranges, any devices that are configured to monitor those directed call park numbers by using the BLF must restart to correct the display. Change notification automatically restarts impacted devices when it detects directed call park number changes. You can also use the Restart Devices button on the Directed Call Park Configuration window.

Related Topics

Directed Call Park Configuration, on page 142

Find a Directed Call Park Number, on page 140

Directed Call Park Configuration

Directed Call Park allows a user to transfer a call to an available user-selected directed call park number. Configure directed call park numbers in the Cisco Unified Communications Manager Directed Call Park Configuration window. Configured directed call park numbers exist clusterwide. You can configure phones that support the directed call park Busy Lamp Field (BLF) to monitor the busy/idle status of specific directed call park numbers. Users can also use the BLF to speed dial a directed call park number.

Cisco 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. Configure the retrieval prefix in the Directed Call Park Configuration window.

The following table provides a checklist to configure directed call park.

Table 20: Directed Call Park Configuration Settings

Field	Description
Number	Enter the directed call park number. You can enter literal digits or the wildcard character 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-quotes (“), percentage sign (%), ampersand (&), or angle brackets (<>)

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 box. If you do not want to restrict access to the directed call park numbers, leave the partition as the default of <None>. See the *Cisco Unified Communications Manager Administration Guide* for instructions on finding a partition when there are a large number of them configured. **Note** Make sure that the combination of directed call park number and partition is unique within the Cisco 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 box, 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.

Note Whenever changes are made to directed call park numbers, any devices that are configured to monitor those directed call park numbers by using the directed call BLF must restart to correct the display. Change notification automatically restarts impacted devices when it detects directed call park number changes. You also can use the Restart Devices button on the Directed Call Park Configuration window.

Related Topics

Interactions and Restrictions, on page 137

Directed Call Park Feature, on page 136

Configure BLF/Directed Call Park Buttons

To configure BLF/Directed Call Park buttons, perform the following procedure:

Procedure

Step 1 To configure the BLF/Directed Call Park button in the Phone Configuration window, find the phone, as described in the Cisco Unified Communications Manager Administration Guide.

Step 2 To configure the BLF/Directed Call Park button for user device profiles, find the user device profile as described in the Cisco Unified Communications Manager Administration Guide.

Step 3 After the configuration window displays, click the Add a new BLF Directed Call Park link in the Association Information pane.

Tip 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 4 Configure the settings, as described in BLF/Directed Call Park Configuration, on page 144.

Step 5 After you complete the configuration, click **Save** and close the window.

The directory number(s) display in the Association Information pane of the Phone Configuration Window.

BLF/Directed Call Park Configuration

The following table describes the settings that you configure for BLF/Directed Call Park buttons.

Table 21: BLF/Directed Call Park Button Configuration Settings

Field	Description
Directory Number	The Directory Number drop-down list box displays a list of directory numbers 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 displays) 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. **Tip** 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

To synchronize devices with directed call park information that has undergone configuration changes, perform the following procedure, which will apply any outstanding configuration settings in the least-intrusive manner possible. (For example, a reset/restart may not be required on some affected devices.)

Procedure

Step 1 Choose **Call Routing** > **Directed Call Park**.

The Find and List Directed Call Parks window displays.

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 displays.

Step 5 Make any additional configuration changes.

Step 6 Click **Save.**

Step 7 Click **Apply Config**.

The Apply Configuration Information dialog displays.

Step 8 Click **OK.**

Delete a Directed Call Park Number

This section describes how to delete directed call park numbers from the Cisco Unified Communications Manager database.

Procedure

Step 1 Using the procedure in the Find a Directed Call Park Number, on page 140, locate the directed call park number or range of numbers.

Step 2 Click the directed call park number or range of numbers that you want to delete.

Step 3 Click **Delete**.

Note Deleting a directed call park number causes Cisco Unified Communications Manager to immediately revert any call that is parked on that number. This occurs because, when the number is deleted, a parked call on that number cannot remain parked or be retrieved in the usual way and must be reverted.

Note 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 cannot be deleted because it is in use. To determine which devices are using the number, click the Dependency Records link in the Directed Call Park Configuration window.

Assisted Directed Call Park for Cisco Unified IP Phones (SIP)

Assisted directed call park is supported on all Cisco Unified IP Phones 7900, 8900, and 9900 series that support SIP. With assisted directed call park, the end user needs to press only one button to direct-park a call. You must configure a BLF Directed Call Park button. Then, when the user presses an idle BLF Directed Call Park feature button for an active call, the active call gets parked immediately at the Dpark slot that associates with the Directed Call Park feature button.

Related Topics

Configure BLF/Directed Call Park Buttons, on page 143

CHAPTER 7

Call Pickup

This chapter provides information about the Call Pickup features which allow users to answer calls that come in on a directory number other than their own.

Configure Call Pickup and Group Call Pickup

The Call Pickup feature allows users to pick up incoming calls within their own group. Cisco Unified Communications Manager automatically dials the appropriate call pickup group number when the user activates this feature from a Cisco Unified IP Phone. Use the softkey, PickUp, for this type of call pickup.

Note Cisco Unified IP Phone 6900 uses the Call Pickup programmable feature button or the Call Pickup softkey; Cisco Unified IP Phone 8900 and 9900 use only the Call Pickup programmable feature button.

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.

Note Cisco Unified IP Phone 6900 uses the Group Pickup programmable feature button or the Group Pickup softkey; Cisco Unified IP Phone 8900 and 9900 use only the Group Pickup programmable feature button.

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.

Note The same procedures apply for configuring call pickup and group call pickup features. Group call pickup numbers apply to lines or directory numbers.

Perform the following steps to configure Call Pickup and Group Call Pickup features.

Procedure

Step 1 Configure partitions if you will be using them with call pickup groups.

For more information, see topics related to using Call Pickup features with partitions to restrict access and the *Cisco Unified Communications Manager Administration Guide* for partition configuration settings.

Step 2 Configure a call pickup group. Make sure that the name and number are unique.

Step 3 Assign the call pickup group that you created to the directory numbers that are associated with phones on which you want to enable call pickup:

a) To use the Call Pickup feature, you must use only directory numbers that are assigned to a call pickup group.
b) 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.

Step 4 (Optional) Configure the audio or visual, or both, notification.

a) Set the Call Pickup Group Audio Alert Setting service parameter.
b) Configure the type of notification (audio, visual, both) in the Call Pickup Group Configuration window.
c) Configure the notification timer in the Call Pickup Group Configuration window.
d) Configure the audio alert setting for each phone in the Directory Number Configuration window.

For more information, see topics related to Call Pickup notification and group configuration, as well as topics related to directory number configuration settings in the *Cisco Unified Communications Manager Administration Guide*.

Step 5 Add a call pickup or group pickup button to the phone button templates, if needed.

For more information, see topics related to phone button template configuration in the *Cisco Unified Communications Manager Administration Guide* .

Step 6 Assign the Standard User or Standard Feature softkey template to the phone that will be using the Pickup (PickUp) and Group Call Pickup (GPickUp) softkeys.

For more information, see topics related to

Note To restrict calls to be picked up by a phone within only its own group, deny the Group Pick Up (GPickUp) or Other Pick Up (OPickUp) softkeys in the softkey template by moving them to the Unselected Softkeys box that is in the Softkey Template Configuration window.

See topic related to assigning softkey templates to IP phones in the *Cisco Unified Communications Manager Administration Guide*

Step 7 If you want automatic call answering for call pickup groups, enable the Auto Call Pickup Enabled service parameter by choosing the value True. The default specifies False.

For more information, see topics related to Auto Call Pickup, and topics related to service parameter configuration in the *Cisco Unified Communications Manager Administration Guide*.

Step 8 If the Auto Call Pickup Enabled service parameter is False, enter a value for the Call Pickup No Answer Timer service parameter. 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.

For more information, see topics related to service parameter configuration in the *Cisco Unified Communications Manager Administration Guide*.

Step 9 Enter a value for the Pickup Locating Timer service parameter. This parameter controls the time for call selection for call pickup, group call pickup, and other group call pickup.

For more information, see topics related to service parameter configuration in the *Cisco Unified Communications Manager Administration Guide*.

Step 10 Notify users that the Call Pickup and/or Group Call Pickup feature is available.

See the phone documentation for instructions on how users access the Call Pickup and Group Call Pickup features on their Cisco Unified IP Phone.

Related Topics

- Assign a Call Pickup Group to Directory Numbers, on page 178
- Auto Call Pickup, on page 162
- Call Pickup, on page 147
- Call Pickup Feature, on page 155
- Call Pickup Notification, on page 166
- Call Pickup Group Configuration, on page 172
- Configure a Call Pickup Group, on page 172
- Use Call Pickup Features with Partitions, on page 165

Configure Other Group Pickup

The Other Group Pickup feature allows users to pick up incoming calls in a group that is associated with their own group. The Cisco 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. Use the softkey, OPickUp, for this type of call pickup.

Note Cisco Unified IP Phone 6900 uses the Other Pickup programmable feature button or the Other Pickup softkey; Cisco Unified IP Phone 8900 and 9900 use only the Other Pickup programmable feature button.

When more than one associated group exists, the priority of answering calls for the associated group goes from the first associated group to the last associated group. For example, groups A, B, and C associate with group X, and the priority of answering calls goes to group A, B, and then C. First, 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 Usually, within the same group, 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.

Procedure

Step 1 Configure a list of associated groups that can be chosen from all pickup groups. The list can include up to 10 groups.

For more information, see topics related to defining a pickup group for Other Group Pickup.

Step 2 Configure Calling Search Space and TOD parameters for members of the associated groups to your group.

For more information, see topics related to the following in the *Cisco Unified Communications Manager Administration Guide*:

- Calling Search Space
- Time schedule configuration
- Time period configuration

See also topics related to time-of-day routing in the *Cisco Unified Communications Manager System Guide*.

Step 3 If you want automatic call answering for other group call pickup, enable the Auto Call Pickup Enabled service parameter by entering the value True. The default specifies False.

For more information, see topics related to Auto Call Pickup and topics related to service parameter configuration in the *Cisco Unified Communications Manager Administration Guide*.

Step 4 If the Auto Call Pickup Enabled service parameter is False, enter a value for the Call Pickup No Answer Timer service parameter. This parameter controls the time that a call takes to get restored if a call is picked up but not answered by other group call pickup.

For more information, see topics related to service parameter configuration in the *Cisco Unified Communications Manager Administration Guide*.

Step 5 Enter a value for the service parameter Pickup Locating Timer. This parameter controls the time for call selection for call pickup, group call pickup, and other group call pickup.

For more information, see topics related to service parameter configuration in the *Cisco Unified Communications Manager Administration Guide*.

Step 6 To configure the Other Pickup (OPickUp) softkey for the phone, modify and add the Standard User or Standard Feature softkey template to the phone. Modify the template to include the OPickUp softkey by using the following steps.

a) Choose **Device** > **Device Settings** > **Softkey Template** in Cisco Unified Communications Manager Administration.
b) Choose the desired softkey template.
c) Choose the Softkey Layout Configuration link.
d) Choose **On Hook** or **Off Hook** call states.

e) Choose **Other Pickup (OPickUp)** in the Unselected Softkeys box. Click the right arrow to move the Other Pickup (OPickup) softkey to the Selected Softkeys box.

Note To restrict calls to be picked up by a phone within only its own group, deny the OPickUp softkey in the softkey template.

For more information, see topics related to assigning softkey templates to IP phones in the *Cisco Unified Communications Manager Administration Guide*.

Step 7 Add the OPickup button to the phone button templates, if needed.

For more information, see topics related to phone button template configuration in the *Cisco Unified Communications Manager Administration Guide*.

Step 8 Notify users that the Other Group Pickup feature is available.

See the phone documentation for instructions on how users access the Other Group Pickup feature on their Cisco Unified IP Phone.

Related Topics

Auto Call Pickup, on page 162
Call Pickup, on page 147
Call Pickup Feature, on page 155
Define a Pickup Group for Other Group Pickup, on page 177

Configure Directed Call Pickup

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. Cisco 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 have been 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 from which 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.

Perform the following steps to configure directed call pickup.

Procedure

Step 1 Configure a list of associated groups that can be chosen from all pickup groups. The list can include up to 10 groups.

For more information, see topics related to defining a pickup group for Other Group Pickup.

Step 2 Configure Calling Search Space and TOD parameters for members of the associated groups to your group.

For more information, see topics related to the following in the *Cisco Unified Communications Manager Administration Guide*:

- Calling Search Space
- Time schedule configuration
- Time period configuration

See also topics related to time-of-day routing in the *Cisco Unified Communications Manager System Guide*.

Step 3 If you want automatic call answering for directed call pickup, enable the Auto Call Pickup Enabled service parameter by entering the value True. The default specifies False.

For more information, see topics related to Auto Call Pickup and topics related to service parameter configuration in the *Cisco Unified Communications Manager Administration Guide*.

Step 4 If the Auto Call Pickup Enabled service parameter is False, enter a value for the Call Pickup No Answer Timer service parameter. This parameter controls the time that a call takes to get restored if a call is picked up but not answered by directed call pickup.

For more information, see topics related to service parameter configuration in the *Cisco Unified Communications Manager Administration Guide*.

Step 5 Enter a value for the service parameter Pickup Locating Timer. This parameter controls the time for call selection for call pickup, group call pickup, and other group call pickup.

For more information, see topics related to service parameter configuration in the *Cisco Unified Communications Manager Administration Guide*.

Step 6 To configure the Group Call Pickup (GPickUp) softkey for the phone, modify and add the Standard User or Standard Feature softkey template to the phone. Modify the template to include the GPickUp softkey with the following steps.

a) Choose **Device** > **Device Settings** > **Softkey Template** in Cisco Unified Communications Manager Administration.
b) Choose the desired softkey template.
c) Choose the Softkey Layout Configuration link.
d) Choose **On Hook** or **Off Hook** call states.
e) Choose **Group Call Pickup(GPickUp)** in the Unselected Softkeys box. Click the right arrow to move the Group Call Pickup (GPickUp) softkey to the Selected Softkeys box.

Note To restrict calls to be picked up by phones only within its own group, deny the GPickUp softkey in the softkey template.

For more information, see topics related to assigning softkey templates to IP phones in the *Cisco Unified Communications Manager Administration Guide*.

Step 7 Add the Group Pickup button to the phone button templates, if needed.

For more information, see topics related to phone button template configuration in the *Cisco Unified Communications Manager Administration Guide*.

Step 8 Notify users that the Directed Call Pickup feature is available.

See the phone documentation for instructions on how users access the Directed Call Pickup feature on their Cisco Unified IP Phone.

Related Topics

Auto Call Pickup, on page 162
Call Pickup, on page 147
Call Pickup Feature, on page 155
Define a Pickup Group for Other Group Pickup, on page 177

Configure BLF Call Pickup

You can associate the busy lamp field (BLF) button on a Cisco Unified IP Phone to a DN. This allows Cisco Unified Communications Manager to notify a phone user when a call is waiting to be picked up from the DN. The DN represents the BLF DN, and the phone that picks up the call to the BLF DN represents the BLF call pickup initiator.

The following rules apply to the BLF DN and the BLF call pickup initiator:

- The BLF call pickup initiator gets 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 call pickup is configured 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.

Note You can optionally configure an audible alert in addition to the visual alert.

The following actions take place for an incoming call to the BLF DN:

1. The BLF SD button flashes on the BLF call pickup initiator phone to indicate that an incoming call to the BLF DN exists.
2. 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.

Perform the following steps to configure BLF call pickup.

Before you begin

Be aware that when you create a BLF pickup group, your system requires that the initiator groups and target groups are associated with each other. If they are in the same group, the pickup group must be associated with itself.

Procedure

Step 1 Configure a call pickup group for the BLF DN. Make sure that the name and number are unique.

For more information, see topics related to Call Pickup Group configuration.

Step 2 Create another call pickup group and associate it to the call pickup group that was created. You can associate a call pickup group to multiple BLF DN call pickup groups.

- Only directory numbers that are assigned to a call pickup group can use the BLF Call Pickup feature.
- 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.

Note You do not always need to create another call pickup group. A pickup group can have itself as its association group.

For more information, see topics related to Call Pickup Group configuration.

Step 3 Create a customized phone button template that contains the Speed Dial BLF button and associate that phone button template with the phone devices that will be used to pick up calls from the BLF DN. The phone that picks up calls from the BLF DN represents the call pickup initiator.

For more information, see topics related to configuring Cisco Unified IP Phones and phone button template configuration in the *Cisco Unified Communications Manager Administration Guide*.

Step 4 Configure the BLF SD number on the phone that you created for the BLF call pickup initiator. To do this, click the Add a new BLF SD link in the Phone Configuration window. The Busy Lamp Field Speed dial Configuration window displays. Select a directory number as the BLF DN to be monitored by the BLF SD button. Use the Call Pickup check box to enable the pickup feature that is associated with the BLF SD button.

Note If the check box is checked, you can use the BLF SD button for BLF call pickup and BLF speed dial. If the check box is not checked, you can use the BLF SD button only for BLF speed dial.

For more information, see topics related to configuring Cisco Unified IP Phones in the *Cisco Unified Communications Manager Administration Guide*.

Step 5 In the Directory Number Configuration window, add the DN that is used as the BLF call pickup initiator to the call pickup group that was created.

Note The pickup group for the BLF DN should belong to the association groups for the initiator. The pickup group created in Step 2 must include the pickup group created in Step 1 in its set of association groups.

For more information, see topics related to directory number configuration in the *Cisco Unified Communications Manager Administration Guide*.

Step 6 In the Directory Number Configuration window, add the BLF DN to the call pickup group that was created.

For more information, see topics related to directory number configuration in the *Cisco Unified Communications Manager Administration Guide*.

Step 7 (Optional) In the Service Parameter Configuration window, enable the following Cisco CallManager service parameters to activate BLF call pickup audio alerting for the cluster:

- BLF Pickup Audio Alert Setting of Idle Station
- BLF Pickup Audio Alert Setting of Busy Station

For more information, see topics related to service parameter configuration in the *Cisco Unified Communications Manager Administration Guide*.

Step 8 (Optional) To enable the BLF call pickup initiator to connect to a caller by pressing the BLF-SD, set the Cisco CallManager service parameter Auto Call Pickup Enabled to true.

If you set this service parameter to false, the call pickup initiator must press the BLF-SD button as well as go offhook or press the answer button to answer the call.

For more information, see topics related to service parameter configuration in the *Cisco Unified Communications Manager Administration Guide*.

Step 9 (Optional) In the Phone Configuration window, enable the following fields to activate BLF call pickup audio alerting for the BLF call pickup initiator:

- BLF Audible Alert Setting (Phone Idle)
- BLF Audible Alert Setting (Phone Busy)

For more information, see topics related to configuring Cisco Unified IP Phones in the *Cisco Unified Communications Manager Administration Guide*.

Step 10 Notify users that the Call Pickup feature is available.

See the phone documentation for instructions on how users access the Call Pickup feature on their Cisco Unified IP Phone.

Related Topics

Call Pickup, on page 147
Call Pickup Feature, on page 155
Configure a Call Pickup Group, on page 172

Call Pickup Feature

Cisco Unified IP Phones support the following types of call pickup: call pickup, group call pickup, other group pickup, directed call pickup, BLF call pickup, and auto call pickup.

The following information applies to all of the call pickup types:

- Both idle and offhook call states make the three softkeys, PickUp, GPickUp, and OPickUp, available. The administrator must modify the standard softkey template to include these softkeys for the users to invoke the Call Pickup features.
- If a user invokes call pickup to pick up a call from a phone that has no incoming calls, the user receives a “No Call(s) for Pickup” message. If a user invokes call pickup to pick up a ringing call from a DN for which the user is not configured to pick up calls, the user receives reorder tone.

- Call Pickup operates with a consult transfer call. The following scenario provides an example. User A calls user C, and user C answers. User C presses the Transfer key and dials phone D. User E hears phone D ring and uses call pickup to pick up the call that is ringing on phone D. After user C presses the Transfer key again, user A and user E connect. Call Pickup also functions if user C presses Transfer before either phone D picks up the call or user E invokes Call Pickup.
- The Call Pickup feature operates with ad hoc conference calls. The following scenario provides an example. User A calls user C, and user C answers. User C presses the Conf key and makes a consultation call to phone D. User E hears phone D ring and uses call pickup to pick up the call that is ringing on phone D. User C then presses the Conf key again, and user A, user C, and user E connect to an ad hoc conference. Call pickup also functions if user C presses the Conf key a second time before user E picks up the call that is ringing on phone D.
- If user E successfully invokes call pickup to pick up a call from user A that is ringing on DN C while the Auto Call Pickup Enabled service parameter is set to False, but user E then does not pick up the call before the time that is specified in the Call Pickup No Answer Timer expires, the original call from user A gets restored and continues to ring at DN C.
- A user can only invoke Call Pickup if the user has a line free to pick up the call. If the user lines are busy with held calls, the user receives a “No Line Available for Pickup” message on the display and the original call continues to ring at the called number.

Related Topics

Configure Call Pickup and Group Call Pickup, on page 147
Configure Directed Call Pickup, on page 151
Configure Other Group Pickup, on page 149

Call Pickup

The Call Pickup feature allows users to pick up incoming calls within their own group. Cisco Unified Communications Manager automatically dials the appropriate call pickup group number when the user activates this feature from a Cisco Unified IP Phone. Use the softkey or feature button, PickUp, for this type of call pickup.

The Call Pickup feature functions whether auto call pickup is enabled or not. See the Auto Call Pickup, on page 162 for details.

Group Call Pickup

The Group Call Pickup feature allows users to pick up incoming calls in another group. User must dial the appropriate call pickup group number when this feature is activated from a Cisco Unified IP Phone. Use the softkey, GPickUp, or the feature button, Group Pickup, 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.

Note The same procedures apply for configuring call pickup and group call pickup features. Group call pickup numbers apply to lines or directory numbers.

The Group Call Pickup feature functions whether auto call pickup is enabled or not. See the Auto Call Pickup, on page 162 for details.

Other Group Pickup

The Other Group Pickup feature allows users to pick up incoming calls in a group that is associated with their own group. The Cisco 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. Use the softkey or feature button, OPickUp, for this type of call pickup.

When more than one associated group exists, the priority of answering calls for the associated group goes from the first associated group to the last associated group. For example, groups A, B, and C associate with group X, and the priority of answering calls goes to group A, B, and then C. First, 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 Usually, within the same group, 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.

The Other Group Pickup feature functions whether auto call pickup is enabled or not. See the Auto Call Pickup, on page 162 for details.

Directed Call Pickup

The Directed Call Pickup feature allows a user to pick up a ringing call on a DN directly by pressing the GPickUp softkey or Group Pickup feature button and entering the directory number of the device that is ringing. Cisco 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 have been 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 from which 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.

The Directed Call Pickup feature functions whether auto call pickup is enabled or not. See the Auto Call Pickup, on page 162 for details.

Examples of Directed Call Pickup

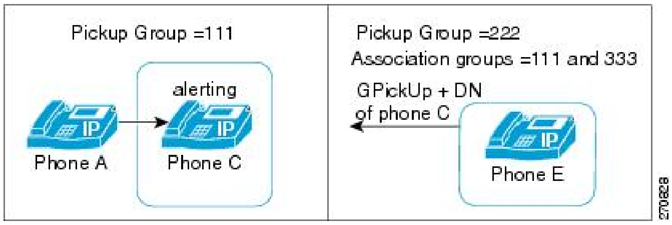
The following examples illustrate various Directed Call Pickup scenarios.

Basic Directed Call Pickup

This scenario illustrates Directed Call Pickup. The following setup takes place, as shown in the following figure:

1. Three pickup groups that are created comprise group numbers 111, 222, and 333.
2. Pickup group 222 includes association groups such that its Other Pickup Groups specify 111 and 333.
3. DN of phone C specifies 1000 in pickup group 111.
4. DN of phone E specifies 2000 in pickup group 222.

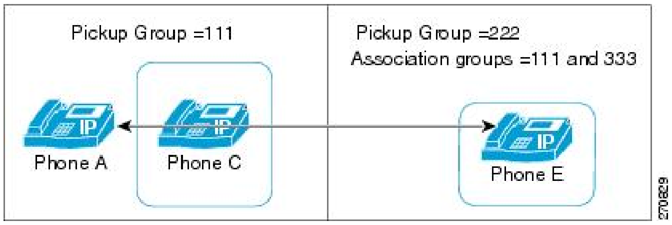
Figure 4: Basic Directed Call Pickup Setup



5. User A calls phone C, and phone C begins to ring.
6. User E presses the GPickUp softkey and enters DN of phone C, which is 1000.
7. Phone A and phone E connect, and phone C stops ringing.

The following figure shows the connection state between phone A and phone E after Directed Call Pickup completes.

Figure 5: Basic Directed Call Pickup Completes

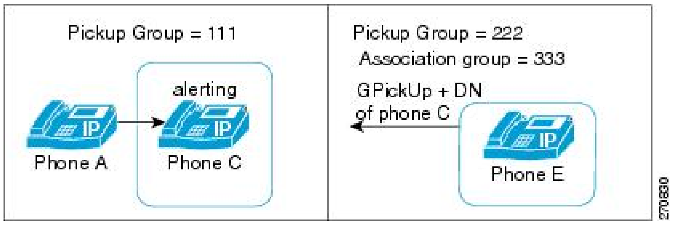


Directed Call Pickup Control Mechanism - Reject Example 1

This scenario illustrates the control mechanism that causes rejection of a Directed Call Pickup attempt. The following setup takes place, as shown in the following figure:

1. Three pickup groups that are created comprise group numbers 111, 222, and 333.
2. Pickup group 222 includes association group 333.
3. DN of phone C specifies 1000 in pickup group 111.
4. DN of phone E specifies 2000 in pickup group 222.

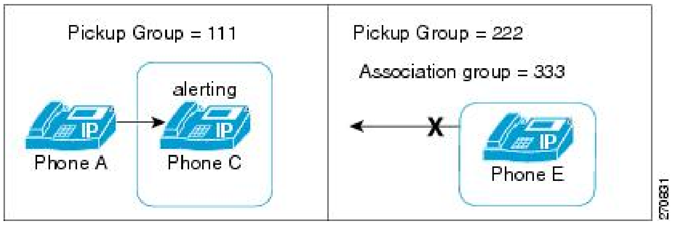
Figure 6: Directed Call Pickup Setup 1 That Leads to Rejection



5. User A calls phone C, and phone C begins to ring.
6. User E presses the GPickUp softkey and enters DN of phone C, which is 1000.
7. The Directed Call Pickup attempt for phone E gets rejected because the pickup group of phone E, 222, does not have group 111 in its association list.

The following figure shows the connection state between phone A and phone E after Directed Call Pickup fails.

Figure 7: Directed Call Pickup Gets Rejected, Example 1

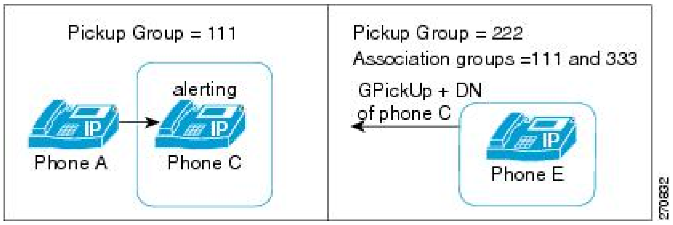


Directed Call Pickup Control Mechanism - Reject Example 2

This scenario illustrates the control mechanism that causes rejection of a Directed Call Pickup attempt. The following setup takes place, as shown in the following figure:

1. Three pickup groups that are created comprise group numbers 111, 222, and 333.
2. Pickup group 222 includes association groups 111 and 333.
3. DN of phone C specifies PT_C/1000 in pickup group 111, and PT_C specifies the partition of phone C.
4. DN of phone E specifies PT_E/2000 in pickup group 222, PT_E specifies the partition of phone E, and the Calling Search Space (CSS) of phone E specifies PT_E.

Figure 8: Directed Call Pickup Setup 2 That Leads to Rejection

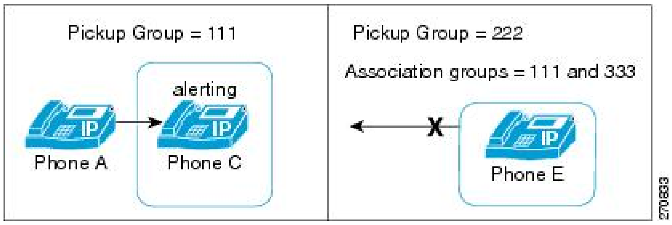


5. User A calls phone C, and phone C begins to ring.
6. User E presses the GPickUp softkey and enters DN of phone C, which is 1000.

7. The Directed Call Pickup attempt for phone E gets rejected because the CSS of phone E does not contain the partition of phone C.

The following figure shows the connected state between phone A and phone E after Directed Call Pickup fails.

Figure 9: Directed Call Pickup Gets Rejected, Example 2

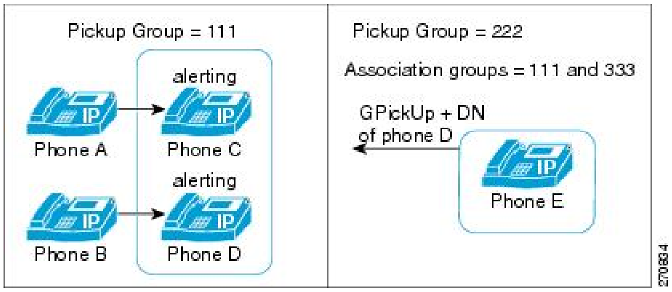


Directed Call Pickup Control Mechanism - Multiple Calls

This scenario illustrates Directed Call Pickup when multiple calls are available for pickup. The following setup takes place, as shown in the following figure:

1. Three pickup groups that are created comprise group numbers 111, 222, and 333.
2. Pickup group 222 includes association groups 111 and 333.
3. DN of phone C specifies 1000, DN of phone D specifies 3000, and both phones reside in pickup group 111.
4. DN of phone E specifies 2000 in pickup group 222.

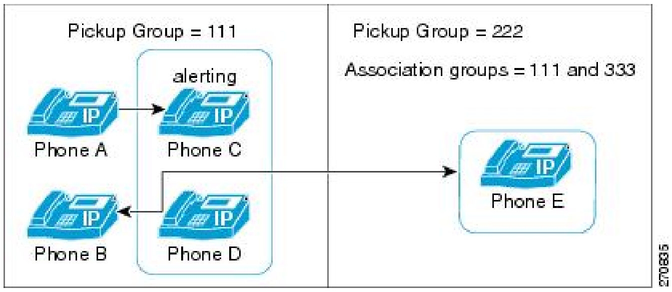
Figure 10: Directed Call Pickup Setup with Multiple Calls



5. User A calls phone C, and user B calls phone D. Phone C and phone D begin to ring.
6. User E presses the GPickUp softkey and enters DN of phone D, which is 3000.
7. Phone B and phone E connect, and phone D stops ringing.

The following figure shows the connection state between phone B and phone E after Directed Call Pickup completes.

Figure 11: Directed Call Pickup with Multiple Calls Completes



Busy Lamp Field Call Pickup

You can associate the busy lamp field (BLF) button on a Cisco Unified IP Phone to a DN. This allows Cisco Unified Communications Manager to notify a phone user when a call is waiting to be picked up from the DN. The DN represents the BLF DN, and the phone that picks up the call to the BLF DN represents the BLF call pickup initiator.

The following rules apply to the BLF DN and the BLF call pickup initiator:

- The BLF call pickup initiator gets 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 call pickup is configured 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.

Note You can optionally configure an audible alert in addition to the visual alert.

The following actions take place for an incoming call to the BLF DN:

1. The BLF SD button flashes on the BLF call pickup initiator phone to indicate that an incoming call to the BLF DN exists.
2. 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.

BLF Call Pickup Example

This scenario illustrates BLF call pickup. The following elements are configured:

- Group 111 represents a call pickup group that includes the BLF DN (phone B), an outside phone (phone A), and other phones.
- Group 222 represents a call pickup group that is associated to Group 111. Group 222 includes phone C.
- Phone A represents an outside phone.
- Phone B represents the BLF DN phone in Group 111.
- Phone C represents a user phone in Group 222 that has the BLF SD button configured to monitor the phone B BLF DN and has call pickup enabled. It represents the BLF call pickup initiator phone.

When a call from phone A comes in to phone B, the BLF SD button on phone C lights. The user at phone c presses the button and connects to the phone A caller.

If a hunt list pilot number is configured as part of Group 111, a call from phone A to the hunt group causes the BLF SD button on phone c to light, and the user at phone C can press the button to connect to the caller at phone A.

Auto Call Pickup

You can automate call pickup, group pickup, other group pickup, directed call pickup, and BLF call pickup by enabling the Auto Call Pickup Enabled service parameter.

When this parameter is enabled, Cisco Unified Communications Manager automatically connects users to the incoming call in their own pickup group, in another pickup group, or a pickup group that is associated with their own group after users press the appropriate softkey on the phone. This action requires only one keystroke.

Auto call pickup connects the user to an incoming call in the group of the user. When the user presses the PickUp softkey on the phone, Cisco Unified Communications Manager locates the incoming call in the group and completes the call connection. If automation is not enabled, the user must press the softkeys, PickUp and Answer, to make the call connection.

Auto group call pickup connects the user to an incoming call in another pickup group. The user presses the GPickUp softkey on the phone, then dials the group number of another pickup group. Upon receiving the pickup group number, Cisco Unified Communications Manager completes the call connection. 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.

Auto other group pickup connects the user to an incoming call in a group that is associated with the group of the user. The user presses the OPickUp softkey on the phone. Cisco Unified Communications Manager automatically searches for the incoming call in the associated groups in the sequence that the administrator enters in the Call Pickup Group Configuration window and completes the call connection after the call is found. If automation is not enabled, the user must press the softkeys, OPickUp and Answer, to make the call connection.

Auto directed call pickup connects the user to an incoming call in a group that is associated with the group of the user. The user presses the GPickUp softkey on the phone, then dials the DN of the ringing phone. Upon receiving the DN, Cisco Unified Communications Manager completes the call connection. 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.

Note CTI applications support monitoring the party whose call is picked up. CTI applications do not support monitoring the pickup requester or the destination of the call that is picked up. Hence, Cisco Unified Communications Manager Assistant does not support auto call pickup (one-touch call pickup).

Note Auto call pickup interacts with Cisco Unified Mobility features on a limited basis. See Interactions, on page 258 in the Cisco Unified Communications Manager Features and Services Guide for details.

Call Pickup No Answer

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 Busy

When a call pickup occurs with the service parameter Auto Call Pickup Enabled set to false, the original call gets restored while the call pickup requestor phone is busy.

Call Pickup No Bandwidth

When a call pickup occurs with the service parameter Auto Call Pickup Enabled set to false, the original call gets restored when no bandwidth exists between the call originator and requestor phones.

Use Call Pickup Features with Hunt Lists

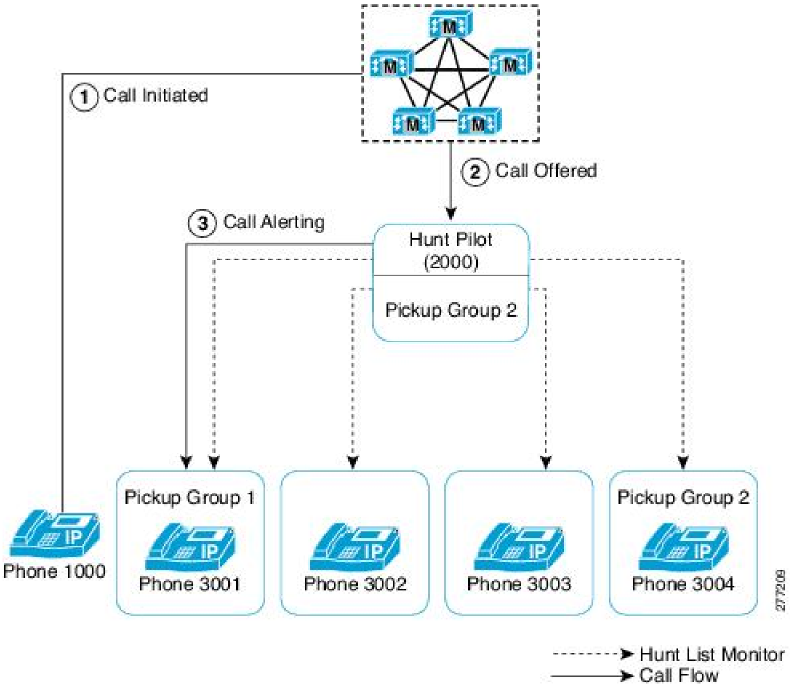
You can assign a call pickup group to a hunt pilot DN. Doing this affects how call pickup works. Users can pick up calls that are alerting in the line group members. If call pickup group notification is enabled, calls alerting in line group members get notified to the devices that are associated with the same call pickup group.

The service parameter “Allow Calls to be picked up from Line Group Members” controls this behavior. When this service parameter is set to False (the default), when line group members are included as part of a call pickup group, calls alerting in the line group members cannot be picked up from other call pickup group members. This is the same behavior as in Cisco Unified Communications Manager releases before this service parameter got added.

When the service parameter “Allow Calls to be picked up from Line Group Members” is set to True, any call pickup group configuration at the hunt pilot gets ignored. Alerting calls at the hunt list will neither get notified for pick up to the hunt pilot's call pickup group, nor will those calls get picked up. When the service parameter “Allow Calls to be picked up from Line Group Members” is set to False, any call pickup group configuration at the line group members gets ignored.

The following figures provide examples of the effects of this configuration.

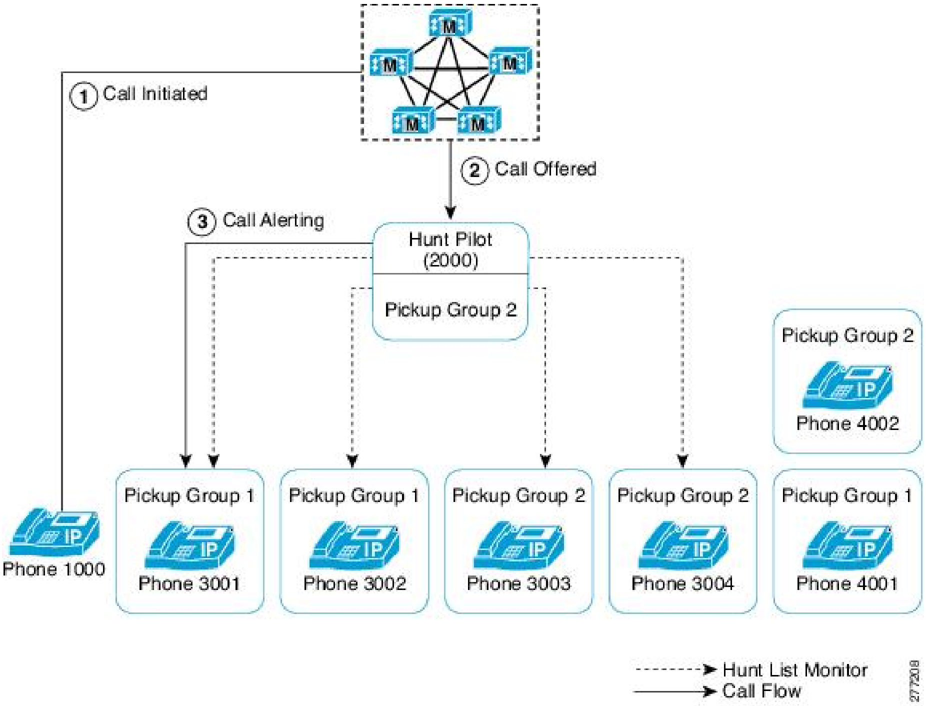
Figure 12: Using Call Pickup Features with Hunt Lists Example 1



In the previous figure, when the service parameter “Allow Calls to be picked up from Line Group Members” is set to True, calls alerting at Phone 3002 or Phone 3003 cannot get picked up even though Hunt Pilot (2000) is in Pickup Group1. If the service parameter is set to False, calls alerting at 3001, 3002, 3003 or 3004 can get picked up from members associated with Pickup Group 1.

When the service parameter “Allow Calls to be picked up from Line Group Members” is set to True, if both hunt pilot and line group members are included in a call pickup group, only line group members' call pickup group will be notified of calls available for pick up. Also calls alerting in the line group members can be picked up by lines associated with the same call pickup group as the line group members.

Figure 13: Using Call Pickup Features with Hunt Lists Example 2



In the previous figure, when the service parameter “Allow Calls to be picked up from Line Group Members” is set to True, calls alerting at Phone 3001 or Phone 3002 get notified to all of the members associated with Pickup Group 1: 3001, 3002 and 4001. If the service parameter is set to False, calls alerting at 3001, 3002, 3003 or 3004 get notified to 3003, 3004 and 4002.

When the service parameter “Allow Calls to be picked up from Line Group Members” is set to True, calls alerting at the line group members will be notified for pickup. But the pickup notification timer gets reset every time the call moves from one member to another. This results in multiple pickup notifications (to corresponding pickup group members) for the same call as it moves from one line group member to another. This notification gets provided if the “old” and “new” alerting line group member is in the same or different call pickup group. Call pickup notifications include the caller and the line group member information.

When the service parameter “Allow Calls to be picked up from Line Group Members” is set to True, the longest alerting call gets determined by the amount of time a call has been alerting in one specific call pickup group. If the call moves to another line group member that is in another call pickup group, the longest alerting timer gets reset. Also, if the call moves to another line group member that is not in any call pickup group, the longest alerting timer is reset.

Broadcast call distribution algorithm is not supported for calls to be picked up from line group members when the “Allow Calls to be picked up from Line Group Members” is enabled.

Use Call Pickup Features with Partitions

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.

- If call pickup group numbers are assigned 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 the pickup groups are assigned to the appropriate partition for each tenant.

A multitenant configuration provides an example of using partitions with call pickup groups. Assign the pickup groups to the appropriate partition for each tenant, and the group number will not be visible to other tenants.

With the Directed Call Pickup feature, 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.

Call Pickup Notification

The Call Pickup Notification feature provides an audio or visual, or both, notification on Cisco Unified IP Phones when other members of a pickup group receive a call. Call Pickup Notification gets configured in three configuration windows for three types of settings: system, call pickup group, DN/phone.

- Service Parameters Configuration - The type of audio notification (beep or ring) to be heard when a phone is idle or busy gets set from the Service Parameters Configuration window. This setting becomes the system default.
- Call Pickup Group Configuration - The type of notification for each call pickup group gets configured from the Call Pickup Group Configuration window in Cisco Unified Communications Manager Administration. In addition to configuring the type of notification, you can configure the time, in seconds, to delay the audio and visual alerts after the call comes into that group. This allows the original called party a chance to pick up the call prior to the audio and/or visual alert being sent to the pickup group. See the Call Pickup Group Configuration, on page 172.
    - To configure whether the notification will be audio or visual, or both, use the configuration settings in the Call Pickup Group Notification Settings section of the Call Pickup Group Configuration window. The notification gets sent only to the primary line of a device.
    - To configure the visual notification on the Call Pickup Group Configuration window, use the configuration settings in the Call Information Display For Call Pickup Group Notification section. This setting allows the administrator to have detailed calling party and/or called party information in the notification message. The display will contain the name of calling/called party if available. If not, the number will display. The visual notification comprises a message on the phone status line.
- Directory Number Configuration - This window provides fields where you can configure the audio alert setting for each phone. Configure the type of audio alert for phones by using the Pickup Audio Alert Setting. This lets users configure the type of audio alert to be provided when phone is idle or has an active call. See the Cisco Unified Communications Manager Administration Guide.

Keep in mind that call pickup notification can get sent to the other members of a pickup group only when a member of the pickup group receives an incoming call.

System Requirements for Call Pickup

To operate, call pickup requires the following software and hardware components:

- Cisco Unified Communications Manager
- Cisco Unified IP Phone that supports Call Pickup

The following table lists the Cisco Unified IP Phones that support Call Pickup.

Table 22: Cisco Unified IP Phones That Support Call Pickup

Cisco Unified IP Phone Model	Call Pickup Feature	Softkey	Button
Cisco Unified IP Phone 6900 Series (except 6901) Cisco Unified IP Phone 6911 does not support softkeys; the system administrator configures a feature number for Call Pickup, and the user presses the feature key and then dials the call pickup feature number.	Call Pickup Group Pickup Other Pickup Directed Call Pickup	X	X
Cisco Unified IP Phone 7900 Series	Call Pickup Group Pickup Other Pickup Directed Call Pickup	X	X
Cisco Unified IP Phone 8900 Series	Call Pickup Group Pickup Other Pickup Directed Call Pickup	X	X
Cisco Unified IP Phone 9900 Series	Call Pickup Group Pickup Other Pickup Directed Call Pickup	X	X

Note For the 3500 Cisco Unified IP Phone, the Call Pickup feature is activated using the menu.

For more information about Cisco Unified IP Phones and Call Pickup, see the user guides for your phone model.

Note The administrator must add the Other Pickup (OPickUp) softkey to the softkey templates. Configure Call Pickup, Group Call Pickup, Other Pickup, and Directed Call Pickup on the phone button template by using the programmable line key feature (see the *Cisco Unified Communications Manager System Guide*).

Interactions and Restrictions

This section describes the interactions and restrictions for call pickup.

Interactions

This section describes how call pickup interacts with Cisco Unified Communications Manager applications and call processing features.

Route Plan Report

The route plan report displays the patterns and DNs that are configured in Cisco Unified Communications Manager. Use the route plan report to look for overlapping patterns and DNs before assigning a DN to call pickup group. See the Cisco Unified Communications Manager Administration Guide.

Calling Search Space and Partitions

Assign a partition to the Call Pickup Group number to limit call pickup access to users on the basis of the device calling search space. See topics related to Calling Search Space configuration in the *Cisco Unified Communications Manager Administration Guide*.

Time of Day

To pick up calls from a group that is associated with your own group, you must configure the calling search space, partition, and the Time of Day (TOD) parameter for members in the associated group to be active and able to accept calls within the same time period as your own group. TOD associates a time stamp to the calling search space and partition.

For example, a partition, ABC, remains active between 9 am to 5 pm. A calling search space, cssABC, contains partition ABC. A pickup group, pickABC contains phone 1 and phone 2. Phone 1 and phone 2 reside in the same calling search space, cssABC. If phone 1 rings at 5:30 pm and phone 2 tries to pick up the call, this attempt fails because the partition is not active after 5 pm. If phone 1 rings at 9:30 am, phone 2 can pick up the call.

Call Accounting

Call pickup features interact with call accounting.

- When a call pickup occurs via 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 as specified. If users are interested in the 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.

Dependency Records

If you need to find devices to which a specific call pickup number is assigned, click the Dependency Records link that the Cisco Unified Communications Manager Administration Call Pickup Group Configuration window provides. The Dependency Records Summary window displays information about devices that are using the call pickup number.

If a pickup group is associated with other pickup groups, the dependency record of the pickup group shows the association information. For example, if pickup group A is associated with pickup group B and pickup group C, the dependency record of pickup group A shows the information on the association of pickup group A to pickup groups B and C.

To find out more information about the devices, click the device, and the Dependency Records Details window displays. If the dependency records are not enabled for the system, the dependency records summary window displays a message.

For more information about Dependency Records, see the *Cisco Unified Communications Manager Administration Guide*.

Restrictions

The following restrictions apply to call pickup group:

- Although different lines on a phone can be assigned to different call pickup groups, Cisco does not recommend this setup because it can be confusing to users.
- 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. 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.
- The system does not support call pickup notification, audio, and visual alert on Cisco Unified IP Phones 7940 and 7960 that are running SIP.
- Call pickup notification, audio, and visual alert only supports licensed, third-party phones that are running SIP.
- Users cannot pick up calls to a DN that belongs to a line group by using the Directed Call Pickup feature.
- If a device belongs to a hunt list and the device 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.

The following restriction applies to BLF call pickup:

- The configuration is available for you to configure a URI BLF pickup, but you cannot invoke it.

Install and Activate Call Pickup

Call pickup, a system feature, comes standard with Cisco Unified Communications Manager software. It does not require special installation.

Configure Call Pickup Features

This section contains information about setting the service parameters for Call Pickup.

Tip Before you configure call pickup, review topics related to configuring Call Pickup, group Call Pickup, Other Group Pickup, Directed Call Pickup, and BLF Call Pickup.

Related Topics

Configure BLF Call Pickup, on page 153
Configure Call Pickup and Group Call Pickup, on page 147
Configure Directed Call Pickup, on page 151
Configure Other Group Pickup, on page 149

Set the Service Parameters for Call Pickup

Cisco Unified Communications Manager provides the following clusterwide service parameters for call pickup features. Each service parameter includes a default and requires no special configuration.

- Auto Call Pickup Enabled - Default specifies False. This parameter determines whether the auto call pickup feature is enabled. To enable this capability, set the field to True.
- Call Pickup Locating Timer - Default specifies 1 second. This service parameter specifies the maximum time, in seconds, for a pickup to wait to get all alerting calls in the pickup groups.
- Call Pickup No Answer Timer - Default specifies 12 seconds. This required parameter specifies the maximum time, in seconds, to wait before restoring the original call if a user, who initiates a pickup request, decides not to pick up the call.

Note To set the timers, choose **System** > **Service Parameters**, choose the **Advanced** icon or click the **Advanced** button, and update the fields in the Clusterwide Parameters (Feature-Call Pickup) pane.

- Allow Calls to be picked up from Line Group Members - Default specifies False. When this parameter is set to True, any call pickup group configuration at the hunt pilot gets ignored. Alerting calls at the hunt list will neither get notified for pick up to hunt pilot's call pickup group, nor will those calls get picked up. When this parameter is set to False, any call pickup group configuration at the line group members gets ignored. For more information about the effect of this service parameter, see the Use Call Pickup Features with Hunt Lists, on page 163.

Configure Call Pickup Groups

This section contains information to configure Call Pickup groups, define a pickup group for Other Group Pickup, Delete a Call Pickup group, and to assign a Call Pickup group to directory numbers.

Tip Before you configure call pickup, review the summary steps to configure the following:

- Call Pickup and Group Call Pickup
- Other Group Pickup
- Directed Call Pickup
- BLF Call Pickup

Related Topics

Configure BLF Call Pickup, on page 153
Configure Call Pickup and Group Call Pickup, on page 147
Configure Directed Call Pickup, on page 151
Configure Other Group Pickup, on page 149

Find a Call Pickup Group

The Find and List window for call pickup group allows you to search for call pickup groups that you have configured in Cisco Unified Communications Manager Administration.

Because you may have several call pickup groups in your network, Cisco Unified Communications Manager lets you locate call pickup groups on the basis of specific criteria. Use the following procedure to locate call pickup groups.

Note During your work in a browser session, Cisco Unified Communications Manager Administration retains your call pickup group search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your call pickup group search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Call Routing** > **Call Pickup Group**.

The Find and List Call Pickup Groups window displays.

Step 2 To filter or search records,

a) From the first drop-down list box, choose a search parameter.
b) From the second drop-down list box, choose a search pattern.
c) Specify the appropriate search text, if applicable.

Note To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criteria or click the Clear Filter button to remove all added search criteria.

Step 3 To find all records in the database, ensure the dialog box is empty; click **Find**.

All or matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

Note You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking **Delete Selected**. You can delete all configurable records for this selection by clicking **Select All** and then clicking **Delete Selected**.

Step 4 From the list of records that display, click the link for the record that you want to view.

Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Configure a Call Pickup Group

This section describes how to add, copy, and update a single call pickup group.

Procedure

Step 1 Choose **Call Routing** > **Call Pickup Group**.

Step 2 Perform one of the following tasks:

a) To add a new Call Pickup Group, click **Add New**.
b) To copy a Call Pickup Group, use the procedure in the Configure Call Pickup Groups, on page 171 to locate the call pickup group. Click the **Copy** icon.
c) To update a Call Pickup Group, use the procedure in the Configure Call Pickup Groups, on page 171 to locate the call pickup group.

The Call Pickup Group Configuration window displays.

Step 3 Enter or update the appropriate settings as described in Call Pickup Group Configuration, on page 172.

Step 4 To save the new or changed call pickup groups in the database, click **Save.**

Call Pickup Group Configuration

The Call Pickup feature allows users to pick up incoming calls within their own group. Cisco Unified Communications Manager automatically dials the appropriate call pickup group number when the user activates this feature from a Cisco Unified IP Phone. Use the softkey, PickUp, for this type of call pickup.

The Group Call Pickup feature allows users to pick up incoming calls in another group. User 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.

Note The same procedures apply for configuring call pickup and group call pickup features. Group call pickup numbers apply to lines or directory numbers.

The following table describes the call pickup group configuration settings.

Table 23: Call Pickup Group Configuration Settings

Field	Description
Call Pickup Group Information	
Call Pickup Group Name	Enter up to 100 alphanumeric characters. For example, Operations. The pickup group name associates with the pickup group number. You can choose a pickup group by the pickup group name.
Call Pickup Group Number	Enter a unique directory number (integers) for the call pickup group that you want to add. Enter up to 24 digits. The following characters are allowed: numeric (0 to 9), A through D, plus (+), pound (#), and asterisk (*). If a number begins with the international escape character (+), you must precede the + with a backslash (\).
Description	Enter a description for the call pickup group (for example, Operations Department Group Pickup).

Field	Description
Partition	If you want to use a partition to restrict access to the call pickup group, choose the desired partition from the drop-down list box. If you do not want to restrict access to the call pickup group, choose <None> for the partition. You can configure the number of partitions that display 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 displays next to the drop-down list box. Click the Find button to display the Find and List Partitions window. For more information, see topics related to searching for a partition in the *Cisco Unified Communications Manager Administration Guide*. **Note** To set the maximum list box items, choose **System** > **Enterprise Parameters** and choose **CCMAdmin Parameters**. **Note** Make sure that the combination of call pickup group number and partition is unique within Cisco Unified Communications Manager.
Call Pickup Group Notification Settings	
Call Pickup Group Notification Policy	From the drop-down list box, choose one of the following notification types: • No Alert • Audio Alert • Visual Alert • Audio and Visual Alert
Call Pickup Group Notification Timer (seconds)	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 to occur.
Call Information Display For Call Pickup Group Notification	

Field	Description
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. If you choose to display both Calling Party Information and Called Party Information, only the first 11 characters of each display. If you choose to display only one or the other, the first 23 characters display. **Note** In the case of multiple active notification alerts, the latest visual alert overwrites the previous ones. When a user activates call pickup, the user connects to the earliest call that is available for pickup, even if that visual alert does currently display on the phone. You can avoid this mismatch by using visual notification without displaying calling or called party information. With this configuration, a generic message reading, “Call(s) available for Pickup” displays. The user can obtain the caller identification if Auto Call Pickup (AutoCallPickupEnabled service parameter) is disabled; see the Auto Call Pickup, on page 162 for more information.

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. If you choose to display both Calling Party Information and Called Party Information, only the first 11 characters of each display. If you choose to display only one or the other, the first 23 characters display. **Note** In the case of multiple active notification alerts, the latest visual alert overwrites the previous ones. However, when a user activates call pickup, the user connects to the earliest that is call available for pickup, even if that visual alert does not currently display on the phone. You can avoid this mismatch by using visual notification without displaying calling or called party information. With this configuration, a generic message reading, “Call(s) available for Pickup” displays. The user can obtain the caller identification if Auto Call Pickup (AutoCallPickupEnabled service parameter) is disabled; see the Auto Call Pickup, on page 162 for more information.
Associated Call Pickup Group Information - Find Pickup Numbers by Numbers/Partition	
Partition	See Partition in Call Pickup Group Information in this table.
Call Pickup Group Numbers Contain	Enter the DN or part of the DN of the call pickup group that you want to find; then, click Find.
Available Call Pickup Groups	To add a member to the associated call pickup group list in the Current Associated Call Pickup Groups area, choose a DN/partition from this list; then, click Add to Associated Pickup Groups. The group that is being configured automatically gets added to the list of Current Associated Call Pickup Groups. This allows pickup of calls within your own group by using the OPickUp softkey.
Associated Call Pickup Group Information - Current Associated Call Pickup Groups	

Field	Description
Selected Call Pickup Groups	To change order of the Call Pickup Groups listings, use the Up and Down arrows on the right side of this box to move the listings. Click Reverse Order of Selected Numbers to reverse the order of the listings. Use the Up and Down arrows below this box to move a call pickup group from this box to the Removed Call Pickup Groups box.
Removed Call Pickup Groups	Use the Up and Down arrows above this box to move a call pickup group from this box to the Selected Call Pickup Groups box.

Related Topics

Call Pickup, on page 147

Call Pickup Feature, on page 155

Delete a Call Pickup Group

This section describes how to delete a call pickup group from the Cisco Unified Communications Manager database.

Before you begin

You cannot delete a call pickup group number that is assigned to a line or directory number. To see a list of the directory numbers that are using this call pickup group, click the Dependency Records link. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about Dependency Records, see the Auto Call Pickup, on page 162 section in the Cisco Unified Communications Manager Administration Guide. To enable call pickup again for those directory numbers, you must reassign each of them to a new call pickup group. For details, see the Assign a Call Pickup Group to Directory Numbers, on page 178.

Procedure

Step 1 Locate the call pickup group by using the procedure in the Configure Call Pickup Groups, on page 171.

Step 2 Click the call pickup group that you want to delete.

Step 3 Click **Delete**.

The call pickup group no longer displays in the Find and List Call Pickup Groups window.

Define a Pickup Group for Other Group Pickup

This section describes how to associate a call pickup group to your group for answering incoming calls for this associated group. You can associate up to 10 call pickup groups with your group. The priority of answering calls for the associated groups goes from the first associated group to the last associated group on the associated group list. You can organize the list in the Call Pickup Group Configuration window.

Procedure

Step 1 Locate your group by using the procedure in the Configure Call Pickup Groups, on page 171.

Step 2 In the Call Pickup Group Configuration window, scroll down to the Associated Call Pickup Group Information area.

Step 3 Enter information in the appropriate fields as described in Call Pickup Group Configuration, on page 172.

Step 4 Click **Save.**

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.

Before you begin

Before you can assign a call pickup group to a directory number, you must create the call pickup group as described in the Configure a Call Pickup Group, on page 172.

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 on 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 box 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.**

Assign a Call Pickup Group to Hunt Pilots

This section describes how to assign a call pickup group to a hunt pilot. 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.

Before you begin

Before you can assign a call pickup group to a hunt list, you must create the call pickup group as described in the Configure a Call Pickup Group, on page 172.

Procedure

Step 1 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 displays.

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 box that displays in the Hunt Forward Settings area, choose the desired call pickup group.

Step 5 To save the changes in the database, click **Save.**

Related Topics

Use Call Pickup Features with Hunt Lists, on page 163

CHAPTER 8

Call Queuing

Set Up Call Queuing

This procedure lists the tasks used to configure the Call Queuing feature. For more information on the Call Queuing feature, see the Introducing Call Queuing section.

Procedure

Step 1 Configure customized announcements

For more information, see topics related to announcement configuration in the *Cisco Unified Communications Manager Administration Guide*.

Step 2 Add custom announcements. This includes:

- Uploading wav file announcements
- Viewing and/or changing customized announcements

For more information, see topics related to announcement configuration in the *Cisco Unified Communications Manager Administration Guide*.

Step 3 Configure the Music On Hold (MoH) source

For more information, see Music On Hold in the *Cisco Unified Communications Manager Features and Services Guide*.

Step 4 Configure queuing capability for a Hunt Pilot number

For more information, see Hunt Pilot configuration in the *Cisco Unified Communications Manager Administration Guide*.

Step 5 Configure Line Group setting page for Automatically Logout Hunt Member on No Answer.

For more information, see Line group settings in the *Cisco Unified Communications Manager Administration Guide*.

Call Queuing Considerations

Unified CM provides call queuing natively to users so that callers can be held in a queue until hunt members are available to answer them. Callers in a queue receive an initial greeting announcement followed by music on hold or tone on hold. If the caller remains in queue for a period of time, a secondary announcement is played at a configured interval until the call can be answered—or until the maximum wait timer expires.

Call Queuing Operation

Cisco Unified Communications Manager Administration Considerations

The Call Queuing feature provides an enhanced capability to handle incoming calls to a hunt pilot number. When an incoming call reaches the hunt pilot, the following capabilities are provided:

- A caller may be connected to an initial customizable greeting announcement before proceeding
- If one or more line members are logged into the hunt pilot and are in an idle state, and if no calls are queued, then the call is extended to the line member that has been idle for the longest period of time
- If no line members answer a call, then that caller will not be placed in queue. The call is routed to a new destination, or disconnected, based on the setting under "When no hunt members answer, are logged in, or registered"
- Calls will be placed in queue only if all members are busy.
- If a line member does not answer a queue-enabled call, that line member is logged off the hunt group only if the setting "Automatically Logout Hunt Member on No Answer" is selected on the line group page
- While the caller is in the queue they may hear Music On Hold and a repeating (customizable) periodic announcement
- Once a line member becomes idle, the caller with the longest wait time across multiple hunt groups is extended to the idle line member. If the idle line member does not answer the call, the caller is returned to their previous position in the queue
- If a queued call exceeds its maximum wait time, it can be routed to another pattern or it can be disconnected, depending upon how the hunt pilot configuration is configured
- If the maximum number of callers allowed in queue has been reached, any subsequent caller can be routed to another pattern or disconnected, depending upon how the hunt pilot configuration is configured
- Line members can display the queue status of their queue-enabled hunt pilots (in other words, the hunt pilots with which they are associated). The queue status display provides the following types of information:
    - Hunt pilot pattern
    - Number of queued callers on each hunt pilot
    - Longest waiting time

Note You can configure a maximum of 25 hunt pilots per hunt list in Call Queuing. If you exceed this limit, the queue status will not be displayed.

For shared-line deployments, the availability of all devices with that shared-line are combined to provide a final status. If a shared-line device for one or members appears as on-hook, but all others are indicating off-hook, the final status for that line member remains off-hook.

Call queuing works in conjunction with existing hunt pilots, but there are no changes in the behavior of the hunting mechanism for either queuing or non-queuing hunt pilots. There are, however; specific features associated with hunt pilots that have call queuing enabled:

1. Queuing-enabled hunt pilot calls can only be received by line members one call at a time. Two queuing-enabled hunt pilot calls cannot be offered to a line member (no matter what the busy trigger is set to). This does not limit a line member to only receive calls directly to their DN or from non-queuing hunt pilots.
2. Line members who do not answer hunt pilot routed calls are automatically logged out. A line member is automatically logged out of a device if the line member receives a queuing-enabled hunt pilot call and does not answer the call until an RNA reversion time-out occurs. In the case of a shared-line deployment, all devices configured with the same shared-line are logged out. This behavior can be configured from the Line group page setting "Automatically Logout Hunt Member on No Answer" - line members are logged out only if this has been set.

While the calling party is in queue, the caller receives a MoH treatment depending upon the network MoH settings for that hunt pilot. There is option available to play the initial announcement first and then offer a call to a hunt pilot. If the call is not answered by any of the line members, the caller is placed on hold (in queue) with an announcement provided periodically in addition to MoH. The second option involves offering the call to a hunt pilot DN first, and then place caller on hold (in queue) if the call is not answered. Again, an announcement is provided periodically in addition to MoH. When a line member becomes available to answer the next caller in the queue, the call that has been in the queue the longest is offered to line member. If the line member does not answer the call, the caller is placed back in the queue at the same position.

Alternate Number Configuration

Call Queuing configuration provides for the routing of calls to an alternate number. These alternate numbers may be:

- A hunt pilot DN with queuing either enabled or disabled
- A voice mail DN
- A line DN
- A shared DN

There are three main scenarios where alternate numbers are used:

1. When queue is full
2. When maximum wait time is met
3. When no hunt members are logged in or registered

When queue is full

Call Queuing allows up to 100 callers to be queued per hunt pilot (the maximum number of callers allowed in queue on a hunt pilot page). Once this limit for new callers been reached on a particular hunt pilot, subsequent calls can be routed to an alternate number. This alternate number can be configured through the Hunt Pilot configuration page (through the “Destination When Queue is Full” settings).

When maximum wait time is met

Each caller can be queued for up to 3600 seconds per hunt pilot (the maximum wait time in queue). Once this limit is reached, that caller is routed to an alternate number. This alternate number can be configured through the Hunt Pilot configuration page (through the “Maximum wait time in queue” settings).

When no hunt members are logged in or registered

In a scenario where none of the members of the hunt pilot are available or registered at the time of the call, hunt pilot configuration provides an alternate number field (through the “When no hunt members are logged in or registered” settings) where calls can be routed. For Call Queuing, a hunt pilot member is considered available if that member has both deactivated do not disturb (DND) and logged into the hunt group. In all other cases, the line member is considered unavailable or logged off.

Music on Hold

MoH capabilities have been enhanced to play an optional initial greeting announcement when a caller is first put on hold and also to play a periodic repeating announcement when a caller is hearing the normal MoH audio. These announcements can use one of the Cisco-provided audio files or a custom file that is uploaded into the system.

Video on Hold (VoH) can be provided instead of MoH by including a VoH server in the Media Resource Group and Media Resource Group List configuration for the Held party. Only the default video configured for the VoH server is played if the VoH server is selected.

Real-time Monitoring

A number of new serviceability counters have been added to a folder called "Cisco Hunt Pilots" to monitor queuing. These counters, based on the Hunt Pilot DN, include:

- HuntPilot/QCallsAbandoned - the number of calls (since the last system reboot) which were queued, but disconnected, prior to being answered by a hunt member or redirected normally
- HuntPilot/CallsInQueue - the number of calls currently in queue
- HuntPilot/QCallsRingNoAnswer - the number of calls (since the last system reboot) which were not answered after being routed to a line group member
- HuntPilot/QLongestCallWaiting - the time, in seconds, of the call that currently has the longest wait time in queue
- HuntPilot/MaxQDepthExceeded - the number of occurrences (since the last system reboot) when a call was routed to an alternate destination after the maximum number of callers allowed in queue was reached
- HuntPilot/MaxQWaitTimerExceeded - the number of occurrences (since the last system reboot) when a call was routed to an alternate destination after the maximum wait time in queue was reached
- HuntPilot/LineGroupMembersAvailable - the number of idle (on-hook) line group members (DNs) currently eligible to receive calls from the queuing-enabled hunt pilot

Announcement Monitoring

The new performance counter for Media Streaming Annunciator can be reached from the Real Time Monitoring Tool via **Performance > expand server name > Cisco Media Streaming App > ANNPlayFailed**.

For more information, see the Cisco Unified Real Time Monitoring Tool Administration Guide.

Call Queuing System Requirements

Call Queuing requires the following software components:

- Cisco Unified Communications Manager 9.0 or later

- Cisco IP Voice Media Streaming (IPVMS) Application, which should be activated on at least one node in the cluster
- Cisco CallManager service that is running on at least one server in the cluster
- Cisco RIS Data Collector service that is running on the same server as the Cisco CallManager service
- Cisco Unified Communications Manager Locale Installer, that is, if you want to use non-English phone locales or country-specific tones

Call Queuing Interactions and Restrictions

SIP Rel1XX Options

If a call is routed to a queuing-enabled Hunt Pilot through SIP ICT, the SIP ICT uses the SIP Profile which has SIP Rel1XX Options set to "Send PRACK if 1XX contains SDP". As a result, the initial announcement is played to every call before the call is extended to the line member.

For more information, see SIP Profile Configuration, *Cisco Unified Communications Manager Administration Guide*.

Hunt Pilots and Hunt Groups

- The log off notification functionality for hunt groups changes when Call Queuing is enabled for a hunt pilot. The Hunt Group Logoff Notification does not play when a user logs out of a hunt group, or is logged off because they missed their turn in the queue, if Call Queuing is enabled for a hunt pilot.
- If the hunt list has multiple line groups then these line groups need to have the same setting for **Automatically Logout Hunt Member on No Answer**
- All Hunt options need to be set to Try Next Member, then Try Next Group in the hunt list.
- To avoid call looping, configure the secondary routing so that the call is not redirected back to same hunt pilot.

H323 Gateway and Trunk

If a call is routed to a queuing-enabled Hunt Pilot through the H323 gateway, the Service Parameter "Send H225 User Info Message" needs to be changed to "Use ANN for Ring Back" so that caller can hear ring back tone when the call is de-queued or routed to the alternate number.

Note In cases where queuing is used with H225 ICT, both clusters must be version 9.0 or above.

For more information, see H323 Gateway Configuration, Cisco Unified Communications Manager Administration Guide.

H323 Limitation

H323 Fast Start does not support Call Queuing.

Queue Status PLK

Queue status PLK is only supported with the following LCD display phones for both SCCP and SIP protocols:

- 6921
- 6941
- 6945
- 6961
- 7911 G
- 7931 G
- 7942 G
- 7945 G
- 7962 G
- 7965 G
- 7975 G
- 8961
- 8945
- 8941
- 9951
- 9971

HLOG PLK

You must configure phones that support hunt group logging in or out through HLOG softkey or PLK. If a phone does not support HLOG softkey or PLK, line members cannot log in from their phone.

Note HLOG is not compatible with EMCC, hence Call Queuing should not be deployed with EMCC.

For more information, see Log Out of Hunt Groups, Cisco Unified CM System Guide.

Mobility

Cisco Unified Communications Manager does not support Unified Mobility with Call Queuing.

Periodic Announcements

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

Performance and Scalability

- A single Unified CM Cluster supports a maximum of 15,000 hunt list devices.

- A single Unified CM Subscriber supports a maximum of 100 hunt pilots with call queuing enabled per node.
- Hunt list devices may be a combination of 1500 hunt lists with ten IP phones in each hunt list, 750 hunt lists with twenty IP phones in each hunt list, or similar combinations

Note When using the broadcast algorithm for call coverage, the number of hunt list devices is limited by the number of busy hour call attempts (BHCA). Note that a BHCA of 10 on a hunt pilot pointing to a hunt list or hunt group containing 10 phones and using the broadcast algorithm is equivalent to 10 phones with a BHCA of 10.

- The maximum number of simultaneous callers in queue for each hunt pilot that you can configure ranges from 1-100 (default 32).
- The maximum wait time in queue for each hunt pilot that you can configure ranges from 0-3600 seconds (default 900).
- An increase in the number of hunt lists can require you to increase the dial plan initialization timer that is specified in the Unified CM service parameters. Cisco recommends you to set the dial plan initialization timer to 600 seconds if you have 1500 hunt lists configured.
- Cisco recommends having no more than 35 directory numbers for a single line group when using broadcast algorithms with call queuing. Additionally, the number of broadcast line groups depends on the busy hour call completions (BHCC). If there are multiple broadcast line groups in a Unified CM system, the number of maximum directory numbers in a line group must be less than 35. The number of busy hour call attempts (BHCA) for all the broadcast line groups should not exceed 35 calls set up per second.

Troubleshoot Call Queuing

Use the Cisco Unified Serviceability Trace Configuration and Real Time Monitoring Tool to help troubleshoot call queuing problems. See the Cisco Unified Serviceability Administration Guide and the Cisco Unified Real Time Monitoring Tool Administration Guide.

CHAPTER 9

Call Throttling and the Code Yellow State

This chapter provides information about Call throttling which allows Cisco Unified Communications Manager to automatically throttle (deny) new call attempts when it determines that various factors, such as heavy call activity, low CPU availability to Cisco Unified Communications Manager, routing loops, disk I/O limitations, disk fragmentation or other such events, could result in a potential delay to dial tone (the interval users experience from going off hook until they receive dial tone).

Call Throttling Feature

Call throttling occurs automatically when Cisco Unified Communications Manager determines such conditions to be present, and the system exits throttling automatically when such conditions are alleviated. You can configure the parameters that are associated with entering and exiting call throttling through several service parameters in Cisco Unified Communications Manager Administration (**System** > **Service Parameters**) although Cisco does not advise modification of these parameters unless recommended by Cisco customer support. See topics related to service parameter configuration in the *Cisco Unified Communications Manager Administration Guide* for information on accessing and configuring service parameters.

Cisco Unified Communications Manager uses the values that are specified in the call-throttling-related parameters to evaluate the possibility of a delay to dial tone and also to determine when conditions no longer necessitate call throttling. When throttling is necessary to prevent excessive delay to dial tone, Cisco Unified Communications Manager enters a Code Yellow state, and new call attempts are throttled (denied). You can disable call throttling via the System Throttle Sample Size service parameter, but Cisco does not recommend disabling call throttling. The following list defines several of the call throttling-related service parameters:

- Code Yellow Entry Latency defines the maximum allowable delay, in milliseconds, to handle SDL messages that are sent to Cisco Unified Communications Manager by the various devices in the system as well as the wealth of internal messages that are received and sent by Cisco Unified Communications Manager for various activities such as KeepAlives, change notification, and many more types of internal messaging. If the calculated average expected delay is more than the value that is specified in this service parameter, Cisco Unified Communications Manager enters a Code Yellow state to initiate call throttling, and stops accepting new calls.

- Code Yellow Exit Latency Calculation determines the acceptable percentage of Code Yellow Entry Latency to specify exit criteria for leaving the Code Yellow state (Code Yellow exit latency) when Cisco Unified Communications Manager has initiated call throttling. The basis for the value that you specify in this parameter comprises a formula that uses the value in the Code Yellow Entry Latency parameter, which specifies the delay in milliseconds. To arrive at a percentage, use the following formula: Code Yellow Entry Latency value multiplied by the Code Yellow Exit Latency value. For example:

Code Yellow Entry Latency service parameter value: 20 msec

Code Yellow Exit Latency service parameter value: 40%

Code Yellow Exit Latency value = 20 X 0.4 = 8 msec, which means Cisco Unified Communications Manager exits Code Yellow state if the calculated message latency drops to 8 msec or lower.

To get out of the Code Yellow state, Cisco Unified Communications Manager ensures that the average expected delay is less than the value of the Code Yellow exit latency.

- Code Yellow Duration specifies the number of minutes that a Cisco Unified Communications Manager system can remain in a Code Yellow state (call throttling). If this duration is met and the system is still in Code Yellow state, Cisco Unified Communications Manager enters a Code Red state, which indicates that Cisco Unified Communications Manager has remained in a Code Yellow state for an extended period and cannot recover. When Cisco Unified Communications Manager enters a Code Red state, the Cisco CallManager service restarts, which also produces a memory dump that may be helpful for analyzing the failure.
- System Throttle Sample Size indicates the size of the sample, in seconds, that is used to calculate the average expected delay for Cisco Unified Communications Manager to handle an SDL message. For example, a sample size of 10 means that Cisco Unified Communications Manager must calculate a non-zero latency value for 10 consecutive seconds before it will calculate the average expected delay and compare it to the value in the CodeYellow Entry Latency parameter. You can disable call throttling via this parameter.

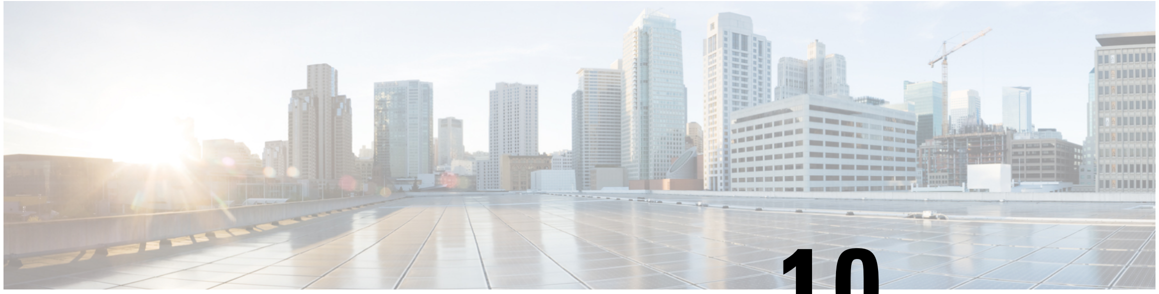
When delay to dial tone is calculated to be over the threshold that is configured in the call-throttling-related service parameters, Cisco Unified Communications Manager begins rejecting new calls. When call throttling is engaged, a user who attempts a new call will receive reorder tone and, depending on the phone model, may also receive a prompt on the phone display. Call throttling effectively avoids the problem in which a user tries to place a new call, but the length of delay between going off-hook and receiving dial tone is excessive enough to cause a reaction in the user (such as complaining to the system administrator or questioning whether the system is down or the phone is broken, for example). Cisco Unified Communications Manager uses a complex algorithm to constantly monitor the system to anticipate when such latency could occur.

When the delay to dial tone is within the guidelines of the call-throttling-related service parameters, Cisco Unified Communications Manager ceases throttling calls by exiting the Code Yellow state and new calls events are again allowed.

Troubleshooting Call Throttling

CCM/SDI and SDL trace files record call throttling events and can provide useful information. Also, you generally will require performance monitoring data for debugging. The Cisco CallManager System Performance object (viewable in the Real Time Monitoring Tool) includes a counter called ThrottlingSampleActivity, which indicates whether Cisco Unified Communications Manager has calculated a non-zero value for latency and helps you understand how busy the system is. Frequent non-zero values in this counter could indicate a potential overload condition on the system. To try to circumvent the possibility of a Code Yellow event, consider the possible causes of a system overload, such as heavy call activity, low CPU availability to Cisco Unified Communications Manager, routing loops, disk I/O limitations, disk fragmentation or other such events, and begin to investigate those possibilities.

Generally, repeated call throttling events require assistance from the Cisco Technical Assistance Center (TAC). TAC will likely request these trace files for closer examination.



CHAPTER 10

Calling Party Normalization

This chapter provides information about calling party normalization, in line with E.164 standards, which 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 displays on the phone.

Tip Configuring calling party normalization alleviates issues with toll bypass where the call is routed to multiple locations over the IP WAN. In addition, it allows Cisco Unified Communications Manager to distinguish the origin of the call to globalize or localize the calling party number for the phone user.

Configure Calling Party Normalization

In line with E.164 standards, 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 needing 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 displays on the phone.

Tip Configuring calling party normalization alleviates issues with toll bypass where the call is routed to multiple locations over the IP WAN. In addition, it allows Cisco Unified Communications Manager to distinguish the origin of the call to globalize or localize the calling party number for the phone user.

Before you begin

Before proceeding to globalize and normalize the calling party number, perform the following:

- Review the interactions and restrictions for this feature. For more information, see topics related to globalizing the calling party number, localizing the calling party number, interactions and restrictions.
- If you have not already done so, activate the Cisco CallManager service in Cisco Unified Serviceability. For more information, see the *Cisco Unified Serviceability Administration Guide*.

Procedure

Step 1 Perform the following steps to globalize and localize the calling party number:

a) To globalize the Calling Party Number, proceed to the next step.
b) To localize the Calling Party Number, go to step 9.

Step 2 If you want to do so, configure the Calling Party Number Type.

For more information, see topics related to globalizing the calling party number and configuring the calling party number type.

Step 3 For incoming national, international, subscriber, and unknown calls via the PSTN, create the prefixes that you want to associate with these types of calls. You create prefixes for device types; for example, phones, MGCP gateways, H.323 gateways/trunks, SIP trunks, and so on.

For more information, see topics related to globalizing the calling party number and setting the service parameters for calling party normalization.

Step 4 If your service provider prepends leading digits (for example, a zero) to the calling party number and you want to strip these digits before prepending other digits (for example, if the leading digits are not part of the E.164 number and you want to transform the calling party number to the E.164 format), you can configure the incoming calling party number settings for device pools, gateways, and trunks to ensure that Cisco Unified Communications Manager strips the leading digits before applying the prefixes to an incoming calling party number.

For more information, see topics related to applying the calling party transformation Calling Search Spaces (CSS) to localized the calling party number and incoming calling party number settings for device pools, gateways, and trunks.

Step 5 Create various partitions for the calling party transformation patterns under **Call Routing** > **Class of Control** > **Calling Search Space**.

Create different partitions and calling search spaces for different calling party transformation patterns and different number types, respectively. For more information, see topics related to partition configuration settings in the *Cisco Unified Communications Manager Administration Guide*.

Step 6 Create incoming calling party number calling search spaces (CSS) for the various calling party number types under **Call Routing** > **Class of Control** > **Calling Search Space**. In the Calling Search Space Configuration window for the CSS, move the partition that you created for the calling party transformation pattern to the Available Partitions pane. Perform this task for each CSS that you create.

You can create a CSS for the national calling party number type, a CSS for the international calling party number type, and so on. For more information, see topics related to CSS configuration settings in the *Cisco Unified Communications Manager Administration Guide*.

Step 7 Choose **Call Routing** > **Transformation Patterns** > **Calling Party Transformation Pattern** to create the Calling Party Transformation Pattern; in the Calling Party Transformation Pattern Configuration window, assign the partition that you associated with the incoming calling party transformation CSS to the calling party transformation pattern.

For more information, see topics related to calling party transformation pattern configuration settings in the *Cisco Unified Communications Manager Administration Guide*.

Step 8 Choose the appropriate Incoming Calling Party Transformation CSS in the device configuration window; for example, in the Gateway Configuration, SIP Trunk Configuration, and so on.

Tip To choose the incoming calling party number CSS in the device configuration window, configure the Calling Search Space settings for the calling party number types in the Incoming Calling Party Number Settings pane.

For more information, see topics related to applying the calling party transformation CSS to localize the calling party number.

The Calling Party Number is now globalized.

Step 9 Create a partition for the calling party transformation pattern under **Call Routing** > **Class of Control** > **Calling Search Space**.

For more information, see topics related to partition configuration settings in the *Cisco Unified Communications Manager Administration Guide*.

Step 10 Create the Calling Party Transformation calling search space (CSS) under **Call Routing** > **Class of Control** > **Calling Search Space**; in the Calling Search Space Configuration window for the calling party transformation CSS, move the partition that you created for the calling party transformation pattern to the Available Partitions pane.

For more information, see topics related to CSS configuration settings in the *Cisco Unified Communications Manager Administration Guide*.

Step 11 Choose **Call Routing** > **Transformation Patterns** > **Calling Party Transformation Pattern** to create the Calling Party Transformation Pattern; in the Calling Party Transformation Pattern Configuration window, assign the partition that you associated with the calling party transformation CSS to the calling party transformation pattern.

For more information, see topics related to calling party transformation pattern configuration settings in the *Cisco Unified Communications Manager Administration Guide*.

Step 12 Choose the Calling Party Transformation CSS in the device configuration window; for example, in the Gateway Configuration, Phone Configuration, Trunk Configuration, and the CTI Route Point Configuration window.

Tip To choose the Calling Party Transformation CSS in the device configuration window, configure the Calling Party Transformation CSS setting (not the Calling Search Space setting). If you want the device to use the Calling Party Transformation CSS that is assigned to the device pool that the device uses, check the Use the Device Pool Calling Party Transformation CSS.

For more information, see topics related to applying the calling party transformation CSS to localize the calling party number.

The Calling Party Number is now localized.

Related Topics

Apply the Calling Party Transformation Calling Search Spaces (CSS), on page 230
Calling Party Normalization, on page 193
Calling Party Normalization Feature, on page 196
Configure the Calling Party Number Type, on page 209
Globalize the Calling Party Number, on page 196
Incoming Calling Party Number Settings, on page 215
Interactions, on page 203
Localize the Calling Party Number, on page 200
Restrictions, on page 206
Set the Service Parameters for Calling Party Normalization, on page 207

Calling Party Normalization Feature

In line with E.164 standards, 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 displays on the phone.

Tip Configuring calling party normalization alleviates issues with toll bypass where the call is routed to multiple locations over the IP WAN. In addition, it allows Cisco Unified Communications Manager to distinguish the origin of the call to globalize or localize the calling party number for the phone user.

Globalize the Calling Party Number

This section provides information about globalizing the Calling Party number.

Tip This section does not describe the international escape character, +, which you can configure for globalizing the calling party number. For information on the international escape character, see the *Cisco Unified Communications Manager System Guide*.

Globalization of the Calling Party Number

To globalize the calling party number for calls that get routed to multiple geographical locations, Cisco Unified Communications Manager allows you to configure prefixes for required access codes, escape codes, country codes, and so on, based on the calling party number type that the PSTN provides. The calling party number type that the PSTN provides determines whether the incoming call arrives from the PSTN as a national, international, subscriber, or unknown call. For example, if the call comes from a caller in Hamburg to an enterprise gateway in Hamburg, the call arrives to Cisco Unified Communications Manager with calling party number 69XXXXXXX with number type of Subscriber. However, if the call comes from a caller in Frankfurt to an enterprise gateway in Hamburg, the call arrives to Cisco Unified Communications Manager with caller party number 69XXXXXXX with number type of National.

Configuring the Calling Party Number Type setting and prefixes in Cisco Unified Communications Manager Administration allows Cisco Unified Communications Manager to reformat the calling party number from the PSTN-localized version to the globally dialable version by prefixing required access codes, international access codes, and so on, to the calling party number. You can configure the Calling Party Number Type setting for various patterns, for example, translation patterns, calling party transformation patterns, and route patterns, for both called and calling parties to ensure that Cisco Unified Communications Manager stamps the number type during various stages of incoming and outgoing calls. After Cisco Unified Communications Manager globalizes the calling party number, the call gets routed as expected to its destination.

Tip If your service provider prepends leading digits (for example, a zero) to the calling party number and you want to strip these digits before prepending other digits (for example, if the leading digits are not part of the E.164 number and you want to transform the calling party number to the E.164 format), you can configure the digits to strip fields to ensure that Cisco Unified Communications Manager strips the leading digits before applying the prefixes to an incoming calling party number. For more information, see the Strip Digits Field Considerations, on page 214.

Depending on your configuration for globalizing and localizing the calling party number, the phone user may see a localized number, a globalized number with access codes and prefixes, and/or the international escape character, +, in the calling party number. For example, the phone can show the localized calling party number on the phone screen and the globalized number in the call log directories on the phone. For example, the phone may show both the globalized and localized calling party number in the Call Details.

To ensure that the phone user does not need to edit the call log directory entry on the phone before placing a call, map the global calling party number to its local variant to route calls to the correct gateway; you can use route patterns and called party transformation patterns to route the call correctly, as the Map the Global Party Calling Number to Its Local Variant, on page 201 describes.

Configuration Windows to Globalize the Calling Party Number

The following table lists the configuration windows in Cisco Unified Communications Manager Administration where you can configure prefixes, the number of leading digits that you want to strip from the calling party number before applying the prefix, and the incoming calling party transformation CSS for various calling party number types (subscriber, national, and so on).

Table 24: Configuration Windows for Globalizing the Calling Party Number

Configuration Window	Considerations
Device Pool	You can configure prefixes in the device pool, which support digital gateways or trunks. In addition, if your service provider prepends digits to the calling party number, you can configure the number of leading digits that Cisco Unified Communications Manager must strip from the calling party number before applying the prefix. In this window, you can apply an incoming calling party transformation CSS for various calling party number types; for example, subscriber, unknown, and so on, depending on the device type. Configuring this CSS ensures that the device can globalize the calling party number based on the calling party number type.
Gateway	You can configure prefixes for H.323, MGCP (T1-PRI/BRI), and MGCP (E1-PRI/BRI) gateways. If you have gateways in multiple geographical locations, configure the prefix settings for each gateway in the Gateway Configuration window. For example, if you have a gateway in RTP and an incoming call arrives with caller ID 555 1212, you want to prefix the caller ID with 919 to yield 9195551212. However, if the call routes to another gateway, for example, in Dallas, which uses area code 214, before reaching its final destination, you want 91214 to display for the prefix instead of 91919. To globalize calling party numbers for incoming calls, you must configure the prefixes for gateways that handle incoming calls. In addition, if your service provider prepends digits to the calling party number, you can configure the number of leading digits that Cisco Unified Communications Manager must strip from the calling party number before applying the prefix. In this window, you can apply the incoming calling party transformation CSS for various calling party number types; for example, subscriber, unknown, and so on, depending on the device type. Configuring this CSS ensures that the device can globalize the calling party number based on the calling party number type. If you want to do so, you can apply the calling party transformation CSS that you chose in the device pool and applied to the device.

Configuration Window	Considerations
Trunk	You can configure prefixes for all trunk types. SIP trunks only support the incoming calling party settings (prefix, strip digits, and so on) for calling party number types of Unknown. In addition, if your service provider prepends digits to the calling party number, you can configure the number of leading digits that Cisco Unified Communications Manager must strip from the calling party number before applying the prefix. In this window, you can apply incoming calling party transformation CSS for various calling party number types; for example, subscriber, unknown, and so on, depending on the device type. Configuring this CSS ensures that the device can globalize the calling party number based on the calling party number type. If you want to do so, you can apply the calling party transformation CSS that you chose in the device pool and applied to the device.
Service Parameter	The prefix service parameters, Incoming Calling Party National Number Prefix, Incoming Calling Party International Number Prefix, Incoming Calling Party Subscriber Number Prefix, and Incoming Calling Party Unknown Number Prefix, each display for the phone, H.323. MGCP, and SIP (Unknown only for SIP) in the Service Parameters Configuration window. If you have a single H.323, MGCP (T1-PRI/BRI), or MGCP (E1-PRI/BRI) gateway in your network, you can configure the prefix service parameters, which support the Cisco CallManager service, for the particular gateway type in the Service Parameter Configuration window. If you configure the prefix service parameters for a particular gateway type, for example, H.323, be aware that all H.323 gateways that you configure in Cisco Unified Communications Manager Administration use the configuration from the service parameter unless you configure the prefix settings for a particular gateway in the Gateway Configuration window. The prefix service parameters allow you to configure a colon (:), which indicates that Cisco Unified Communications Manager must strip leading digits from the calling party number before applying the prefix. For more information, see the Set the Service Parameters for Calling Party Normalization, on page 207.

Localize the Calling Party Number

For the final presentation of the calling party number, Cisco Unified Communications Manager allows you to configure calling party transformation patterns for each calling party number type (National, International, Subscriber, and Unknown), so the number displays on the phone as the end user expects it to display; that is, you can configure the calling party transformation pattern to strip digits or add digits to the calling party number. To present the shortest recognizable number on the phone, you can strip unnecessary country codes, international access codes, and so on, depending on the locations of the caller and the called parties.

Tip You configure calling party transformation patterns to provide context-sensitive modifications to a calling party, not for routing purposes.

The following example shows how you can configure transformation patterns to localize a globalized calling party number.

Localizing the Calling Party Presentation

Tip You can globalize the calling party number before localizing the number. In this example, to globalize the calling party number before localizing the number, the administrator can configure the incoming gateway in Hamburg with the following information: Number Type of Subscriber with +4940 prefix; Number Type of National with +49 prefix; Number Type of International with + prefix. After the administrator configures the gateway, he configures the transformation patterns in the following table.

To globalize the calling party number before localizing the number, Cisco Unified Communications Manager applies the prefix and digits-to-strip configuration based on the calling party number type before applying the calling party transformation.

For example, a call occurs between two parties in Hamburg. The incoming call over the PSTN in Hamburg gets globalized as +49 40 69XXXXXXX, but the administrator has configured multiple transformation patterns to localize the calling party number before it reaches the desktop phone of the called party in Hamburg. These transformation patterns, which use closest match routing to strip unnecessary digits, contain the configuration, as shown in the following table:

Table 25: Calling Party Transformation Patterns (Example)

Calling Party Transformation Pattern 1	Calling Party Transformation Pattern 2	Calling Party Transformation Pattern 3
\+4940.! (Pattern Setting)	\+49.!	\+.!
discard Predot (Discard Digits Instructions Setting)	discard Predot	discard Predot
prefix 0 (Prefix Digits Setting)	prefix 00	prefix 000
Subscriber (Calling Party Number Type Setting)	National	International

By using digit analysis matching semantics, all the patterns in the previous table match the provided dial string; however, Transformation Pattern 1, which constitutes the closest match for a call within Hamburg, indicates that if the call is from Germany and from Hamburg, strip the German country code, 49, and the Hamburg city code, 40, and add the prefix 0 to the calling party number. So, when both parties in a call are in Hamburg, +494069XXXXXXX changes to 069XXXXXXX.

If the caller is from Frankfurt, Transformation Pattern 1 does not match, but Transformation Patterns 2 and 3 match. Representing the best match, Transformation Pattern 2 indicates that the system needs to strip the + and the German country code, 49, and then prefix 00 to the calling party number. So, for a long-distance call from Frankfurt to Hamburg, +494069XXXXXXX changes to 0069XXXXXXX.

If the caller is international, Transformation Pattern 3 works because Cisco Unified Communications Manager strips the international escape character, +, and prefixes the German international code, 000, to the calling party number.

Tip All phone device types, CTI route points, gateways, remote destination profiles, and trunks in Cisco Unified Communications Manager Administration localize the calling party number for themselves; to ensure that the device can localize the calling party number, you must configure the Calling Party Transformation CSS (calling search space) and assign this calling search space to the device. The Calling Party Transformation CSS takes on the attributes of the calling party transformation pattern, which you assign to the partition where the Calling Party Transformation CSS exists. If you want to do so, you can choose the Calling Party Transformation CSS in the device pool; when you assign the device pool to the device, the device uses the Calling Party Transformation CSS in the device pool; that is, if you check the Use Device Pool Calling Party Transformation CSS check box in the device configuration window.

The Calling Party Transformation CSS settings do not apply to T1-CAS and FXO ports on the gateway.

Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the Calling Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.

Map the Global Party Calling Number to Its Local Variant

To ensure that the phone user does not need to edit the call log directory entry on the phone before placing a call, map the global calling party number to its local variant to route calls to the correct gateway; you can use route patterns and called party transformation patterns to route the call correctly, as the following table describes.

Mapping the Global Calling Party Number to Its Local Variant

A Cisco Unified IP Phone in Hamburg (Phone Q) receives calls over the Hamburg or Frankfurt PSTN from different localized and globalized calling party numbers. To ensure that the phone user for the Phone Q does not need to edit the call log directory entry on the phone to return the call, you can associate the route patterns to the calling search space in the Phone Configuration window for Phone Q.

In Cisco Unified Communications Manager Administration, you configure the route patterns in the Route Patterns Configuration window (**Call Routing** > **Route/Hunt** > **Route Patterns**).

Table 26: Mapping the Global Calling Party Number to Its Local Variant (Example)

Route Pattern	Configuration for Route Pattern Setting	Configuration for Discard Digits Setting
Route Pattern 1	\+4940.! Configured for local Hamburg callers that call by using a globalized calling party number.	discard Predot
Route Pattern 2	0.! Configured for local Hamburg callers that call by using a localized calling party number.	discard Predot
Route Pattern 3	0.0! Configured for Germany callers that do not have a Hamburg directory number that is associated with their device; these callers use a localized calling party number from Frankfurt or other cities in Germany.	discard Predot
Route Pattern 4	\+49.! Configured for German callers that do not have a Hamburg directory number that is associated with their device; these callers use a globalized calling party number from Frankfurt or any other city in Germany.	discard Predot

When Phone Q receives a call from the Hamburg calling party number, 69XXXXXXX, via the PSTN, the calling party number +49406XXXXXXX displays on the phone screen for Phone Q. If the phone user for Phone Q returns the call by using the globalized calling party number, Cisco Unified Communications Manager matches the pattern, \+49.!, routes the call to the correct gateway, and sends the relevant digits. If the phone user for Phone Q returns the call by using the localized calling party number, Cisco Unified Communications Manager matches the pattern, 0.!, routes the call to the correct gateway, and sends the relevant digits.

When Phone Q gets a call from the Frankfurt calling party number XXXXXXX via the PSTN, the globalized calling party number +4969XXXXXXX displays on the phone screen for Phone Q, and the localized calling party number displays as 0069XXXXXXX. If the phone user for Phone Q returns the call by using the globalized calling party number, Cisco Unified Communications Manager matches the pattern, \+49.!, routes the call to the correct gateway, and sends the relevant digits. If the phone user for Phone Q returns the call by using the localized calling party number, Cisco Unified Communications Manager matches the pattern, 0.0!, routes the call to the correct gateway, and sends the relevant digits.

System Requirements

The following system requirements apply to calling party normalization:

- Cisco Unified Communications Manager 7.1
- Cisco Unified IP Phones 7906, 7911, 7931, 7961, 7962, 7965, 7970, 7971, and 7975

Calling Party Normalization Interactions and Restrictions

Interactions

This section describes how calling party normalization interacts with Cisco Unified Communications Manager features and applications.

Globalize and Localize Calling Party Numbers for Transferred Calls

The transfer feature relies on midcall updates, so depending on the scenario, a transferred call may not support globalization and localization of the calling party number. (Calling party normalization supports globalization and localization during call setup for each hop of the call, not for midcall updates.) This section provides examples of how calling party normalization works for transferred calls.

Calling Party Normalization for On Net Transferred Call Across a Gateway

Phone A with extension 12345 and phone number of 972 500 2345 calls Phone B with extension 54321 and phone number 972 500 4321; when the call arrives on extension 54321, calling party number 12345 displays on Phone B. Phone B transfers the call to Phone C in San Jose through a San Jose gateway. During the initiation of the transfer, Phone C displays the calling party number for Phone B as 972 500 4321. After the transfer completes, Phone C displays the calling party number for Phone A as 12345.

Calling Party Normalization for Transferred Call Through an Incoming Gateway

Via the PSTN in Dallas, a caller (Phone D) calls Phone E (Cisco Unified IP Phone), which uses extension 7891 and phone number 972 500 6789. On the incoming Dallas gateway, the caller information for Phone D displays as 500 1212/<Subscriber>. Phone E displays +1 972 500 1212 for the globalized calling party number and 500 1212 for the localized calling party number for Phone D. Phone E initiates a transfer to Phone C in San Jose across the San Jose gateway. During the initiation of the transfer, Phone C displays the calling party number for Phone E as 972 500 6789. After the transfer completes, Phone C displays the calling party number for Phone D as +1 972 500 1212.

Globalize and Localize Calling Party Numbers for Forwarded Calls

Forwarded calls support globalized and localized calling party numbers. Globalization and localization of the call occur during call setup for each hop of the call. Depending on the hop for the call and the configuration of the gateway, that is, the calling party transformation and prefix configuration on the gateway, the globalized version or the localized version (or both) may display on the phone. See the following example, which describes how an incoming call via the PSTN gets forwarded to another geographic location.

For example, via the PSTN in Dallas, a caller with Phone F calls Phone G (Cisco Unified IP Phone), which has forwarded all calls to Phone H (Cisco Unified IP Phone) in San Jose. On the incoming Dallas gateway, the caller information for Phone F displays as 500 5555/<Subscriber>. On the outgoing gateway from Dallas to San Jose, the outgoing caller information for the Calling Party Transformation CSS comprises 972 500 5555/National. On the incoming gateway in San Jose, the calling party number gets prefixed with +1 for the National number type; on Phone H in San Jose, the localized calling party number for Phone F displays as 972 500 5555, and the globalized calling party number displays as +1 972 500 5555.

Bulk Administration Tool

For information on how calling party normalization relates to the Bulk Administration Tool, see the Cisco Unified Communications Manager Bulk Administration Guide.

Call Detail Records

For information on how calling party normalization impacts call detail records (CDRs), see the Cisco Unified Communications Manager Call Detail Records Administration Guide.

Cisco Unified Communications Manager Assistant

Cisco Unified Communications Manager Assistant automatically supports localized and globalized calls if you configure the calling party normalization feature. Cisco Unified Communications Manager Assistant can display localized calling party numbers on the user interfaces. In addition, for an incoming call to the manager, Cisco Unified Communications Manager Assistant can display localized and globalized calling party numbers when filter pattern matching occurs. For information on configuring Cisco Unified Communications Manager Assistant, see the Cisco Unified Communications Manager Assistant with Proxy Line Support, on page 305 or the Cisco Unified Communications Manager Assistant with Shared Line Support, on page 345.

CDR Analysis and Reporting

For information on how calling party normalization impacts Cisco Unified Communications Manager CDR Analysis and Reporting (CAR), see the Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide.

Cisco Unity and Cisco Unity Connection

Cisco Unity and Cisco Unity Connection do not support the international escape character (+). Because these applications do not support the +, you must ensure that calls to Cisco Unity or Cisco Unity Connection do not contain the +, which ensures that voice-messaging features work as expected.

If you configure the + for the incoming prefix settings in Cisco Unified Communications Manager Administration to globalize the calling party number, the + gets inserted as a prefix to an incoming calling party number on a H.323, MGCP, or SIP gateway (or trunk, if applicable). If you configure calling party transformations, the device can localize the calling party number to transform the number to display differently than the globalized version. For example, a call from the North American Numbering Plan arrives as a 10-digit calling party number, 2225551234. Cisco Unified Communications Manager prefixes +1 to the calling party number to display the E.164 formatted number as +12225551234. On a phone in North America, Cisco Unified Communications Manager uses a calling party transformation to convert +12225551234 to 10 digits before the number displays on the phone; on a phone outside of North America, Cisco Unified Communications Manager may transform the number to only strip the + and to prefix the 00, as in 0012225551234.

For Cisco Unity and Cisco Unity Connection to work as expected, treat these applications as devices and configure calling party transformations that ensure that the + does not get sent to these voice-messaging applications. If the Cisco Unity or Cisco Unity Connection server uses a North American-based dial plan, localize the calling party number to NANP format before the voice-mail application receives the calling party number. Because no calling party transformation options exist in Cisco Unified Communications Manager Administration for voice-messaging ports, make sure that you configure the calling party number transformations in the device pool that is associated with the voice-messaging ports. To localize the calling party number, also consider prefixing access codes, so the voice-messaging application easily can redial the number for certain features, such as Live Reply. For example, you can convert +12225551234 to 912225551234, and you can convert international number, +4423453456, to include the international escape code, 90114423453456.

Cisco Unity Connection

Cisco Unity Connection does not support the international escape character (+). Because this application does not support the +, you must ensure that calls to Cisco Unity Connection do not contain the +, which ensures that voice-messaging features work as expected.

If you configure the + for the incoming prefix settings in Cisco Unified Communications Manager Administration to globalize the calling party number, the + gets inserted as a prefix to an incoming calling party number on a H.323, MGCP, or SIP gateway (or trunk, if applicable). If you configure calling party transformations, the device can localize the calling party number to transform the number to display differently than the globalized version. For example, a call from the North American Numbering Plan arrives as a 10-digit calling party number, 2225551234. Cisco Unified Communications Manager prefixes +1 to the calling party number to display the E.164 formatted number as +12225551234. On a phone in North America, Cisco Unified Communications Manager uses a calling party transformation to convert +12225551234 to 10 digits before the number displays on the phone; on a phone outside of North America, Cisco Unified Communications Manager may transform the number to only strip the + and to prefix the 00, as in 0012225551234.

For Cisco Unity Connection to work as expected, treat this application as a device and configure calling party transformations that ensure that the + does not get sent to this voice-messaging application. If the Cisco Unity Connection server uses a North American-based dial plan, localize the calling party number to NANP format before Cisco Unity Connection receives the calling party number. Because no calling party transformation options exist in Cisco Unified Communications Manager Administration for voice-messaging ports, make sure that you configure the calling party number transformations in the device pool that is associated with the voice-messaging ports. To localize the calling party number, also consider prefixing access codes, so the voice-messaging application easily can redial the number for certain features, such as Live Reply. For example, you can convert +12225551234 to 912225551234, and you can convert international number, +4423453456, to include the international escape code, 90114423453456.

Cisco Extension Mobility

Cisco Extension Mobility works as expected; that is, a phone user that is logged in to a Cisco Extension Mobility phone may see globalized or localized calling party numbers on the phone screen or in the call log directories on the phone.

Device Mobility

The following example shows how calling party normalization works when you move a phone from its home location, as supported with the device mobility feature in Cisco Unified Communications Manager.

A Cisco Unified IP Phone (Phone N) with home location in Dallas moves to San Jose. The Cisco Unified IP Phone in Dallas uses device pool, DP_Dallas, which has the Calling Party Transformation CSS as CallingTransform_Dallas; the Calling Transform_Dallas CSS contains the DallasPhone and the CommonTransform partitions. The roaming device in San Jose uses device pool, DP_SanJose, which has the

Calling Party Transformation CSS as CallingTransform_SJ; the CallingTransform_SJ CSS contains the SJPhone and the CommonTransform partitions. Cisco Unified Communications Manager Administration contains the configuration in the following table:

Table 27: Globalizing and Localizing Calling Party Numbers with Device Mobility (Example)

Calling Party Transformation Pattern 1	Calling Party Transformation Pattern 2	Calling Party Transformation Pattern 3
• Pattern— \+.@ • Partition—CommonTransform • Disregard Digits Instructions—Predot • Calling Party Number Type—National	• Pattern—\+1.408! • Partition—SJPhone • Disregard Digits Instructions—Predot • Prefix—9 • Calling Party Number Type—Subscriber	• Pattern—\+1972.! • Partition—DallasPhone • Discard Digits Instructions—Predot • Prefix—9 • Calling Party Number Type—Subscriber

When the phone is in its home location in Dallas, a call comes via the PSTN from 408 500 1212 <National> in San Jose. On the incoming Dallas gateway, the calling party number number gets converted to the global format of + 1 408 500 1212. On the phone that currently is in Dallas, the calling party number displays as 1 408 500 1212.

When the phone is in its home location in Dallas, a call comes via the PSTN from 400 2323 <Subscriber> from a seven-digit dialing area in Dallas. On the incoming Dallas gateway, the calling party number gets converted to the global format of + 1 972 400 2323. On the phone that currently is in Dallas, the calling party number displays as 9 400 2323.

When the phone is roaming in San Jose, a call comes via the PSTN from 972 500 1212 <National> in Dallas. On the incoming San Jose gateway, the calling party number gets converted to the global format of + 1 408 500 1212. On the phone that currently is in San Jose, the calling party number displays as 1 972 500 1212.

When the phone is roaming in San Jose, a call comes via the PSTN from 500 1212 <Subscriber> from a seven-digit dialing area in San Jose. On the incoming San Jose gateway, the calling party number gets converted to the global format of + 1 408 500 1212. On the phone that currently is in San Jose, the calling party number displays as 9 500 1212.

Note The Calling Party Transformation CSS of the roaming device pool overrides the device level configuration of the phone roaming within same DMG, even when the Use Device Pool Calling Party Transformation CSS check box in the phone configuration window remains unchecked.

Restrictions

Before you configure calling party normalization, review the following restrictions:

- The calling party number that displays for a shared line depends on the sequence of call control events in Cisco Unified Communications Manager. To avoid displaying an incorrect localized calling party number on a shared line, especially when the shared line occurs in different geographical locations, make sure that you configure the same Calling Party Transformation CSS for different devices that share the same line.

- SIP trunks and MGCP gateways can support sending the international escape character, (+) for calls. H.323 gateways do not support the +. QSIG trunks do not attempt to send the +. For outgoing calls through a gateway that supports +, Cisco Unified Communications Manager can send the + with the dialed digits to the gateway. For outgoing calls through a gateway that does not support +, the international escape character + gets stripped when Cisco Unified Communications Manager sends the call information to the gateway.
- SIP does not support the number type, so calls through SIP trunks support only the Incoming Number settings for calling party number types of Unknown.
- A QSIG configuration usually supports a uniform dial plan. Transformation of numbers and prefixes may cause feature interaction issues if you use QSIG.
- For localizing the calling party number, the device must apply the transformation by using digit analysis. If you configure the Calling Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.
- The Calling Party Transformation CSS settings do not apply to T1-CAS and FXO ports on the gateway.
- Cisco Unity Connection does not support the international escape character (+). Therefore, you must ensure that calls to Cisco Unity Connection do not contain the +, so that voice-messaging features work as expected. For more information, see Cisco Unity Connection, on page 205.

Install and Activate Calling Party Normalization

After you install Cisco Unified Communications Manager, you can configure calling party normalization. Calling party normalization service parameters support the Cisco CallManager service, so activate the Cisco CallManager service in Cisco Unified Serviceability before you configure calling party normalization.

Calling Party Normalization Configuration

This section contains information about configuring Calling Party Normalization.

Tip Before you configure calling party normalization, review the task to configure Calling Party Normalization.

Related Topics

Configure Calling Party Normalization, on page 193

Set the Service Parameters for Calling Party Normalization

Tip To locate the service parameters in Cisco Unified Communications Manager Administration, choose **System** > **Service Parameters**; choose the server and the Cisco CallManager service. After the parameters display, click Advanced. For information on the service parameter, click the hyperlink for the service parameter name or the question mark that displays in the upper, right corner of the window.

If your service provider prepends leading digits (for example, a zero) to the calling party number and you want to strip these digits before prepending other digits (for example, if the leading digits are not part of the E.164 number and you want to transform the calling party number to the E.164 format), you can enter a colon (:) followed by the number of digits that you want to strip in the Incoming Calling Party National Number Prefix, Incoming Calling Party International Number Prefix, Incoming Calling Party Unknown Number Prefix, and/or Incoming Calling Party Subscriber Number Prefix service parameters to ensure that Cisco Unified Communications Manager strips the leading digits before applying the prefixes to an incoming calling party number. The value that you configure before the colon (:) represents the prefix; the value that you configure after the colon (:) specifies the number of digits that you want Cisco Unified Communications Manager to strip from the calling party number before it applies the prefix.

For example, you configure +:1 in the incoming prefix service parameters, which alerts Cisco Unified Communications Manager to strip the first digit from the calling party number and then apply the international escape character +. If an incoming call arrives as 04423452345, Cisco Unified Communications Manager strips the first digit, in this case, zero, from the calling party number and prefixes the international escape character + to the calling party number. As a result, the calling party number gets transformed to +4423452345.

To strip digits without prefixing anything, you can configure the colon (:) in the incoming prefix service parameters without configuring a prefix. If you do not enter a prefix before the colon (:), Cisco Unified Communications Manager strips the number of leading digits that you specify and does not apply a prefix to the calling party number. For example, if you configure :2, Cisco Unified Communications Manager strips 2 leading digits without applying a prefix.

If you want Cisco Unified Communications Manager to strip a certain number of leading digits, and the entire number of digits for the calling party number equals or specifies less than the value that you configure, Cisco Unified Communications Manager strips all digits but still applies the prefix; that is, if you configure a prefix. For example, if you enter +1:6 in the incoming prefix fields, and the calling party number contains 6 or fewer digits, Cisco Unified Communications Manager strips all digits and applies the prefix +1.

If you configure Cisco Unified Communications Manager to strip more digits than exist in the calling party number, Cisco Unified Communications Manager clears the calling party number (makes it blank).

If you do not configure a colon (:) in the incoming prefix service parameters, Cisco Unified Communications Manager does not strip any digits from the calling party number; that is, unless you configure the incoming fields that are described in Incoming Calling Party Number Settings, on page 215, which support the configuration at the device level.

If you configure a prefix but the calling party number that arrives is empty, Cisco Unified Communications Manager does not apply the prefix.

Cisco Unified Communications Manager can strip up to 24 digits from the calling party number. If you enter :26 in the incoming prefix service parameters, Cisco Unified Communications Manager Administration displays a message and does not allow the configuration.

If an error occurs when Cisco Unified Communications Manager attempts to strip the digits and apply the prefix to the calling party number, Cisco Unified Communications Manager does not manipulate the digits or apply the prefixes; instead, Cisco Unified Communications Manager uses the calling party number that arrived for the call.

Tip If you configure the incoming fields that display in the device configuration windows and the service parameters, Cisco Unified Communications Manager uses the configuration that you configured in the device configuration window.

Clusterwide Parameters (Device - PRI and MGCP Gateway)

- Incoming Calling Party National Number Prefix - MGCP
- Incoming Calling Party International Number Prefix - MGCP
- Incoming Calling Party Subscriber Number Prefix - MGCP
- Incoming Calling Party Unknown Number Prefix - MGCP

Tip If you have a single H.323, MGCP (T1-PRI/BRI), or MGCP (E1-PRI/BRI) gateway in your network, you can configure the prefix service parameters, which support the Cisco CallManager service, for the particular gateway type in the Service Parameter Configuration window. If you configure the prefix service parameters for a particular gateway type, for example, H.323, be aware that all H.323 gateways that you configure in Cisco Unified Communications Manager Administration use the configuration from the service parameter unless you configure the prefix settings for a particular gateway in the Gateway Configuration window.

Clusterwide Parameters (Device - H323)

- Incoming Calling Party National Number Prefix - H.323
- Incoming Calling Party International Number Prefix - H.323
- Incoming Calling Party Subscriber Number Prefix - H.323
- Incoming Calling Party Unknown Number Prefix - H.323

Tip If the incoming prefix service parameters for H.323 use the same prefix as the incoming prefix service parameters for the phone, the prefix gets used twice for the calling party; first, when the incoming call gets to the gateway and again, when the call terminates at the phone.

Clusterwide Parameters (Device - SIP)

Incoming Calling Party Unknown Number Prefix - SIP

Configure the Calling Party Number Type

Configuring the Calling Party Number Type setting and prefixes in Cisco Unified Communications Manager Administration allows Cisco Unified Communications Manager to reformat the calling party number from the PSTN-localized version to the globally dialable version by prefixing required access codes, international access codes, and so on, to the calling party number. You can configure the Calling Party Number Type setting for various patterns for both called and calling parties to ensure that Cisco Unified Communications Manager stamps the number type during various stages of incoming and outgoing calls.

You configure the Calling Party Number Type setting in the Calling Party Transformation Pattern Configuration, Route Pattern Configuration, Hunt Pilot Configuration, Translation Pattern Configuration, and the Route List Detail Configuration windows in Cisco Unified Communications Manager Administration.

The following table describes the Calling Party Number Type setting that displays in Cisco Unified Communications Manager Administration.

Table 28: Description for Calling Party Number Type

Setting	Description
Calling Party Number Type	

Setting	Description
	Choose the format for the number type in calling party directory numbers. Cisco Unified Communications Manager sets the calling directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified Communications Manager does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the calling directory number to be encoded to a non-national numbering plan type. Choose one of the following options: • Cisco CallManager - The Cisco Unified Communications Manager sets the directory number type. • Unknown - Choose when the dialing plan is unknown. • National - Use when you are dialing within the dialing plan for your country. • International - Use when you are dialing outside the dialing plan for your country. • Subscriber - Use when you are dialing a subscriber by using a shortened subscriber number. In the following windows in Cisco Unified Communications Manager Administration, you can configure the Calling Party Number Type setting: • Hunt List Detail Configuration - **Call Routing** > **Route/Hunt** > **Hunt List** (Add the hunt list; after you click **Save**, the **Add Line Group** button displays. To display the Hunt List Detail Configuration window, click the **Add Line Group** button.) • Route Pattern Configuration - **Call Routing** > **Route/Hunt** > **Route Pattern** • Hunt Pilot Configuration - **Call Routing** > **Route/Hunt** > **Hunt Pilot** • Translation Pattern Configuration - **Call Routing** > **Translation Pattern** • Calling Party Transformation Pattern Configuration - **Call Routing** > **Transformation Pattern** > **Calling Party Transformation Pattern** **Tip**

Setting	Description
	In the Gateway and Trunk Configuration window, you can configure the Calling Party IE Number Type Unknown setting. If you can configure this setting and choose any other option except for Cisco CallManager, which is the default, your configuration for this field overwrites the Calling Party Number Type setting for the outgoing call through a particular gateway.

Configure the Incoming Calling Party Settings

This section contains information about prefix fields, strip digits fields, and incoming Calling Party number settings.

Prefix Field Considerations

Before you configure the prefix fields that are described in Incoming Calling Party Number Settings, on page 215, consider the following information.

- In the Device Pool, Gateways, and Trunk Configuration windows, to delete the prefixes in all incoming calling party settings at the same time, click Clear Prefix Settings; to enter the default value for all incoming calling party settings at the same time, click Default Prefix Settings.
- If the word Default displays in the Prefix field in the Gateway or Trunk Configuration window, you cannot configure the Strip Digits field in the Gateway or Trunk Configuration window. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word Default displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip digit functionality.
- To configure the Strip Digits field in the Device Pool, Gateway, or Trunk Configuration window, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word Default in the Prefix field.
- When the prefix gets applied to the incoming calling party number on the device, Cisco Unified Communications Manager includes the prefix in the calling party number field for all additional actions, such as supplementary services including call forwarding, call park, voice messaging, CDR data, and so on, that pertain to the call.
- If you configure a prefix but the calling party number that arrives is empty, Cisco Unified Communications Manager does not apply the prefix. (For example, the calling party number arrives empty because you chose Restricted from the Calling Line ID Presentation drop-down list box in the Route Pattern, Gateway, or Trunk Configuration windows.)
- If an error occurs when Cisco Unified Communications Manager attempts to strip the digits and apply the prefix to the calling party number, Cisco Unified Communications Manager does not manipulate the

digits or apply the prefixes; instead, Cisco Unified Communications Manager uses the calling party number that arrived for the call.

- Configure the incoming prefix fields in conjunction with the strip digit fields; that is, if your service provider prepends leading digits (for example, a zero) to the calling party number. For more information on stripping leading digits from the calling party number, see the Strip Digits Field Considerations, on page 214.

Strip Digits Field Considerations

If your service provider prepends leading digits (for example, a zero) to the calling party number and you want to strip these digits before prepending other digits (for example, if the leading digits are not part of the E.164 number and you want to transform the calling party number to the E.164 format), you can configure the fields in Incoming Calling Party Number Settings, on page 215 to ensure that Cisco Unified Communications Manager strips the leading digits before applying the prefixes to an incoming calling party number.

Before you configure the number of leading digits that Cisco Unified Communications Manager must strip from the calling party number, consider the following information:

- You can strip digits either by configuring the Incoming Prefix service parameters in the Service Parameter Configuration window or by configuring the Strip Digits fields in the Device Pool, Gateway, or Trunk Configuration windows. For information on how to configure the service parameters for this functionality, see the Set the Service Parameters for Calling Party Normalization, on page 207.
- If the word Default displays in the Prefix field in the Gateway or Trunk Configuration window, you cannot configure the Strip Digits field in the Gateway or Trunk Configuration window. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word Default displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip digit functionality.
- To configure the Strip Digits field in the Device Pool, Gateway, or Trunk Configuration window, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word Default in the Prefix field.
- Be aware that Cisco Unified Communications Manager can strip up to 24 digits. If you enter a value that is larger than 24 in the field, for example, 26, Cisco Unified Communications Manager Administration does not allow the configuration.
- If you want Cisco Unified Communications Manager to strip a certain number of leading digits, and the entire number of digits for the calling party number equals or specifies less than the value that you configure, Cisco Unified Communications Manager strips all digits but still applies the prefix; that is, if you configure a prefix.
- If you configure Cisco Unified Communications Manager to strip more digits than exist in the calling party number, Cisco Unified Communications Manager clears the calling party number (makes it blank).
- If you do not configure a value for the Strip Digits fields, Cisco Unified Communications Manager does not strip any digits from the calling party number.
- If an error occurs when Cisco Unified Communications Manager attempts to strip the digits and apply the prefix to the calling party number, Cisco Unified Communications Manager does not manipulate the digits or apply the prefixes; instead, Cisco Unified Communications Manager uses the calling party number that arrived for the call.

Incoming Calling Party Number Settings

The following windows in Cisco Unified Communications Manager Administration display incoming calling party number settings:

- Device Pool (**System** > **Device Pool**) - Applies the configuration to all digital gateways and trunks; that is, if you choose the device pool for the device.
- Gateway (**Device** > **Gateway**) - Displays settings in the H.323 gateway configuration window and in the port windows (Gateway Configuration window) for MGCP (T1-PRI/BRI) and MGCP (E1-PRI/BRI).
- Trunk (**Device** > **Trunk**) - Displays all settings in all trunk configuration windows except the SIP trunk.

Tip The SIP Trunk Configuration window only displays the Incoming Number settings, which is used for the Unknown calling party number type.

For configuration procedures for each configuration window, see the *Cisco Unified Communications Manager Administration Guide*.

The following table describes the incoming calling party number settings for device pools, gateways, and trunks.

Table 29: Incoming Calling Party Number Settings for Device Pools, Gateways, and Trunks

Setting	Description
Clear Prefix Setting	To delete all prefixes for all calling party number types, click **Clear Prefix Settings**.
Default Prefix Setting	To enter the default value for all prefix fields at the same time, click **Default Prefix Settings**.

Setting	Description
National Number	

Setting	Description
	Configure the following settings to globalize calling party numbers that use National for the Calling Party Number Type. • Prefix - Cisco Unified Communications Manager applies the prefix that you enter in this field to calling party numbers that use National for the Calling Party Numbering Type. You can enter up to 8 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. **Tip** If the word, Default, displays in the Prefix field in the Gateway or Trunk Configuration window, you cannot configure the Strip Digits field in the Gateway or Trunk Configuration window. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip digit functionality. **Tip** To configure the Strip Digits field in the Device Pool, Gateway, or Trunk Configuration window, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field. • Strip Digits - Enter the number of digits that you want Cisco Unified Communications Manager to strip from the calling party number of National type before it applies the prefixes. • Use Device Pool CSS - This setting displays in the Gateway and Trunk Configuration windows, not the Device Pool Configuration window. Check this check box to use the calling search space for the National Number field that is configured in the device pool that is applied to

Setting	Description
	the device. - Calling Search Space - This setting allows you to globalize the calling party number of National calling party number type on the device. Make sure that the calling search space that you choose contains the calling party transformation pattern that you want to assign to this device.

Setting	Description
International Number	

Setting	Description
	Configure the following settings to globalize calling party numbers that use International for the Calling Party Number Type. • Prefix - Cisco Unified Communications Manager applies the prefix that you enter in this field to calling party numbers that use International for the Calling Party Numbering Type. You can enter up to 8 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. **Tip** If the word, Default, displays in the Prefix field in the Gateway or Trunk Configuration window, you cannot configure the Strip Digits field in the Gateway or Trunk Configuration window. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip digit functionality. **Tip** To configure the Strip Digits field in the Device Pool, Gateway, or Trunk Configuration window, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field. • Strip Digits - Enter the number of digits that you want Cisco Unified Communications Manager to strip from the calling party number of International type before it applies the prefixes. • Use Device Pool CSS - This setting displays in the Gateway and Trunk Configuration windows, not the Device Pool Configuration window. Check this check box to use the calling search space for the International Number field that is configured in the device pool that is applied to

Setting	Description
	the device. • Calling Search Space - This setting allows you to globalize the calling party number of International calling party number type on the device. Make sure that the calling party transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device. **Tip** Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the CSS as None, the transformation does not match and does not get applied. Ensure that you configure the calling party transformation pattern in a non-null partition that is not used for routing.

Setting	Description
Subscriber Number	

Setting	Description
	Configure the following settings to globalize calling party numbers that use Subscriber for the Calling Party Number Type. • Prefix - Cisco Unified Communications Manager applies the prefix that you enter in this field to calling party numbers that use Subscriber for the Calling Party Numbering Type. You can enter up to 8 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. **Tip** If the word, Default, displays in the Prefix field in the Gateway or Trunk Configuration window, you cannot configure the Strip Digits field in the Gateway or Trunk Configuration window. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip digit functionality. **Tip** To configure the Strip Digits field in the Device Pool, Gateway, or Trunk Configuration window, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field. • Strip Digits - Enter the number of digits that you want Cisco Unified Communications Manager to strip from the calling party number of Subscriber type before it applies the prefixes. • Use Device Pool CSS - Check this check box to use the calling search space for the Subscriber Number field that is configured in the device pool that is applied to the device. • Calling Search Space - This setting allows you to globalize the calling party number of

Setting	Description
	Subscriber calling party number type on the device. Make sure that the CSS that you choose contains the calling party transformation pattern that you want to assign to this device. **Tip** Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the CSS as None, the transformation does not match and does not get applied. Ensure that you configure the calling party transformation pattern in a non-null partition that is not used for routing.

Setting	Description
Unknown Number (does not display in the SIP Trunk Configuration window)	

Setting	Description
	Configure the following settings to globalize calling party numbers that use Unknown for the Calling Party Number Type. • Prefix - Cisco Unified Communications Manager applies the prefix that you enter in this field to calling party numbers that use Unknown for the Calling Party Numbering Type. You can enter up to 8 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. **Tip** If the word, Default, displays in the Prefix field in the Gateway or Trunk Configuration window, you cannot configure the Strip Digits field in the Gateway or Trunk Configuration window. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip digit functionality. **Tip** To configure the Strip Digits field in the Device Pool, Gateway, or Trunk Configuration window, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field. • Strip Digits - Enter the number of digits that you want Cisco Unified Communications Manager to strip from the calling party number of Unknown type before it applies the prefixes. • Use Device Pool CSS - This setting displays in the Gateway and Trunk Configuration windows, not the Device Pool Configuration window. Check this check box to use the calling search space for the Unknown Number field that is configured in the device pool that is applied to

Setting	Description
	the device. • Calling Search Space - This setting allows you to globalize the calling party number of Unknown calling party number type on the device. Make sure that the calling party transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device. **Tip** Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the CSS as None, the transformation does not match and does not get applied. Ensure that you configure the calling party transformation pattern in a non-null partition that is not used for routing.

Setting	Description
Incoming Number (displays in the SIP Trunk Configuration window only)	

Setting	Description
	SIP trunks support calling party number type of Unknown only. For SIP trunks only, configure the following settings to globalize calling party numbers that use Unknown for the Calling Party Number Type. • Prefix - Cisco Unified Communications Manager applies the prefix that you enter in this field to calling party numbers that use Unknown for the Calling Party Numbering Type. You can enter up to 8 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. **Tip** If the word, Default, displays in the Prefix field in the Gateway or Trunk Configuration window, you cannot configure the Strip Digits field in the Gateway or Trunk Configuration window. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip digit functionality. **Tip** To configure the Strip Digits field in the Device Pool, Gateway, or Trunk Configuration window, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field. • Strip Digits - Enter the number of digits that you want Cisco Unified Communications Manager to strip from the calling party number of Unknown type before it applies the prefixes. • Use Device Pool CSS - This setting displays in the Gateway and Trunk Configuration windows, not the Device Pool Configuration window. Check this check box to use the calling search space for the Unknown Number field that is

Setting	Description
	configured in the device pool that is applied to the device. • Calling Search Space - This setting allows you to globalize the calling party number of Unknown calling party number type on the device. Make sure that the calling party transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device. **Tip** Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the CSS as None, the transformation does not match and does not get applied. Ensure that you configure the calling party transformation pattern in a non-null partition that is not used for routing.

Apply the Calling Party Transformation Calling Search Spaces (CSS)

Before you configure the Calling Party Transformation CSS, make sure that you understand the steps that are required to localize the calling party number; for example, configuring the partition, configuring the calling search space, and so on. For more information, see the Configure Calling Party Normalization, on page 193.

The following table describes the various Calling Party Transformation CSS settings and lists the configuration windows in Cisco Unified Communications Manager Administration where you assign the settings.

Table 30: Configuring the Calling Party Transformation CSS to Localize the Calling Party Number

Setting	Description
Calling Party Transformation CSS	This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device. **Tip** Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the Calling Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing. All phone device types, CTI route points, gateways, remote destination profiles, and trunks in Cisco Unified Communications Manager Administration can localize the calling party number for themselves; therefore, you can access this setting in the following windows in Cisco Unified Communications Manager Administration: • Device Pool (**System** > **Device Pool**) • Phone (**Device** > **Phone**) • CTI Route Points (**Device** > **CTI Route Point**) • Gateway (**Device** > **Gateway**) - Depending on the gateway type, the setting may display in the port configuration window or the gateway configuration window. • Trunk (**Device** > **Trunk**) • Remote Destination Profile (**Device** > **Device Settings** > **Remote Destination Profile**)

Setting	Description
Use Device Pool Calling Party Transformation CSS	To use the Calling Party Transformation CSS that is configured in the device pool that is assigned to this device, check this check box. If you do not check this check box, the device uses the Calling Party Transformation CSS that you configured in the device configuration window. All phone device types, CTI route points, gateways, remote destination profiles, and trunks in Cisco Unified Communications Manager Administration can localize the calling party number for themselves; therefore, you can access this setting in the following windows in Cisco Unified Communications Manager Administration: • Phone (**Device** > **Phone**) • CTI Route Points (**Device** > **CTI Route Point**) • Gateway (**Device** > **Gateway**) - Depending on the gateway type, the setting may display in the port configuration window or the gateway configuration window. • Trunk (**Device** > **Trunk**) • Remote Destination Profile (**Device** > **Device Settings** > **Remote Destination Profile**)

Provide Information to Users

Depending on your configuration, a phone user may not need to edit the call log directory entry on the phone before placing a call. Depending on your configuration, the phone user may see the international escape character, +, in the call log directories on the phone.

CHAPTER 11

Cisco Mobility

Cisco Unified Mobility

This chapter provides information about Cisco Unified Mobility which extends the rich call control capabilities of Cisco Unified Communications Manager from the primary workplace desk phone of a mobile worker to any location or device of their choosing.

For example, Cisco Unified Mobility associates a user mobile phone number with the user business IP phone number. Cisco Unified Mobility then directs incoming calls to ring on a user mobile phone as well as the business phone, thus providing a single number for callers to reach the user. Calls that go unanswered on all the designated devices get redirected to the enterprise voice mailbox of the user (not to the mobile voice mailbox).

Administrators can configure Cisco Unified Mobility, formerly known as Cisco Unified Mobility Manager, by using the Cisco Unified Communications Manager Administration windows to configure the setup for end users. End users can use Cisco Unified Communications Self Care Portal windows to configure their own personal settings.

Cisco Unified Mobility comprises a number of features that this chapter discusses. The chapter provides an overview of the configuration procedures that administrators follow.

See the user guide for a particular Cisco Unified IP Phone model for procedures that end users follow to configure the Cisco Unified Mobility settings for their phones by using the Cisco Unified Communications Self Care Portal windows.

Configure Cisco Unified Mobility

Cisco Unified Mobility gives users the ability to redirect incoming IP calls from the Cisco Unified Communications Manager to up to ten different designated client devices such as mobile phones. For more information on Cisco Unified Mobility features, see the List of Cisco Unified Mobility Features, on page 236.

Perform the following steps to configure Cisco Unified Mobility.

Note The CMC and FAC feature on Cisco Mobility does not support an alternative number as its DVO callback number. The DVO callback number has to be the number registered in the MI (Mobility Identity) page. For example, consider a dual-mode phone that has a registered MI of 408-555-1111. The route-pattern "9.@" is used to route the external call and has FAC enabled. The DVO callback number in Cisco Jabber on the dual-mode device must be set to 408-555-1111.

Procedure

Step 1 Activate the Cisco Unified Mobile Voice Access Service in Cisco Unified Serviceability. You must activate this service on the first node in the cluster.

Step 2 Configure user accounts.

Note Make sure that you check the Enable Mobility check box and the Enable Mobile Voice Access check box in the End User Configuration window.

Note Checking the Enable Mobility check box triggers User Connect License (UCL) to provide licensing for Cisco Unified Mobility.

Step 3 Create access lists for Cisco Unified Mobility by assigning each list to the Cisco Unified Mobility user and specifying whether the list is an allowed or blocked list.

Step 4 Create remote destination profiles and assign each user to a profile.

Step 5 Associate desktop directory numbers (DNs) for the user.

Step 6 Add remote destinations by selecting the previously-defined profile as part of the configuration.

Step 7 In the Service Parameters Configuration window:

- Choose True for Enable Mobile Voice Access and enter the Mobile Voice Access Number, which is the DID number that end users use to reach Mobile Voice Access.

Note To make Mobile Voice Access calls, you must configure these service parameters and check the Enable Mobile Voice Access check box in the End User Configuration window.

- Choose True for Enable Enterprise Feature Access to enable access to hold, resume, transfer, and conference features from remote destinations.

Step 8 Configure the directory number for Mobile Voice Access.

Step 9 As an alternative, configure Enterprise Feature Access Two-Stage Dialing (also known as Enterprise Feature Access) by configuring a service parameter and the enterprise feature access DID directory number.

Note Enterprise Feature Access provides the same functionality as Mobile Voice Access but does not support the IVR component. Also, Enterprise Feature Access does not require configuration of the H.323 gateway nor VXML.

Step 10 Configure mobility settings for dual-mode phone handoff.

Step 11 Configure a Mobility softkey for the phone user that uses Cisco Unified Mobility.

Step 12 Configure time-of-day access for users. Use the fields in the When Cisco Unified Mobility is Enabled pane of the Remote Destination Configuration window to do so.

Related Topics

Access List Configuration and Deletion, on page 271
Remote Destination Profile Configuration, on page 274
Associate a Directory Number with a Remote Destination Profile, on page 278
About Remote Destination Setup, on page 278
Mobile Voice Access Directory Number Configuration, on page 284
Configure Enterprise Feature Access Two-Stage Dialing, on page 291
About Handoff Mobility Setup, on page 293
Mobility Softkey Configuration, on page 298

Cisco Unified Mobility Feature

This section describes the Cisco Unified Mobility feature. Administrators configure the basic setup of Cisco Unified Mobility for end users by using the Cisco Unified Communications Manager Administration windows.

Terminology

The following table provides definitions of terms that are related to Cisco Unified Mobility.

Table 31: Definitions

Term	Definition
Access List	List that determines the phone numbers that the system can pass or block from being passed to remote destinations.
Session Handoff	Transfer of session/conversations such as voice, video, and meetings between various Unified Communications clients that associate with a single user.
Enterprise Feature Access	Feature that provides the ability for users to access midcall features (Hold, Resume, Transfer, Conference, Directed Call Park), two-stage dialing, and Cisco Unified Mobility activate and deactivate from a remote destination. With this method, the user does not get prompted for keypad entries and must be aware of the required key sequence.
Cisco Unified Mobility	Feature that allows users to answer incoming calls on the desk phone or at a remote destination and to pick up in-progress calls on the desk phone or at a remote destination without losing the connection.

Term	Definition
Mobile Voice Access	Interactive voice response (IVR) system that is used to initiate two-stage dialed calls through the enterprise and to activate or deactivate Cisco Unified Mobility capabilities.
Remote Destination	Phones that are available for Cisco Unified Mobility answer and pickup and that can leverage Mobile Voice Access and Enterprise Feature Access for two-stage dialing. Remote destinations may include any of the following devices: • Single-mode mobile (cellular) phones • Smartphones • Dual-mode phones • Enterprise IP phones that are not in the same cluster as the desk phone • Home phone numbers in the PSTN.
Remote Destination Profile	Set of parameters that apply to all remote destinations for the user.
Time-of-Day Access	Feature that associates ring schedules to access lists and determines whether a call will be extended to a remote destination during the time of day when such a call is received.
Toast	A pop-up indication that expects user input.

Types of Session Handoff

Two-touch Session Handoff - In this type, no Unified Communications client proximity detection logic gets used; all devices under the same user ring and first one to accept gets the call.

List of Cisco Unified Mobility Features

This section provides a list of Cisco Unified Mobility features that administrators configure by using Cisco Unified Communications Manager Administration.

The following features, which were originally part of Cisco Unified MobilityManager, now reside in Cisco Unified Communications Manager:

- Cisco Unified Mobility - This feature enables users to manage business calls by using a single phone number to pick up in-progress calls on the desk phone and the mobile phone.
- Desktop Call Pickup - Users can switch between desk phone and mobile phone during an active call without losing the connection. Based on the needs of the moment, they can take advantage of the reliability of the wired office phone or the mobility of the mobile phone.
- Send Call to Mobile Phone(s) - Users access this feature on the IP phone via the Mobility softkey. The feature triggers a remote destination pickup, which allows the user to move an active mobility call from the user desk phone to a configured remote destination phone.

- Mobile Voice Access - This feature extends Cisco Unified Mobility capabilities by providing an interactive voice response (IVR) system to initiate two-stage dialed calls through the enterprise and activate or deactivate Cisco Unified Mobility capabilities
- Access List - Users can restrict the set of callers that cause a designated remote destination to ring on an incoming call (allowed access list) or for which the remote destinations do not ring on an incoming call (blocked access list). Each remote destination represents a mobile or other phone that can be configured to accept transfers from the desk phone for the user.

Cisco Unified Communications Manager supports the following Cisco Unified Mobility features:

- Midcall Enterprise Feature Access Support Using DTMF - You can configure DTMF feature codes as service parameters: enterprise hold (default equals *81), enterprise exclusive hold (default equals *82), resume (default equals *83), transfer (default equal *84), and conference (default equals *85).

  Note *81 specifies enterprise hold. When invoked, enterprise hold allows the user to resume the call on the desk phone. *82 specifies enterprise exclusive hold. When invoked, enterprise exclusive hold does not provide the ability to resume the call on the desk phone. If a mobility call that is on enterprise hold disconnects in this state, the user can resume the call on the desk phone. Alternatively, if a mobility call that is on enterprise exclusive hold disconnects in this state, the user cannot resume the call on the desk phone.

- Two-stage Dialing - Be aware that enterprise features are available with two-stage dialing for smartphones. Two-stage dialing allows smartphones to make outgoing calls through Cisco Unified Communications Manager if the smartphone is in business mode. The smartphone dials the Enterprise Feature Access number for Cisco Unified Communications Manager and then dials the destination number.
- Dual-mode Phone Support - Cisco Unified Mobility supports dual-mode phones.
- Manual Handoff of Calls on a Dual-mode Phone - Dual-mode devices offer an option to manually hand off calls from the PSTN to WLAN and vice versa.
- Time-of-Day Access - When the Cisco Unified Mobility feature is enabled, calls get extended to remote destinations if the associated DN is called based on time-of-day-access-based configuration.
- Directed Call Park via DTMF - This feature allows a mobile phone user to park a call by transferring the parked party to a park code, so the call can be retrieved later. The feature combines the standard Cisco Unified Communications Manager Directed Call Park feature with the DTMF feature. Support of the Directed Call Park via DTMF feature leverages the Midcall Enterprise Transfer feature.
- SIP URI Dialing - This feature supports SIP URI as an additional type of remote destination for Cisco Unified Mobility.
- Intelligent Session Control - This feature modifies the behavior of outgoing calls placed from the enterprise directly to mobile phones and anchors such calls to the user desktop number. (Prior to the implementation of this feature, if an enterprise user made a direct call to a mobile phone, the call was treated like a normal outgoing PSTN call: the call got directed to the mobile phone only, the call was not anchored to the user desk phone, and the mobile user could not invoke any mobility features.) During such calls, the user can invoke mobility features such as midcall features and Session Handoff from the user mobile phone.
- Session Handoff - This feature leverages the existing Cisco Unified Communications Manager experience by allowing the user to move voice, video, and meeting sessions and conversations between different

Unified Communications clients, such as Cisco Unified Personal Communicator (running on a PC in Softphone as well as CTI control mode), Cisco Unified Mobile Communicator (running on a mobile phone), and Cisco Unified IP Phone Series 9900 and legacy phones that are running SIP.

The conversation can be moved from mobile phone to any other Unified Communications client. All devices that the user owns and that share the same line ring or show a toast, and the call gets answered by whichever device picks it up first. Upon answer, all the other shared-line devices enter Remote in Use mode.

Note that the only client that can actually hand off a session (because it is the only client that has an anchored DTMF path back to Cisco Unified Communications Manager) is Cisco Unified Mobile Communicator. Neither Cisco Unified Personal Communicator nor 9900 series Cisco Unified IP Phones can initiate a session handoff. These devices can, however, handle an incoming session handoff.

Benefits of Cisco Unified Mobility Features

Cisco Unified Mobility allows flexible management of enterprise and mobile phone communications and provides these additional features and benefits:

- Simultaneous desktop ringing - Incoming calls ring simultaneously on the IP phone extension and the designated mobile handset. When the user answers one line, the unanswered line automatically stops ringing. Users can choose the preferred device each time that a call comes in.
- Single enterprise voice mailbox - The enterprise voice mailbox can serve as single, consolidated voice mailbox for all business, including calls to the desktop or configured remote devices. Incoming callers have a predictable means of contacting employees, and users can check multiple voice-messaging systems in less time.
- System remote access - A mobile phone for the user can initiate calls as if it were a local IP PBX extension. User-initiated calls can take advantage of local voice gateways and WAN trunking, and the enterprise can track employee call initiation.
- Caller ID - The system preserves and displays caller ID on all calls. Users can take advantage of Cisco Unified Mobility with no loss of expected IP phone features.
- Remote on/off control - User can turn Cisco Unified Mobility feature. See Cisco Unified Mobility, on page 239 for details.
- Call tracing - The system logs detailed Cisco Unified Mobility calls and provides information to help the enterprise optimize trunk usage and debug connection problems.
- Security and privacy for Cisco Unified Mobility calls - During an active Cisco Unified Mobility call, the associated desktop IP phone remains secured. The system removes access to the call from the desktop as soon as the mobile connection becomes active, which prevents the possibility of an unauthorized person listening in on the call that is bridged to the mobile phone.
- Client Matter Codes (CMC) and Forced Authorization Codes (FAC) - You can manage call access and accounting. CMCs assist with call accounting and billing for billable clients. FACs regulate the types of calls that certain users can place and force the user to enter a valid authorization code before the call is established.
- IPv6 support - Cisco Unified Communications Manager supports IPv6 addressing from mobile phones. For information about how to configure IPv6 in Cisco Unified Communications Manager, see “IPv6 for Cisco Unified Communications Manager” in the *Cisco Unified Communications Manager Features and Services Guide*.

- Session persistency - Mobile users can roam between different networks (e.g. Wi-Fi, VPN over 3G/4G) without having to re-register with Cisco Unified Communications Manager. This feature allows users to maintain registration with Cisco Unified Communications Manager in the case of network connectivity loss, allows users to transit calls from one network to another without call drops, and prevents the loss of SIP-based subscription status while users are roaming.

Cisco Unified Mobility

Cisco Unified Mobility allows users to answer incoming calls on the desk phone or mobile phone, and to pick up in-progress calls on the desk phone or mobile phone without losing the connection.

Note You can use any mobile phone, including Code Division Multiple Access (CDMA) and Global System for Mobile Communications (GSM) phones, for Cisco Unified Mobility and Mobile Voice Access. In some cases, however, you may need to modify timer settings in Cisco Unified Communications Manager to ensure compatibility. See the About Remote Destination Setup, on page 278.

Methods for Enabling and Disabling Cisco Unified Mobility

The following methods are available for enabling and disabling the Cisco Unified Mobility feature. This list provides the methods that are available to the administrator and to end users.

- Cisco Unified Communications Manager Administration windows. Menu path specifies **Device** > **Phone**, then configure the Mobility Identity of the Cisco Unified Mobile Communicator by checking the Enable Cisco Unified Mobility check box (to enable Cisco Unified Mobility) or by unchecking this check box (to disable Cisco Unified Mobility).
-
- Desk phone by using the Mobility softkey. To configure, use these menu options:
  - **Device** > **Phone**, and specify the Mobility softkey template in the Softkey Template field.
  - **Device** > **Phone**, and assign the same mobility user ID on the remote destination profile as the desk phone owner user ID.
- Mobile phone by using Mobile Voice Access (uses IVR prompts; 2 to enable or 3 to disable)
- Mobile phone by using Enterprise Feature Access (after PIN entry, 2 to enable or 3 to disable). The sequence specifies <PIN>#2# or <PIN>#3#.
- Cisco Unified Mobile Communicator client: The client offers the mobile user the option to change the user Cisco Unified Mobility status. See Enable or Disable Cisco Unified Mobility From Mobile Phone, on page 302 for details.

Cisco Unified Mobility Status

If at least one configured remote destination for a user is enabled for Cisco Unified Mobility, the user desk phone displays Cisco Unified Mobility as Enabled.

RDNIS/Diversion Header

The RDNIS/diversion header for Cisco Unified Mobility enhances this Cisco Unified Mobility feature to include the RDNIS or diversion header information on the forked call to the mobile device. Service providers and customers use the RDNIS for correct billing of end users who make Cisco Unified Mobility Cisco Unified Mobility calls.

For Cisco Unified Mobility calls, the Service Providers use the RDNIS/diversion header to authorize and allow calls to originate from the enterprise, even if the caller ID does not belong to the enterprise Direct Inward Dial (DID) range.

Example RDNIS/Diversion Header Use Case

Consider a user that has the following setup:

Desk phone number specifies 89012345.

Enterprise number specifies 4089012345.

Remote destination number specifies 4088810001.

User gets a call on desk phone number (89012345) that causes the remote destination (4088810001) to ring as well.

If the user gets a call from a nonenterprise number (5101234567) on the enterprise number (4089012345), the user desk phone (89012345) rings, and the call gets extended to the remote destination (4088810001) as well.

Prior to the implementation of the RDNIS/diversion header capability, the fields populated as follows:

Calling Party Number (From header in case of SIP): 5101234567

Called Party Number (To header in case of SIP): 4088810001

After implementation of the RDNIS/diversion header capability, the Calling Party Number and Called Party Number fields populate as before, but the following additional field gets populated as specified:

Redirect Party Number (Diversion Header in case of SIP): 4089012345

Thus, the RDNIS/diversion header specifies the enterprise number that is associated with the remote destination.

Configuration of RDNIS/Diversion Header in Cisco Unified Communications Manager Administration

To enable the RDNIS/diversion header capability for Cisco Unified Mobility calls, ensure the following configuration takes place in Cisco Unified Communications Manager Administration:

All gateways and trunks must specify that the Redirecting Number IE Delivery — Outbound check box gets checked.

In Cisco Unified Communications Manager Administration, you can find this check box by following the following menu paths:

- For H.323 and MGCP gateways, execute Device > Gateway and find the gateway that you need to configure. In the Call Routing Information - Outbound calls pane, ensure that the Redirecting Number IE Delivery - Outbound check box gets checked. For T1/E1 gateways, check the Redirecting Number IE Delivery - Outbound check box in the PRI Protocol Type Information pane.
- For SIP trunks, execute Device > Trunk and find the SIP trunk that you need to configure. In the Outbound Calls pane, ensure that the Redirecting Diversion Header Delivery - Outbound check box gets checked.

Use Case Scenarios for Cisco Unified Mobility

See the Use Case Scenarios for Cisco Unified Mobility, on page 252 for the use case scenarios that Cisco Unified Communications Manager supports with this feature.

Desktop Call Pickup

User can perform desktop call pickup on in-progress mobility calls either by hanging up the call on the mobile phone or by putting the mobility call on hold with the midcall hold feature. When hanging up or ending the call at the mobile phone, the user can then resume the call on the desk phone within 10 seconds (default). When the remote destination hangs up, Cisco Unified Communications Manager puts the associated desk phone in Hold state, which allows the user to resume the call by pressing the Resume softkey. The Maximum Wait Time for Desk Pickup setting on the End User Configuration window determines the amount of time the call remains on hold after the hang-up at the remote destination. The default specifies 10000 milliseconds (10 seconds).

Alternatively, the user can also perform desktop call pickup by placing the call on the mobile phone on enterprise hold with the midcall hold feature (*81) and then resuming the call on the desk phone. When Cisco Unified Communications Manager receives the *81, Cisco Unified Communications Manager places the associated desk phone in a Hold state so the user can resume the call. Note that with this method, the Maximum Wait Time for Desk Pickup timer does not apply to the hold state and the call gets held indefinitely until the user resumes the call.

Send Call to Mobile Phone

Users can perform remote destination pickup on in-progress mobility calls by using the Send Call to Mobile Phone feature. To do so, users press the Mobility softkey on the desk phone and select Send Call to Mobile Phone, which generates calls to all of the remote destinations that are configured. Users can then answer this call at the desired remote destination and continue the call.

When a desk phone invokes the Send Call to Mobile Phone feature and the remote destination specifies a dual-mode smartphone, the following behavior results:

- If the dual-mode smartphone is registered to Wi-Fi, the call is sent to the device on the Wi-Fi side.
- If the dual-mode smartphone is not registered to Wi-Fi, the call is sent to the device on the cellular side.

Mobile Voice Access

Mobile Voice Access extends Cisco Unified Mobility capabilities by allowing users to originate a call from a remote destination such as a mobile phone as if dialing from the desk phone. A remote destination represents a phone that is designated as available for Cisco Unified Mobility answer and pickup. The user dials Mobile Voice Access from the remote destination. The system prompts the user for the PIN that is assigned to the user in Cisco Unified Communications Manager. After being authenticated, the user can make a call by using the same dialing methods that would be available if the user originated the call from the enterprise desk phone.

When Mobile Voice Access is called, the system prompts the user for the originating phone number in addition to the PIN if any of the following statements is true:

- The number from which the user is calling does not represent one of the remote destinations for the user.
- The user or the carrier for the user blocks the number (shown as “Unknown Number”).

- The number does not get accurately matched in the Cisco Unified Communications Manager database; for example, if the number is 510-666-9999, but it is listed as 666-9999 in the database, or the number is 408-999-6666, but it is entered as 1-408-999-6666 in the database.

- Mobile Voice Access gets configured in hairpin mode. (When Mobile Voice Access that is configured in hairpin mode is used, users who are calling the system do not get identified automatically by their caller ID. Instead, users must manually enter their remote destination number prior to entering their PIN number.)

If the user incorrectly enters any requested information (such as mobile phone number or PIN) three times in a row, the Mobile Voice Access call can disconnect, and the system will lock out the user for a period of time. (The credential information for the user controls the allowed number of login attempts.)

Note Mobile Voice Access uses the first locale that displays in the Selected Locales pane in the Mobile Voice Access window in Cisco Unified Communications Manager Administration (**Media Resources** > **Mobile Voice Access**) when the IVR is used. For example, if English United States displays first in the Selected Locales pane, the Cisco Unified Mobility user receives English when the IVR is used during a call.

See the Use Case Scenarios for Mobile Voice Access, on page 252 for the use case scenarios that Cisco Unified Communications Manager supports with this feature.

Midcall Enterprise Feature Access Support

Users can leverage enterprise media resources and capabilities by invoking midcall features. DTMF digits that are relayed from the remote destination in-band in the audio path and then relayed out-of-band from the enterprise gateway to Cisco Unified Communications Manager invoke midcall features. When Cisco Unified Communications Manager receives the DTMF digits, appropriate midcall features get facilitated based on the DTMF digit sequence. Such features include adding or remove call legs for transferred or conferenced calls, as well as invoking media resources like music on hold for held calls and conference bridges as required.

The feature access codes that are configured within Cisco Unified Communications Manager under Service Parameters determine the midcall feature DTMF code sequences.

Two-Stage Dialing

The user can originate calls from the remote destination phone through the enterprise by leveraging the enterprise telephony infrastructure. Two-stage dialing provides the following benefits:

- The ability to make calls through the enterprise, which leads to centralized billing and call detail records. This ability provides the potential for cost savings by ensuring that international calls get billed to the enterprise rather than to the mobile or cellular plan. However, this capability does not eliminate normal per-minute local/long-distance charges at the mobile phone.

- The ability to mask the mobile phone number from the far-end or dialed phone. Instead of sending the mobile number to the called party, the user enterprise number gets sent to the called party during a two-stage dialed call. This method effectively masks the user mobile number and ensures that returned calls get anchored in the enterprise.

Time-of-Day Access

An access list determines whether a call should be extended to a remote destination that is enabled for the Cisco Unified Mobility feature. With the addition of time-based control, the Time-of-Day Access feature adds time as another determination factor. The feature allows administrators and users to determine whether a call should reach a remote destination based on the time of day when the call is received.

For calls to remote destinations, the Time-of-Day Access feature adds a ring schedule and associates the ring schedule with an access list to determine the time-of-day access settings for a remote destination.

The provisioning process includes provisioning the following entities:

- Access lists
- Remote destinations (configuring a ring schedule and associating the ring schedule with an access list for a remote destination)

As an extension to the existing access list feature, ensure the Time-of-Day Access feature is accessible to end users of Cisco Unified Communications Manager. Therefore, you can provision the feature through use of both Cisco Unified Communications Manager Administration (by administrators) and Cisco Unified Communications Self Care Portal (by end users).

Use case scenarios are provided for the time-of-day access feature with Cisco Unified Mobility, including migration considerations when migrating from a release of Cisco Unified Communications Manager prior to Release 7.0(x) or later.

Related Topics

Use Case Scenarios for Time-of-Day Access, on page 252

Time-of-Day Access Configuration

Perform the following steps to configure the Time-of-Day Access feature for Cisco Unified Mobility.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, configure an end user for whom you will enable the Time-of-Day Access feature. Use the **User Management** > **End User** menu option.

Note Make sure that you check the Enable Mobility check box in the End User Configuration window.

Note Checking the Enable Mobility check box triggers licensing to consume device license units (DLUs) for Cisco Unified Mobility.

Step 2 For a particular user, configure access lists to use for Time-of-Day Access by assigning each list to the user. Create separate access lists for callers that are allowed and callers that are blocked. Use the **Call Routing** > **Class of Control** > **Access List** menu option.

Note An access list must have an owner. No system access list exists.

Step 3 Create remote destination profiles and assign each user to a profile.

Step 4 Configure a remote destination for a user. Remote destinations represent the mobile (or other) phones that can accept Cisco Unified Mobility calls and calls that are moved from the desk phone. Remote destinations can initiate calls by using Mobile Voice Access. Use the **Device** > **Remote Destination** menu option.

Note The same configuration also applies to dual-mode phones and to Cisco Unified Mobile Communicator Mobility Identity to set up time-of-day access.

For successful time-of-day access configuration, you must configure the following areas in the Remote Destination Configuration window:

- Use the Ring Schedule pane to configure a ring schedule for the remote destination.
- Use the When receiving a call during the above ring schedule pane to specify the access list for which the Ring Schedule applies.

Checking the Enable Cisco Unified Mobility check box for the remote destination enables Cisco Unified Mobility to apply the settings in the When Cisco Unified Mobility is Enabled pane to calls that are made to this remote destination. If the Enable Cisco Unified Mobility check box is not checked, the settings do not apply to incoming calls to this remote destination, but the settings remain intact for future use.

Related Topics

Access List Configuration and Deletion, on page 271

Remote Destination Profile Configuration, on page 274

About Remote Destination Setup, on page 278

Additional Information for Time-of-Day Access

The following important notes apply to time-of-day access configuration:

- A ring schedule associates with the time zone of a remote destination, not with the time zone of the Cisco Unified Communications Manager server. Use the Time Zone field in the Remote Destination Configuration window to specify the time zone of the remote destination.
- If a remote destination has no time-of-day access configuration, all calls get extended to the remote destination. By default, the All the time ring schedule radio button and the Always ring this destination radio button are checked, so that all calls get extended to the remote destination.
- Cisco recommends that you always configure an access list with members; avoid creating an empty access list that contains no members. If an empty access list is chosen in the Ring this destination only if the caller is in drop-down list box, all calls get blocked (instead of allowed). If an empty access list is chosen in the Do not ring this destination if the caller is in drop-down list box, all calls are allowed during the specified ring schedule. Either use of an empty access list could cause unnecessary confusion for end users.

See the Use Case Scenarios for Time-of-Day Access, on page 252 for the use case scenarios that Cisco Unified Communications Manager supports with this feature.

See the user guide for the applicable Cisco Unified IP Phone model for details of the settings that end users can configure to customize their time-of-day access settings by using the Cisco Unified Communications Self Care Portal windows.

Directed Call Park via DTMF

A user can park an existing call by using DTMF digits. Using Directed Call Park from the mobile phone, a user parks a call and inputs a unique mobility user park code. The user can subsequently retrieve the call with the code or have someone else retrieve the call with the code. This feature proves useful for certain vertical markets that require different departments or users to pick up calls.

When a user is in the enterprise and picks up a call on their mobile phone, they may want to pick the call up on a Cisco Unified IP Phone in a conference room or desk where the DN is not visible. The user can park the call and pick up the parked call with only their code.

When the mobile phone user is on an active call, the user can park the call by transferring the parked party to the park code that the system administrator configures and assigns to the user. The dialing sequence resembles the DTMF transfer sequence, except that a preconfigured parking code replaces the transfer number.

Example of Directed Call Park via DTMF - Parking the Call

In the following example, *82 specifies enterprise exclusive hold, *84 specifies transfer, the pin specifies 12345, and the call park code specifies 3215. The following actions take place from the mobile phone:

1. Dial *82 (to put the call on enterprise exclusive hold).
2. If necessary, put the mobile phone call on Hold, depending on the mobile phone model.
3. Make a new call to the Enterprise Feature Access DID.

Note This same DID gets used for the Enterprise Feature Access two-stage dialing feature. Configure this DID with the Call Routing > Mobility > Enterprise Feature Access Configuration menu option.

1. After the call connects, dial the following field-and-digit sequence: <PIN>#*84#<Park Code>#*84#
2. For example, if the PIN specifies 12345 and park code specifies 3215, the digit sequence would be 12345#*84#3215#*84#

Cisco Unified Communications Manager puts the parked party on hold.

Note The caller ID of the mobile phone must get passed to the enterprise and must match a configured remote destination when the user dials the Enterprise Feature Access DID to invoke this feature. If no caller ID exists or no caller ID match occurs, the user cannot invoke this feature.

After Cisco Unified Communications Manager receives the dialed park code digit, the digit analysis engine verifies whether the dialed park code digits are valid. If so, the Directed Call Park feature intercepts the park code and verifies whether the park code is available. If the dialed park code is valid and available, the parking party receives the ringback tone, and the secondary call terminates to a Cisco Unified Communications Manager generic device that associates with the selected park code. The generic device automatically answers and place the parking party on hold with music on hold (MOH) or tone on hold. The last *84 completes the transfer of the parked party to the Cisco Unified Communications Manager generic device that associates with the selected park code. After the transfer completes, the parked party receives the MOH or tone on hold, and the parked party gets parked on this selected park code and waits for retrieval.

If another user is already using the user-specified park code, Directed Call Park feature logic in Cisco Unified Communications Manager rejects that selected park code. The user gets to select another park code.

If the user-specified park code is not valid, Cisco Unified Communications Manager plays reorder tone to the parking party.

For the Directed Call Park feature, be aware that the park code and code range are configurable throughout the system. Every Cisco Unified Communications Manager server in the system shares the park code and code range.

Example of Directed Call Park via DTMF - Retrieving the Parked Call

When a user attempts to retrieve the parked call, the user can go off hook on another mobile phone, and the user must use two-stage dialing to dial a digit string that contains the Directed Call Park retrieval prefix digits (for example, 22) plus the park code/code range (for example, 3215). The following sequence of events takes place:

1. Dial Enterprise Feature DID on mobile phone.
2. Upon connection, dial the following field-and-digit sequence to retrieve the parked call:
3. <PIN>#1#<Retrieval Prefix><Park Number>#
4. In our example, the full sequence specifies 12345#1#223215# to retrieve the parked call.

Just like the existing Call Park feature, if the call does not get retrieved on time, the parked call reverts back to the phone number that is associated with the parking party by default.

If a shared line is configured for the phone line of the parking party, all phones that are associated with the shared line will ring. In addition, the dPark feature allows the administrator to configure a call park reversion number in the Directed Call Park Configuration window, so if the call park reversion number is configured, the non-retrieved call reverts to this number, instead of to the parking party number.

See the Use Case Scenarios for Directed Call Park via DTMF, on page 253 for the use case scenarios that Cisco Unified Communications Manager supports with this feature.

SIP URI Dialing

This feature supports Session Initiation Protocol (SIP) Universal Resource Identifier (URI) as an additional type of remote destination for Cisco Unified Mobility. When the DN is called, Cisco Unified Communications Manager extends the call to a SIP trunk that digit analysis selects with this SIP URI in the To: header.

This feature only allows routing that is based only on the domain name, not based on the full SIP URI.

When a remote destination of this type is configured, other Cisco Unified Mobility features, such as two-stage dialing, transformation to DN number when calling into Cisco Unified Communications Manager, Interactive Voice Response (IVR) support, caller ID match, or DTMF transfer and conferencing, do not get supported.

SIP URI Administration Details

The SIP URI dialing feature entails a relaxation of the business rules to allow the entry of a URI in the Destination Number field of the Remote Destination Configuration window. (From the Cisco Unified Communications Manager Administration menu bar, choose the **Device** > **Remote Destination** menu option.)

An additional requirement for this feature specifies that a SIP route pattern that matches the configured URI domain must be configured for the feature to work. To configure a SIP route pattern, from the Cisco Unified Communications Manager Administration menu bar, choose the **Call Routing** > **SIP Route Pattern** menu option.

SIP URI Example

For a remote destination, the SIP URI user@corporation.com gets configured. A SIP route pattern that specifies corporation.com must also get configured for the SIP URI remote destination to resolve correctly.

Intelligent Session Control

This feature modifies the behavior of outgoing calls placed from the enterprise directly to mobile phones and anchors such calls to the user desktop number. (Prior to the implementation of this feature, if an enterprise user made a direct call to a mobile phone, the call was treated like a normal outgoing PSTN call: the call got directed to the mobile phone only and the mobile user could not invoke any mobility features.)

An outgoing call from the enterprise to a remote destination exhibits the following behavior:

- Mobile user can use DTMF to invoke midcall features, such as Hold, Resume, Transfer, and Conference.
- Mobile user can hang up the call from the mobile phone and pick the call up from the user desk phone.
- A direct call to a remote destination from the enterprise gets anchored to the user desk phone; and the time-of-day access, Do Not Disturb, and Delay Before Ringing settings that are configured in the associated remote destination profile get ignored. The direct call goes immediately to the mobile user.
- Direct calls to remote destinations behave similarly to calls incoming to Cisco Unified Communications Manager from mobile users. Mobile users have access to the following mobility features:
    - Midcall features (Hold, Resume, Transfer, Conference)
    - Session Handoff
    - Call anchoring

Feature Configuration

Basic configuration of the Intelligent Session Control feature requires that the administrator configure the value of the Reroute Remote Destination Calls to Enterprise Number service parameter as True.

Note For IP Multimedia Subsystem (IMS), ensure that the Cisco Unified Mobility feature is enabled in the Remote Destination Configuration window, or by using one of the other methods prescribed for enabling Cisco Unified Mobility, before implementing Intelligent Session Control call processing.

To access the Reroute Remote Destination Calls to Enterprise Number service parameter, execute **System** > **Service Parameters** in Cisco Unified Communications Manager Administration. In the Service Parameter Configuration window that displays, specify a server and the Cisco CallManager service. The following service parameters are found in the Clusterwide Parameters (Feature - Reroute Remote Destination Calls to Enterprise Number) pane:

- Reroute Remote Destination Calls to Enterprise Number - To enable the feature, specify the value for this service parameter as True. When this parameter is enabled, all outgoing calls to a remote destination get anchored in the enterprise number with which the remote destination associates.
- Log Mobile Number in CDR for Rerouted RD Calls - This service parameter determines whether to log the mobile number or the enterprise number in the call detail record (CDR) when outgoing calls to the remote destination get anchored. If set to False, the enterprise number gets logged. If set to True, the mobile number gets logged.

- Ignore Call Forward All on Enterprise DN - This service parameter determines whether to ignore the call forward all (CFA) setting that is configured on the enterprise number when outgoing calls to the remote destination get anchored. If set to True, the CFA gets ignored; if set to False, the CFA setting gets applied.

The following service parameters, found in the Clusterwide Parameters (System - Mobility) pane, also affect the behavior of the Intelligent Session Control feature:

- Matching Caller ID with Remote Destination - If this service parameter is set to Complete Match, all digits of the calling number must match for the call to connect to the remote destination. If this service parameter is set to Partial Match, partial matches are allowed and the Number of Digits for Caller ID Partial Match service parameter applies.
- Number of Digits for Caller ID Partial Match - The number of digits that this service parameter specifies applies to partial matches if the Matching Caller ID with Remote Destination service parameter is set to Partial Match.

Note For each service parameter, click the service parameter name in Cisco Unified Communications Manager Administration for a complete definition of that service parameter.

Use case scenarios are provided for the Intelligent Session Control feature with Cisco Unified Mobility.

Additional Call Processing Details for Intelligent Session Control

If more than one line is configured for the matching remote destination profile for the dialed number, Cisco Unified Communications Manager uses the first matched line to route the call. Because the direct call to mobile number gets matched against the enterprise number, all enterprise number intercepts are honored, including Call Intercept on enterprise number when Call Intercept gets supported for enterprise number. The forward all intercept on enterprise number gets ignored based on the service parameter, Ignore Forward All on Enterprise DN. If this service parameter is set to true, Cisco Unified Communications Manager ignores forward all intercept on enterprise number and still directs the call to the mobile phone. If this service parameter is set to false, Cisco Unified Communications Manager still enables CFA setting on enterprise number and, if configured, sends the call to CFA destination.

This feature does not anchor direct calls to mobile number if the call to mobile number gets sent via an overlap-sending-enabled trunk or gateway. In this case, the call to mobile number does not get anchored.

See the limitations topic for additional restrictions that apply to this feature.

Troubleshooting the Intelligent Session Control Feature

Perform the following checks if the Intelligent Session Control feature does not function as expected:

- Ensure that the Intelligent Session Control is set to True in the Service Parameter Configuration window.
- Ensure that the Cisco Unified Mobility feature is enabled in the Remote Destination Configuration window, or by using one of the other methods prescribed for enabling Cisco Unified Mobility, before implementing Intelligent Session Control call processing for IP Multimedia Subsystem.
- Ensure that the caller ID matches the remote destination number as specified by the Matching Caller ID with Remote Destination setting (either complete match or partial match).

- Ensure that a trace line such as the following prints in the Cisco Unified Communications Manager SSI log after the number gets dialed:

  10/14/2008 15:09:26.507 CCM|Digit analysis: getDaRes - Remote Destination [9725782583]|*^*^*

- Ensure that the enterprise number Line Association check box is checked in the Remote Destination Configuration window (**Device** > **Remote Destination**).
- Ensure that the route pattern partition is part of the calling search space (CSS) that is configured as Rerouting CSS in the Remote Destination Profile Configuration window (**Device** > **Device Settings** > **Remote Destination Profile**).

Related Topics

Interactions, on page 258
Limitations, on page 260
Use Case Scenarios for Intelligent Session Control, on page 254

Session Handoff

The complete Session Handoff feature can move a single call, a conference, and session collaboration among mobile phone, PC, and desk phone. Session Handoff enables a user to move conversations from user mobile phone to user desk phone. Two-touch Session Handoff uses two user inputs: one at the initiating party to hand off and the other at the terminating party to accept.

The major benefit of the Session Handoff feature over Desktop Pickup is that the original conversation can be continued until the handed off call gets answered.

Configuration of the Session Handoff feature entails configuration of specific service parameters and configuration of the mobile device that will hand off calls.

Session Handoff Service Parameters

To configure service parameters in Cisco Unified Communications Manager Administration, choose the **System** > **Service Parameters** menu option. From the Server drop-down list box, choose a server. From the Service drop-down list box, choose the Cisco CallManager service.

The following service parameters must be configured to enable the Session Handoff feature:

- Session Handoff Alerting Timer - This service parameter, found in the Clusterwide Parameters (Device - General) pane, determines the length of time that the session handoff call alerts. The default value specifies 10 seconds, and valid values range from 1 to 999 seconds.
- Enterprise Feature Access Code for Session Handoff - This service parameter, found in the Clusterwide Parameters (System - Mobility) pane, specifies the DTMF feature code to trigger session handoff. The default value specifies *74.

For additional details about these service parameters, click the name of the service parameter in the Service Parameter Configuration window in Cisco Unified Communications Manager Administration, which provides a hyperlink to a complete definition of the service parameter.

Mobility Device Configuration for Session Handoff Feature

Perform the following configuration for the mobility device to enable the Session Handoff feature:

- Configure the directory number in remote destination profile and the desk phone shared line so that line-level directory number and partition match.

- Assign the same mobility user ID on the remote destination profile as the desk phone owner user ID to allow session handoff.
- To configure the Session Handoff feature for basic Cisco Unified Mobility users, the User ID field setting in the Remote Destination Configuration window should match the Owner User ID field on the (desk) phone configuration window.
- To configure the Session Handoff feature for Cisco Unified Mobile Communicator users, both the Owner User ID and the Mobility User ID fields in the Cisco Unified Mobile Communicator device configuration window must match the Owner User ID field on the desk phone configuration window.

Impact of Session Handoff on Other Features

When the user hands off a call, a new call gets presented on the desk phone. While the desk phone is flashing, the following features do not get triggered on the desk phone for the call that was handed off:

- iDivert
- Call Forward All
- DND
- Call Forwarding

If the user hands off a call and does not answer from the desk phone within the time that the Session Handoff Alerting Timer service parameter specifies, the existing Remote In Use state on the desk phone gets lost.

Thus, the desk phone loses shared-line functionality following session handoff. The user cannot perform midcall features for that call, such as Hold from Mobile (using *81) and Resume from desk, or desk pickup. The user can hand off the call again, however, to resume it from the desk phone.

Troubleshooting Information for Session Handoff Feature

If a call that is handed off from a mobile phone does not flash the desk phone, perform the following checks:

- Check whether Owner User ID for the desk phone matches the User ID of Remote Destination Profile.
- In service parameters, check whether Enable Enterprise Feature Access is set to True; also, check whether other DTMF features (Hold [*81], Resume [*83]) are working.
- Check the Session Handoff DTMF code (default specifies *74) and Session Handoff Alerting Timer (default specifies 10 seconds) values.

Related Topics

Limitations, on page 260
Use Case Scenarios for Session Handoff, on page 256

Session Persistency

Session Persistency enhances the mobile user experience while roaming. Session Persistency allows mobile users with supported mobile devices to do the following:

- Roam between different networks (e.g. Wi-Fi, VPN over 3G/4G) without having to re-register with Cisco Unified Communications Manager.

- Maintain the SIP-based subscription status with Cisco Unified Communications Manager while roaming between different networks.
- Maintain registration with Cisco Unified Communications Manager in the case of network connectivity loss.
- Seamlessly transit both active and held calls from one network to another without call drops.

To facilitate connectivity during roaming between networks, Session Persistency allows dynamic IP address/port change via keep-alive registration to facilitate connectivity during roaming between networks. In addition, the feature includes a configurable TCP reconnect timer, which must be enabled at the product level, to allow mobile users to remain connected in case of a temporary network connectivity loss or roaming. The timer is in effect only when the mobile device tears down the original TCP connection explicitly.

To leverage the Session Persistency feature, mobile devices must comply with Cisco-defined SIP interfaces.

TCP Reconnect Timer Configuration

If the TCP reconnect timer has been enabled at the product level, you can configure the timer by setting a value for the Time to Wait for Seamless Reconnect After TCP Drop or Roaming field from any of the following configuration windows:

- Phone Configuration window
- Common Phone Profile window
- Enterprise Phone Configuration window

NextGen Mobile Clients with QoE

If a device that shares the same user identification and is associated with a Hunt Group, signs out of the Hunt Group, then SNR calls are not sent out to the associated mobile device.

Cisco Unified Communications Manager 9.0 extends the Log Out of Hunt Groups capability onto your mobile device. This allows it to function in the same way as your desk phone. When you use the Hlog softkey via your mobile client to Log Out of the Hunt Group, you no longer receive calls placed to the Hunt Pilot.

Cisco Unified Communications Manager 9.0 provides TLS/SRTP support for dual-mode smart phones. TLS establishes the same secure and reliable data transfer mode for mobile phones as for IP phones, and SRTP encrypts voice conversations.

Use Case Scenarios for Cisco Unified Mobility Features

Use cases are provided for the following Cisco Unified Mobility features that are supported by Cisco Unified Communications Manager:

- Mobile Connect
- Mobile voice access
- Time-of-Day access
- Directed Call park via DTMF
- intelligent session control
- session handoff

Use Case Scenarios for Cisco Unified Mobility

Cisco Unified Mobility supports these use case scenarios:

- Receiving an outside call on desk phone or mobile phone - An outside caller dials the user desktop extension. The desk phone and mobile phone ring simultaneously. When the user answers one phone, the other phone stops ringing. The user can switch from the desk phone to a mobile phone during a call without losing the connection. Switching gets supported for incoming and outgoing calls.
- Moving back from a mobile phone to a desk phone - If a call was initiated to or from the desk phone and then shifted to the mobile phone, the call can get shifted back to the desk phone.
- Using midcall enterprise features - During a Cisco Unified Mobility call, users can perform midcall functions, including hold/resume, exclusive hold, transfer, directed call park, and conference.

Use Case Scenarios for Mobile Voice Access

Mobile Voice Access supports these use case scenarios:

- Initiating a mobility call from a remote phone, such as a mobile phone - Users can use Mobile Voice Access to initiate calls from a mobile phone as if dialing from the desk phone.
- Moving from a mobile phone to a desk phone during a mobile-phone-initiated call - If the user initiated a call from a mobile phone by using Mobile Voice Access, the user can shift to the desk phone during the call without losing the connection and can shift back again as needed.

Use Case Scenarios for Time-of-Day Access

The use case scenarios that follow detail the function of the time-of-day access feature with activated access lists that were configured prior to the addition of the time-of-day access feature; the use case scenarios also cover new provisioning that takes place for the feature starting with Release 7.0(1) of Cisco Unified Communications Manager.

Supported Use Cases for Migrating Activated Access Lists from an Earlier Cisco Unified Communications Manager Release

The following use cases detail the function of the Time-of-Day Access feature with Cisco Unified Mobility when migration of an activated access list from a previous release of Cisco Unified Communications Manager to Release 7.0(x) or later takes place.

- Use Case #1 - No allowed or blocked access list got configured prior to Release 7.0(x) of Cisco Unified Communications Manager.

  Result after migration: The system allows all calls at all hours. The Remote Destination Configuration window displays the When Cisco Unified Mobility is Enabled pane. In the Ring Schedule pane, the All the time radio button is checked. In the When Receiving a call during the above ring schedule pane, the Always ring this destination radio button is checked.

- Use Case #2 - Only an allowed access list got configured prior to Release 7.0(x) of Cisco Unified Communications Manager.

  Result after migration: Only the callers that belong to the allowed access list can reach the associated remote destination. The Remote Destination Configuration window displays the When Cisco Unified Mobility is Enabled pane. In the Ring Schedule pane, the All the time radio button is checked. In the When Receiving a call during the above ring schedule pane, the Ring this destination only if caller is in radio button is checked, and the access list displays in the corresponding drop-down list box.

- Use Case #3 - Only a blocked access list got configured prior to Release 7.0(x) of Cisco Unified Communications Manager.

  Result after migration: The callers that belong to the blocked access list cannot reach the associated remote destination, but all other callers can call the remote destination at all hours. The Remote Destination Configuration window displays the When Cisco Unified Mobility is Enabled pane. In the Ring Schedule pane, the All the time radio button is checked. In the When Receiving a call during the above ring schedule pane, the Do not ring this destination if caller is in radio button is checked, and the access list displays in the corresponding drop-down list box.

Use Cases for Time-of-Day Access with the Current Cisco Unified Communications Manager Release

The following use cases detail the function of the Time-of-Day Access feature with Cisco Unified Mobility with the current release of Cisco Unified Communications Manager:

- Use Case #4 - Only allow calls during business hours.

  Configuration: Configure a ring schedule that specifies business hours from Monday to Friday and choose the Always ring this destination radio button.

  Result: The system allows all callers during business hours, but no calls get extended to this remote destination outside business hours.

- Use Case #5 - Only allow calls from certain numbers (for example, from coworkers) during business hours.

  Configuration: Configure a ring schedule that specifies business hours from Monday to Friday, choose the Ring this destination only if the caller is in radio button, and specify an access list.

  Result: Only callers that belong to the access list can call the remote destination during business hours; all other callers get blocked during business hours. Outside business hours, no calls ring this remote destination.

- Use Case #6 - Block certain numbers (for example, 1800 numbers) during business hours.

  Configuration: Configure a ring schedule that specifies business hours from Monday to Friday, choose the Do not ring this destination if caller is in radio button, and specify an access list.

  Result: Only callers that belong to the access list get blocked from calling the remote destination during business hours; all other callers can call the remote destination during business hours. Outside business hours, no calls ring this remote destination.

Use Case Scenarios for Directed Call Park via DTMF

The Directed Call Park via DTMF feature of Cisco Unified Mobility supports the following use cases:

- Mobile phone user parks call on selected park code.
- Mobile phone user parks call on selected park code that is unavailable.
- Mobile phone user parks call on selected park code that is invalid.
- Mobile phone user fails to enter park code after entering the DTMF transfer code.
- Parked party disconnects while the parking party attempts to park the call.
- Parked party disconnects while it is parked on a selected park code and is waiting for retrieval.
- User dials Directed Call Park retrieval digits plus a park code that has not been occupied.

- Administrator configures a translation pattern, so the length of the string of digits to park a call and the length of the string to retrieve a call are the same.
- User retries a parked call.
- A parked call reverts.
- While a park code is occupied, one of the following entities gets modified or deleted: the park code or code range, the Directed Call Park park-prefix digits, or the Directed Call Park retrieval-prefix digits.
- Directed call park gets specified when the network is partitioned.

Use Case Scenarios for Intelligent Session Control

The Intelligent Session Control feature supports these use case scenarios:

- The Reroute Remote Destination Calls to Enterprise Number service parameter is set to False.
- The Reroute Remote Destination Calls to Enterprise Number service parameter is set to True.
- The Ignore Call Forward All on Enterprise DN service parameter is set to False.

The following sections discuss the configuration that takes place in order to demonstrate each user case for the Intelligent Session Control feature.

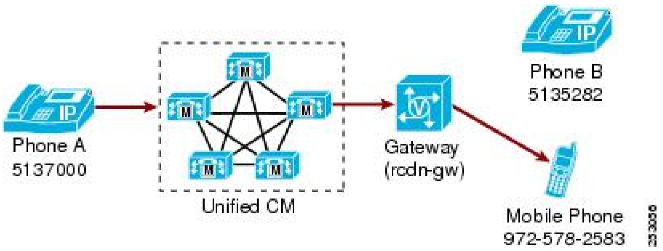
Use Case 1: Reroute Remote Destination Calls to Enterprise Number Service Parameter Is Set to False

In this use case, the following configuration takes place prior to the placement of the direct call from Cisco Unified Communications Manager to the remote destination:

1. Reroute Remote Destination Calls to Enterprise Number service parameter is set to False.
2. Number of Digits for Caller ID Partial Match service parameter specifies 7 digits for partial match.
3. Phone A DN specifies 5137000.
4. Phone B DN specifies 5135282 with owner user ID gbuser1 and remote destination (RD) specifies 9725782583.
5. Route pattern 9.XXXXXXXXXX with DDI as PreDot.
6. Route pattern points to the rcdn-gw gateway.

The following figure illustrates the setup for the direct call to the remote destination when the Reroute Remote Destination Calls to Enterprise Number service parameter is set to False.

Figure 14: Use Case 1: Reroute Remote Destination Calls to Enterprise Number Service Parameter Is Set to False



The following action initiates the feature behavior in this use case:

- Phone A DN 5137000 user calls the mobile phone by dialing 05782583.

The following call processing takes place:

1. The translation pattern gets matched and the called number gets transformed to 99725782583.
2. The route pattern 9.XXXXXXXXXX gets matched.
3. After the route pattern removes the leading (PreDot) 9, the number specifies 9725782583.
4. No remote destination mapping to enterprise number occurs.
5. The call extends only to the mobile user via the gateway: the call does not get anchored at the enterprise number with which this remote destination associates.

Use Case 2: Reroute Remote Destination Calls to Enterprise Number Service Parameter Is Set to True

In this use case, the following configuration takes place prior to the placement of the direct call from Cisco Unified Communications Manager to the remote destination:

1. Reroute Remote Destination Calls to Enterprise Number service parameter is set to True.
2. Number of Digits for Caller ID Partial Match service parameter specifies 7 digits for partial match.
3. Phone A DN specifies 5137000.
4. Phone B DN specifies 5135282 with owner user ID gbuser1 and remote destination (RD) specifies 9725782583.
5. Route pattern 9.XXXXXXXXXX with DDI as PreDot.
6. Translation pattern 0.XXXXXXX with DDI as PreDot and prefix digits specify 9972.
7. Route pattern points to the rcdn-gw gateway.

The following action initiates the feature behavior in this use case:

- Phone A DN 5137000 user calls the mobile phone by dialing 05782583.

The following call processing takes place:

1. The translation pattern gets matched and the called number gets transformed to 99725782583.
2. The route pattern 9.XXXXXXXXXX gets matched.
3. After the route pattern removes the leading (PreDot) 9, the number specifies 9725782583.
4. Remote destination mapping to enterprise number matches the configured remote destination for phone B.
5. The call gets anchored at the enterprise number of the called user and the call extends to the user remote destination.
6. Phone B enters Remote In Use (RIU) state after the mobile user answers the call.

Use Case 3: Ignore Call Forward All on Enterprise DN Service Parameter Is Set to False

In this use case, the following configuration takes place prior to the placement of the direct call from Cisco Unified Communications Manager to the remote destination:

1. Reroute Remote Destination Calls to Enterprise Number service parameter is set to True.
2. Ignore Call Forward All on Enterprise DN service parameter is set to False.
3. Number of Digits for Caller ID Partial Match service parameter specifies 7 digits for partial match.
4. Phone A DN specifies 5137000.
5. Phone B DN specifies 5135282 with owner user ID gbuser1 and remote destination (RD) specifies 9725782583. Call Forward All setting for phone B specifies forwarding to phone C with DN 5138000.
6. Route pattern 9.XXXXXXXXXX with DDI as PreDot.
7. Translation pattern 0.XXXXXXX with DDI as PreDot and prefix digits specify 9972.
8. Route pattern points to the rcdn-gw gateway.

The following action initiates the feature behavior in this use case:

- Phone A DN 5137000 user calls the mobile phone by dialing 05782583.

The following call processing takes place:

1. The translation pattern gets matched and the called number gets transformed to 99725782583.
2. The route pattern 9.XXXXXXXXXX gets matched.
3. After transformation, the number specifies 9725782583.
4. Remote destination mapping to enterprise number matches the configured remote destination for phone B.
5. The call gets redirected to the enterprise number of the user and goes to phone B instead of to the mobile phone.
6. Because of the setting of the Ignore Call Forward All on Enterprise DN service parameter to False, the call gets forwarded from phone B to phone C.

Use Case Scenarios for Session Handoff

The Session Handoff feature supports the following use case scenarios:

- Session Handoff using DTMF Tones (*74)
- Session Handoff using Move Softkey Event
- Session Handoff using VoIP Mode
- Session Handoff Fails or User Cancels Session Handoff

Session Handoff Using DTMF Tones (*74)

For session handoff using DTMF tones (default specifies *74), the following sequence of events takes place:

1. User A calls user B desk phone. Using the Single Number Reach feature, user B answers the call on mobile phone and his desk phone goes into Remote In Use state.
2. User B presses *74 (Session Handoff DTMF code). User B desk phone (a supported phone that is running SCCP or SIP) flashes. User B still talks with user A from user B mobile phone.

3. To move conversation to the desk phone, user B must answer the call from desk phone before the Session Handoff Alerting Timer service parameter (default 10s) expires. After the timer expires, the desk phone stops flashing. User B can still continue conversation from the mobile phone.

Session Handoff Using Move Softkey Event

For session handoff using the Move softkey event, the following sequence of events takes place:

1. Session Handoff gets triggered by using a Move softkey event message that gets embedded inside the SIP REFER message.

2. When Cisco Unified Communications Manager receives the REFER message, Cisco Unified Communications Manager triggers session handoff.

Note If user mobile device disconnects a call for which Session Handoff has been initiated, the call can still be continued by resuming the call at the desk phone prior to the expiration of the Session Handoff Alerting Timer. These cases can occur when a user moves to an area that does not have mobile connectivity, such as an elevator or dead zone/spot.

Session Handoff Using VoIP Mode With SIP Clients

For SIP clients, session handoff support exists for VoIP mode as well as for cellular mode. For this scenario, the following steps take place:

1. User that is using a SIP client on a remote destination in VoIP (Wi-Fi) mode initiates session handoff by using the Move softkey on the smartphone.

2. Cisco Unified Communications Manager flashes the shared line on the desk phone and does not break media until the desk phone answers the call.

Be aware that this function also works if the user is logged on to extension mobility.

Session Handoff Fails or User Cancels Session Handoff

If session handoff fails, the following steps take place:

1. Cisco Unified Mobile Communicator or a VoIP client initiates session handoff to a station that does not have the correct owner user ID.

2. Session handoff fails. A “Cannot move conversation” SIP message gets sent to the client.

   If the user cancels session handoff, the session handoff stops. The following steps take place:

3. The user initiates session handoff from Cisco Unified Mobile Communicator or a VoIP client.

4. Before the session handoff completes, the user cancels the session handoff from the client.

5. Cisco Unified Communications Manager cancels the session handoff. Shared-line devices stop ringing.

Interactions and Limitations

Most standard Cisco Unified Communications Manager features are fully compatible with Cisco Unified Mobility features, except as indicated in the interactions and limitations.

The CMC and FAC feature on Cisco Mobility does not support an alternative number as its DVO callback number. The DVO callback number has to be the number registered in the MI (Mobility Identity) page.

Interactions

The following topics detail the interactions between Cisco Unified Mobility and other Cisco Unified Communications Manager components:

Auto Call Pickup

Cisco Unified Mobility interacts with auto call pickup based on the service parameter selection. When the Auto Call Pickup Enabled service parameter is set to True, end users need only to press the PickUp softkey to pick up a call.

If the Auto Call Pickup Enabled service parameter is set to False, end users need to press the PickUp, GPickUp, or OPickUp softkey and then the Answer softkey.

Auto Call Pickup Example

Phone A, phone B (Cisco Unified Mobility subscriber), and phone C belong to the Engineering group; phone D, phone E, and phone F belong to the Accounting group.

Phone D calls phone A in the Engineering Group. Phone A rings, and phone B and phone C in the group receive pickup notice.

If Auto Call Pickup is enabled, press the PickUp softkey from phone B to use Cisco Unified Mobility features later on.

If Auto Call Pickup is not enabled, press PickUp softkey from phone B, which causes the remote destinations that are associated with phone B to ring. Press the Answer softkey on phone B, which causes the remote destinations to stop ringing. The user can subsequently perform mobile-phone pickup and desktop call pickup.

Automatic Alternate Routing

Prior to the implementation of this interaction, if a desk phone was configured for Automatic Alternate Routing (AAR) and the desk phone was configured with a mobile phone as a remote destination, the AAR feature did not get triggered for calls to the remote destination if the out-of-bandwidth condition applied.

Cisco Unified Mobility now supports Automatic Alternate Routing (AAR) as follows:

- If a rejection occurs due to lack of bandwidth for the location-based service, the rejection triggers AAR for any device that is configured for AAR.
- If a rejection occurs based on Resource Reservation Protocol (RSVP), however, AAR does not get triggered for calls to remote destinations.

Extend and Connect

The Extend and Connect feature allows users to answer incoming calls on any of their Cisco Unified IP phones or remote destination phones under the control of Cisco Jabber for desktop. However, connected (active) calls cannot be moved between their Cisco Unified IP phone and their remote phone. So one gains application control over the remote phone, but loses mobility features such as being able to move the call back to a Cisco Unified IP phone. This feature requires configuration of CTI Remote Devices.

The Unified Mobility feature allows users to answer incoming calls to their enterprise extension on either their Cisco Unified IP phones or any remote destinations, such as a mobile phone, a home phone, or a hotel phone, etc. Users can move active calls between their Cisco Unified IP phone and their mobile phone without losing the connection. This feature requires configuration of Remote Destination Profiles.

Cisco Jabber for mobile provides telephony, availability, IM, and collaboration in a single integrated smart client. In addition, it also integrates with the native smartphone to provide the entire Cisco Unified Mobility feature set. This combination allows users to communicate seamlessly from their mobile devices when they transit between networks (Wi-Fi or cellular). The intelligence built into the mobility solution, dynamically enables different features as the network changes, eliminating the need for user intervention or preconfiguration (for example, DVO support).

Both of these mobility solutions allow users to communicate as if they are within the enterprise, increasing their reachability and providing the active user the flexibility to a move a call to another device or network once they have changed their location.

Users who need the capabilities of both Unified Mobility and Extend and Connect may 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 allows Cisco Mobility features to be used concurrently with Extend & Connect.

Note The ability to configure the same remote destination on both device types is supported using Cisco Unified Communications Manager Release 10 or later.

For more information, see the “Extend and Connect” chapter.

External Call Control

If external call control is configured, as described in the External Call Control, on page 547 chapter, Cisco Unified Communications Manager honors the route decision from the adjunct route server for the following Cisco Unified Mobility features:

- Cisco Unified Mobility
- Mobile Voice Access
- Enterprise Feature Access
- Dial-via-Office Reverse Callback
- Dial-via-Office Forward

Tip To invoke Mobile Voice Access or Enterprise Feature Access, the end user must dial a feature directory number that is configured in Cisco Unified Communications Manager Administration. When the Cisco Unified Communications Manager receives the call, Cisco Unified Communications Manager does not invoke external call control because the called number, in this case, is the feature DN. After the call is anchored, the Cisco Unified Communications Manager asks for user authentication, and the user enters the number for the target party. When Cisco Unified Communications Manager tries to extend the call to the target party, external call control gets invoked, and Cisco Unified Communications Manager sends a call routing query to the adjunct route server to determine how to handle the call.

Cisco 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 get anchored to the enterprise number, the mobile user can invoke the Session Handoff feature and mobile user can hand off the call to the desk phone.

Note For IP Multimedia Subsystem, ensure that the Cisco Unified Mobility feature is enabled in the Remote Destination Configuration window, or by using one of the other methods prescribed for enabling Cisco Unified Mobility, before implementing Intelligent Session Control call processing.

Licensing

Cisco Unified Mobility uses licensing. Checking the Enable Mobility check box in the End User Configuration window triggers licensing to consume device license units (DLUs) for Cisco Unified Mobility; the number of licenses that get consumed depends on whether you assign an adjunct device to the end user specifically for Cisco Unified Mobility. For specific information on how licensing works with Cisco Unified Mobility, see the *Cisco Unified Communications Manager Features and Services Guide*.

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.

Cisco Unified Mobility and 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).

Number of Supported Calls

Each remote destination supports a maximum of two active calls. For Cisco Unified Mobility, each remote destination supports a maximum of two active calls via Cisco Unified Communications Manager. Using the Enterprise Feature Access directory number (DID number) to transfer or conference with DTMF counts as one call. When a Cisco Unified Mobility user receives a call while the user has two active calls for the remote destination or while the user is using DTMF to transfer/conference a call from the remote destination, the received call does not reach the remote destination and instead goes to the enterprise voice mail; that is, if Call Forward No Answer (CFNA) is configured or if the call is not answered on a shared line.

Limitations

Cisco Unified Mobility enforces the following limitations in operating with other Cisco Unified Communications Manager components.

Call Anchoring

Call anchoring, which is performed based on caller ID, is supported only from calls from registered single-mode or dual-mode phones.

Call Forwarding

You do not need to configure settings for Call Forward Unregistered if the end user has configured remote destinations. Appropriate call forwarding is handled as part of the Cisco Unified Mobility process.

Call Queuing

Cisco Unified Communications Manager does not support Call Queuing with Cisco Unified Mobility.

Cisco Unified IP Phones 7940 and 7960 That Are Running SIP

When running SIP, Cisco Unified IP Phones 7940 and 7960 do not support the Remote-In-Use state and therefore cannot support Desktop Call Pickup.

For these phones, if the mobile phone user hangs up a call that the Cisco Unified IP Phone 7940 or 7960 that is running SIP extended to the mobile phone, the calling party hears music on hold for 10 seconds (as configured by the Maximum Wait Time for Desk Pickup field for the remote-destination end user) and then the call drops. Because the Desktop Call Pickup feature is not supported for these phones when they are running as SIP devices, the user desk phone does not display the Resume softkey, so the user cannot pick up the call on the desk phone.

Cisco recommends that you configure Cisco Unified IP Phones 7940 and 7960 to run SCCP for users that are enabled for 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.

For more information about configuring the international escape character in Cisco Unified Communications Manager Administration, see the *Cisco Unified Communications Manager System Guide*.

DND 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 does not get anchored when:

- 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 does get anchored.

Dual-Mode Handoff and Caller ID

Dual-mode handoff requires that caller ID be available in the cellular network.

Dual-Mode Phones and Call Anchoring

Dual-mode phones (Cisco Unified Mobility Advantage and dual-mode phones that are running SCCP or SIP) that are configured as remote destinations cannot anchor calls.

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 disappear if the dual-mode phone goes out of WLAN range.

Dual-Mode Phones and Desktop Call Pickup

The Desktop Call Pickup feature does not apply to the following mobile phone models:

- Nokia 902iL and Nokia 906iL dual-mode phones that are running SIP
- Nokia S60 dual-mode phones that are running SCCP

For these phone models, if the mobile phone user hangs up a call, the calling party hears music on hold for 10 seconds (as configured by the Maximum Wait Time for Desk Pickup field for the remote destination end user) and then the call drops. Because the Desktop Call Pickup feature is not supported for these phone models, the user desk phone does not display the Resume softkey, so the user cannot pick up the call on the desk phone.

Dual-Mode Phones That Are Running SIP and Registration Period

For dual-mode phones that are running SIP, Cisco 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.

Enterprise Features From Cellular Networks

Enterprise features from cellular networks require out-of-band DTMF.

Note 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.

Enterprise Features in the Global System for Mobile Communications (GSM) That Is Using DTMF

Availability of enterprise features in the Global System for Mobile communications (GSM) that are using DTMF depends on the features that are supported in the third-party smartphones.

Gateways and Ports

Both H.323 and SIP VoIP gateways are supported for Mobile Voice Access.

Cisco Unified Mobility features do not get supported for T1 CAS, FXO, FXS and BRI.

IPv6 Support When Used with Cisco Unified Mobility Advantage

Cisco Unified Mobility does not support IPv6 for mobile clients that are using Cisco Unified Mobility Advantage to connect to Cisco Unified Communications Manager for Dial via office or midcall features. Cisco Unified Mobility Advantage does not support IPv6 addresses.

iPhone-Based Cisco Jabber VoIP Calls

Cisco Mobile devices can support Voice over IP (VoIP) and Dial via Office (DVO) calling schemes, but iPhone-based Cisco Jabber supports only VoIP calls.

Note The Android-based Cisco Jabber client supports both VoIP and DVO.

Jabber Devices are Registered 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.

Maximum Wait Timer for Desktop Call Pickup Is Not Applied If User Presses Hold DTMF

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 display 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.)

Cisco Unified Mobility Support Restrictions

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.

Multilevel Precedence and Preemption (MLPP)

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.

Multiple-Node Cluster Environment

In a multiple-node cluster environment, if the Cisco Unified Communications Manager publisher server is unreachable, any changes that end users make to turn Cisco Unified Mobility off or on by way of Mobile Voice Access or two-stage dialing do not get saved.

Overlap Sending

Overlap sending patterns are not supported for the Intelligent Session Control feature.

QSIG

Mobility does not support QSIG.

QSIG Path Replacement

QSIG (Q Signaling) path replacement is not supported.

Remote Destination Profiles

When you configure a directory number that is associated with a remote destination profile, you must use only ASCII characters in the Display (Internal Caller ID) field on the Directory Number Configuration window.

Remote Destinations

Ensure remote destinations are Time Division Multiplex (TDM) devices. You cannot configure IP phones within a Cisco Unified Communications Manager system as remote destinations.

Ensure remote destinations specify PSTN numbers or numbers across ICT trunks.

Remote destinations cannot resume calls that Cisco Unified IP Phones put on hold.

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. Administrators 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 Feature

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.

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.

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.

System Requirements

Cisco Unified Mobility (formerly Mobile Connect) and Mobile Voice Access require the following software components:

- Cisco Unified Communications Manager 6.0 or later.
- Cisco Unified Mobile Voice Access service, which runs only on the publisher.
- Cisco Unified Communications Manager Locale Installer (if you want to use non-English phone locales or country-specific tones).

To see which IP phones work with Cisco Unified Mobility and Mobile Voice Access, see the applicable Cisco Unified IP Phone Administration Guide and Cisco Unified IP Phone User Guide.

HCS Supplementary Services for VoLTE IMS Mobile Device

Cisco Unified Communications Manager 9.0 supports a native way of invoking the supplementary services. The following supplementary services are supported.

- Originating Identification Presentation
- Terminating Identification Presentation
- Originating Identification Restriction
- Terminating Identification Restriction
- Communication Diversion Unconditional
- Communication Diversion on not Logged in
- Communication Diversion on Busy
- Communication Diversion on not Reachable
- Communication Diversion on No Reply
- Barring of All Incoming Calls
- Barring of All Outgoing Calls
- Barring of All Incoming Calls When Roaming
- Barring of Outgoing International Calls
- Communication Hold
- Communication Retrieve
- 3rd Party Registration
- Message Waiting Indication

- Communication Waiting
- Ad-Hoc Multi Party Conference
- Call Transfer

Originating Identification Presentation

The service control in the originating part is done by the home S-CSCF of the originator of the request. The originating S-CSCF can invoke services on behalf of the requestor.

When the initial inbound INVITE to an ISC trunk has mode set to originating, Cisco Unified Communications Manager acts as the application server for the originating DN. In this scenario, Cisco Unified Communications Manager uses the user portion of the P-Asserted-Id to find the corresponding IMS client. When no such IMS client is found, Cisco Unified Communications Manager rejects the call with a 403 forbidden error. After finding the corresponding IMS client, the call is routed through the enterprise DN configured for the IMS client.

The calling search space used for this call can either be a combination of line and IMS client's search space or the ISC trunk's, depending on the configuration of the IMS client.

Cisco Unified Communications Manager validates the destination through its DA. If the destination is not routable in the cluster, Cisco Unified Communications Manager will reject the call. Cisco Unified Communications Manager will not alert the destination and will not provide any terminating feature. Once it is determined that the destination is routable, the call is anchored in Cisco Unified Communications Manager and then immediately routed out through the same ISC trunk, bypassing the RouteList or regular SIP trunk.

Note For unknown destinations to allow the IMS network to route to the default network, the Cisco Unified Communications Manager dial plan can have a default route through the ISC trunk for otherwise unknown destinations.

The originating call from the ISC trunk should not invoke Intelligent Session Control. If the mode is originating, CallControl does not fire intercept to Intelligent Session Control even if caller is the IMS client.

Terminating Identification Presentation

The service control in the terminating part is done by the home S-CSCF of the recipient of the request. The terminating S-CSCF can invoke services on behalf of the recipient.

When the initial inbound INVITE to an ISC trunk has the mode set to terminating, Cisco Unified Communications Manager acts as the application server for the terminating DN. In this scenario, Cisco Unified Communications Manager uses the user portion of the RequestURI to find the corresponding IMS client. When the IMS client is found, Cisco Unified Communications Manager will treat the caller as an internal caller. This impacts other feature interactions, such as Forwarding on Busy, Transfer to an external destination, and adhoc terminating.

Unlike when serving as the originating side, Cisco Unified Communications Manager will not reject the call, even if the caller's P-Asserted-Id does not match any IMS client. It will instead be treated as an external trunk call.

When acting as the application server for terminating DN, Cisco Unified Communications Manager will alert the destination and will provide all terminating features.

If the destination includes an IMS client, the outbound INVITE will go through the same ISC trunk logically, but could be on a different node.

Note The terminating call invokes Intelligent Session Control. It is triggered by intercept by CallControl.

Call Forward

Cisco Unified Communications Manager 9.0 supports call forward treatments for the IMS client either through configuration or after a CFA activation request is received over the ISC trunk. The supported forwarding options are:

- CFA
- CF Not Logged In
- CFB
- CF Not Reachable
- CFNA

Call Barring

Cisco Unified Communications Manager 9.0 provides call barring functionality. This feature allows you to block calls in the following ways:

- Barring of All Incoming Calls
- Barring of All Outgoing Calls
- Barring of All Incoming Calls When Roaming
- Barring of Outgoing International Calls

A new section was added to the Phone Configuration page for Call Barring Information. In this section you can select the checkbox to **Block Incoming Call while Roaming** and define the **Home Network ID**.

Note The **Home Network ID** must be defined to enable the **Block Incoming Call while Roaming** feature.

Hold

Cisco Unified Communications Manager supports hold feature invocation through Invite coming in from the ISC interface. Upon receiving the Invite, Cisco Unified Communications Manager will place the active call on hold, and allocate the necessary Music On Hold resource to stream to the held party, if configured. The IMS network triggered hold receives the same treatment as the internal user originated hold operation.

Retrieve

Cisco Unified Communications Manager now supports Retrieve requests over the ISC interface on a held call in the form of Invite with SendReceive SDP. Upon receiving such request, Cisco Unified Communications

Manager will apply its Retrieve call operations, such as remove and de-allocate any Music On Hold resources, and reconnect the media between two parties.

Third-Party Registration

Cisco Unified Communications Manager 9.0 provides a third-party registration feature.

A new checkbox for **Third-party Registration Required** was added to the Protocol Specific Information section.

Message Waiting Indication

Cisco Unified Communications Manager 9.0 supports subscription from the IMS client in the IMS core network through the SUBSCRIBE method. Upon receiving the SUBSCRIBE request from the IMS core, Cisco Unified Communications Manager determines if the requesting client is qualified to receive Message Waiting Indication (MWI) notification by checking the client provisioning data. If the client is qualified, Cisco Unified Communications Manager delivers the cached MWI data to the client upon completing the SUBSCRIBE handling, and continues to deliver the MWI notification if there is any MWI status change under the condition that the subscription is still valid.

Call Waiting

Cisco Unified Communications Manager 9.0 allows the user to select from various call waiting options. If a mobile user has an active call, and a new incoming call arrives the user has the options to:

- Ignore the new incoming call.

  When the user selects this option, the call forwarding treatment may be applied if the forward on busy configuration is set.

- Quit the incoming call.

  When the user selects this option, the call forwarding treatment may be applied if the forward on no answer configuration is set.

- Answer the incoming call.

  When the user selects this option, the original active call is put on hold first, then the new call can be answered.

IMS Client Initiated Ad-Hoc Conference Request

The single user conference initiates with an Invite with a specified conference service request URI. Upon receiving such a service request URI, the conference feature dynamically allocates a number as the conference identifier and registers that with the Cisco Unified Communications Manager internal DA service. The conference feature allocates the conference resource and creates the conference for the user that initiated the conference service request. The dynamically allocated conference identifier number is used to identify the existing conference and allow a new participant to be added to the same conference.

The conference service request URI must be provisioned through a new service parameter within Unified Communications Manager to ensure the correct behavior of the single user conference creation procedure. This provisioning of service parameter must match what is provisioned in the IMS core network. For instance, it can be configured as cucm-conference-factory@cucm1.company.com.

Additional conference participants will ride with a Refer with the existing dialog for all calls respectively. The call info in this Refer has the conference ID that the conference feature allocated during the single user conference creation. The Cisco Unified Communications Manager Refer/Replace feature picks up the task and joins the participant to the existing single user conference. The Refer feature applies the same mechanism to add all of the conference participants.

Note The new conference flows for single user conference creation as well as adding/dropping conference participant are only available when the request is sent from a Cisco Unified Communications Manager provisioned IMS client on the IMS core network. If this is not the case, the request will be rejected.

Transfer

Cisco Unified Communications Manager can handle transfer requests from the IMS core network. The transfer is done through SIP Refer/Replace method in the ISC interface.

Note Calls are put on hold before the transfer is initiated from the IMS client.

HCS Anonymous Call Rejection ISC Trunks

Cisco Unified Communications Manager 9.0 allows the administrator to block incoming calls from anonymous callers. The administrator can choose to block these calls either at the SIP trunk or at the line or DN levels. Calls that are originating from IP phones within the cluster or over other protocols with Calling Line ID Restriction (CLIR) will also get blocked.

There are three configuration options for the anonymous call rejection feature in Cisco Unified Communications Manager. One on the Directory Number page and two on the SIP Profile page.

Directory Number Configuration

To block outgoing anonymous calls for a particular line or DN, this feature can be configured on the Directory Number configuration page for the specific DN. Select the **Reject Anonymous Calls** checkbox on Directory Number page to reject all anonymous calls for the DN.

In the case of an enterprise directory number (DN) that has anonymous call rejection enabled and also has one or more single number reach destinations associated with it, Cisco Unified Communications Manager will block a call from anonymous callers to the enterprise DN and all associated remote destinations.

In the case of an enterprise directory number that has anonymous call rejection enabled and also has a Call Forward All destination, Cisco Unified Communications Manager will forward anonymous calls to the Call Forward All target.

In the case of an enterprise directory number that has anonymous call rejections enabled and also has a call forward on busy destination, Cisco Unified Communications Manager will reject the anonymous call without triggering call forward on busy.

The Call Forward No-Answer feature is not triggered for an anonymous caller.

For Call Transfer - During attended transfer, if the transfer error has CLIR and places a consult call to a transfer-target who has ACR, the consult call will be rejected. Similarly on getting a REFER from anonymous caller, if the Refer-To DN has ACR, the REFER operation will be blocked. In both cases, the consult call will be blocked when the caller has CLIR and called party has ACR.

SIP Trunk Configuration

Configure anonymous call rejection on Cisco Unified Communications Manager to block calls from anonymous callers at the SIP trunk using the SIP Profile page configuration settings. Select the **Reject Anonymous Incoming Calls** and **Reject Anonymous Outgoing Calls** checkboxes on the SIP Profile page. When the **Reject Anonymous Incoming Calls** checkbox is selected, all anonymous incoming calls on the SIP trunk associated this SIP Profile will be rejected. When the **Reject Anonymous Outgoing Calls** checkbox is selected, all anonymous outgoing calls on the SIP trunk associated this SIP Profile will be rejected.

Anonymous calls in SIP are identified based on the criteria described in RFC 5079. Based on RFC 5079, calls are identified to be anonymous when the incoming initial INVITE meets any of the following criteria:

- From or PAI/PPI header with display-name Anonymous
- From header host-portion = anonymous.invalid
- Privacy: id or Privacy: user or Privacy: header [associated with PAI/PPI]
- Remote-Party-ID header has a display-name Anonymous
- Remote-Party-ID header has privacy=uri/full/name

Note For calls that originate from within the Cisco Unified Communications Manager cluster, if the caller's DN or user information is present but caller name is not available or the presentation is restricted, the call is not marked as an anonymous call.

If the caller's DN is not present or the presentation is restricted, regardless of if the caller's name is presented or not, the caller is deemed to be anonymous.

When an anonymous call is rejected by Cisco Unified Communications Manager, it will send SIP error response 433 - Anonymity Disallowed to the initial INVITE. Cisco Unified Communications Manager will also include Q.850 Reason header with cause = 21 (Call Rejected) in 433 response.

Migrate From Cisco Unified Mobility Manager

Follow this process to migrate standalone Cisco Unified MobilityManager data to Cisco Unified Communications Manager:

1. Upgrade the Cisco Unified MobilityManager system to Release 1.2(5), if necessary. See the Release Notes for Cisco Unified MobilityManager Release 1.2(5).
2. Log in to Cisco Unified MobilityManager and export the configuration data in CSV format. For instructions, see the Release Notes for Cisco Unified MobilityManager Release 1.2(5).
3. Log in to Cisco Unified Communications Manager Administration and use the Bulk Administration Import/Export windows to import the CSV data files that were previously exported from Cisco Unified MobilityManager. See the Cisco Unified Communications Manager Bulk Administration Guide.

Cisco Unified Mobility Configuration

This section provides detailed procedures for each Cisco Unified Communications Manager Administration menu option that must be configured to provision Cisco Unified Mobility features that are native to Cisco Unified Communications Manager.

End users use the Cisco Unified Communications Self Care Portal windows to further configure or modify the Cisco Unified Mobility settings that apply to their mobile phones.

Tip Administrators should review the summary of all the tasks necessary to configure the Cisco Unified Mobility features that are native to Cisco Unified Communications Manager before proceeding to configure Cisco Unified Mobility.

Related Topics

Configure Cisco Unified Mobility, on page 233

Access List Configuration and Deletion

You can define access lists to explicitly allow or block the extension of Cisco Unified Mobility calls to remote destinations based on the caller ID of the caller.

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the *Cisco Unified Communications Manager Administration Guide*.

Tips About Deleting Access Lists

You cannot delete access lists that remote destinations are using. To find out which items are using the access list, choose Dependency Records from the Related Links drop-down list box that is on the Access List Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the *Cisco Unified Communications Manager Administration Guide*. If you try to delete an access list that is in use, Cisco Unified Communications Manager displays a message. Before deleting an access list that is currently in use, you must perform either or both of the following tasks:

- Assign a different access list to any remote destinations that are using the access list that you want to delete.
- Delete the remote destinations that are using the access list that you want to delete.

Related Topics

Access List Member Detail Configuration, on page 273

About Remote Destination Setup, on page 278

Configure Access List

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Class of Control** > **Access List** menu path to configure access lists.

An access list, which supports Cisco Unified Mobility, specifies a list that determines the phone numbers that the system can pass or block from being passed to remote destinations.

While you configure an access list, follow these additional steps to configure its members:

Procedure

Step 1 If you want to configure the members of an access list, click **Add Member** and enter values for the parameters that are described in Access List Member Detail Configuration, on page 273.

Step 2 Click **Save.**

The Access List Configuration window reopens to show the new number or filter in the Selected Filters area.

Step 3 From the Access List Configuration window, add additional filters and also modify any existing access list as needed:

a) To modify a DN mask, click the link for the directory number at the bottom of the window under Access List Members, enter your change, and click **Save.**
b) To delete a filter, select the filter and click **Delete.**
c) To inactivate a filter without deleting it, select the filter in the Selected Filters pane and click the down arrow to move the filter to the Removed Filters pane.
d) To activate a filter, select the filter in the Removed Filters pane and click the up arrow to move the filter to the Selected filters area.
e) To create a new access list with the same members as the existing list, click **Copy.**

Access List Configuration Settings

The following table describes the available settings in the Access List Configuration window.

Table 32: Access List Configuration Settings

Field	Description
Access List Information	
Name	Enter a unique name (between 1 and 50 characters) for this access list. You may use all characters except quotes (“), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).
Description	Enter a text description (between 1 and 128 characters) for this access list. You may use all characters except nonprinting characters, such as tabs and quotes (“).
Owner	From the drop-down list box, choose the end user to whom the access list applies.
Allowed	Click this radio button to allow calls from member phone numbers to be passed to the remote destinations.

Field	Description
Blocked	Click this radio button to block calls from member phone numbers from being passed to the remote destinations.
Access List Member Information	
Selected Filters	This pane displays the current members of this access list. Members comprise the following types: • Private - This filter applies to calls that come from private numbers, which do not display caller ID. • Not Available - This filter applies to calls that come from numbers that do not have caller ID. • Directory Number - This filter specifies a directory number that is specified between parentheses. For example, (12345). Valid values include the digits 0 through 9, the wildcard X, !, and #. Use the arrows below this pane to move the access list members to or from this pane. Add Member - Click this button to add a new member to the Selected Filters pane. The Access List Member Detail window displays.
Removed Filters	This pane specifies filters that have been defined for this access list but that are not currently selected. Use the arrows above this pane to move the access list members to or from this pane.

Related Topics

Access List Member Detail Configuration, on page 273

Access List Member Detail Configuration

The Access List Member Detail window displays when you click the Add Member button on the Access List Configuration window while you configure an access list. The Access List Member Detail window allows you to configure the following settings for an access list member:

- Filter Mask
- DN Mask

After you configure a new access list member, the new access list member displays in the Access List Members pane at the bottom of the corresponding Access List Configuration window. You can click one of the access list members to view or change the settings for that access list member. To exit the Access List Member Detail window without making any changes, choose Back to Find/List from the Related Links drop-down list box and click **Go.**

The following table describes the available settings in the Access List Member Detail window.

Table 33: Access List Member Detail Configuration Settings

Field	Description
Filter Mask	Select an option from the drop-down list box. You can choose to enter a directory number, filter out calls that do not have caller ID (Not Available), or specify a number that will be allowed or blocked without displaying the caller ID (Private).
DN Mask	If you chose Directory Number in the Filter Mask field, enter a phone number or filter in the DN Mask field. You can use the following wild cards to define a filter: • X (upper or lower case) - Matches a single digit. • ! - Matches any number of digits. • # - Used as a single digit for exact match. Examples: • 408! matches any number that starts with 408. • 408555123X matches any number between 4085551230 and 4085551239. **Note** If you want to filter an incoming call from a calling number that begins with a leading +, you must include the leading + in the DN Mask field unless any supported wild card precedes the directory number. For example, if an end user wants to block +14081239876, the user access list needs to include either +14081239876 or !14081239876 in the DN Mask field.

Remote Destination Profile Configuration

This section provides information to configure remote destination profiles.

About Remote Destination Profile Setup

In Unified Communications Manager, use the **Device** > **Device Settings** > **Remote Destination Profile** menu path to configure remote destination profiles.

Remote destination profiles, which support Cisco Unified Mobility, specify a set of parameters that applies to all remote destinations for the user.

The remote destination profile contains the parameters that apply to all remote destinations for the user. After configuring user accounts for Cisco Unified Mobility (see the *Cisco Unified Communications Manager Administration Guide*), you can create a remote destination profile for the user.

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the *Cisco Unified Communications Manager Administration Guide* and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Tips About Deleting Remote Destination Profiles

You can delete remote destination profiles that associate with remote destinations. You receive a warning message that you are about to delete both a remote destination profile and the associated remote destinations.

To find out which items are using the remote destination profiles, choose Dependency Records from the Related Links drop-down list box that is on the Remote Destination Profile Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message.

Remote Destination Profile Configuration Settings

The following table describes the available settings in the **Remote Destination Profile Configuration** window.

Table 34: Remote Destination Profile Configuration Settings

Field	Description
Remote Destination Profile Information	
Name	Enter a text name for the remote destination profile. This name can comprise up to 50 characters. Valid characters include letters, numbers, dashes, dots (periods), spaces, and underscores.
Description	Enter a text description of the remote destination profile. This field can comprise up to 128 characters. You can use all characters except quotes (“), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).
User ID	Choose the user to whom this profile is assigned. The selection must match the ID of a user in the End User Configuration window where Enable Mobility is checked.
Device Pool	Choose the device pool that applies to this profile. The device pool defines sets of common characteristics for devices, such as region, date/time group, softkey template, and MLPP information.
Calling Search Space	Choose the calling search space to be used for routing Mobile Voice Access or Enterprise Feature Access calls. **Note** This calling search space setting applies only when you are routing calls from the remote destination, which specifies the outbound call leg to the dialed number for Mobile Voice Access and Enterprise Feature Access calls.
AAR Calling Search Space	Choose the appropriate calling search space for the remote destination profile to use when automated alternate routing (AAR) is performed. The AAR calling search space specifies 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.
User Hold Audio Source	Choose the audio option for users on hold for Cisco Unified Mobility and Mobile Voice Access calls.

Field	Description
Network Hold MOH Audio Source	Choose the audio source from the IOS gateway that provides multicasting audio source for Cisco Unified Mobility and Mobile Voice Access calls.
Privacy	Choose a privacy option for the remote destination profile. If you choose the Default value for this field, the setting matches the value of the Privacy Setting service parameter. **Note** If you change and save the value of the Privacy Setting service parameter, you must return to the **Remote Destination Profile Configuration** window for a remote destination profile that specifies Default and click Save for the service parameter change to take effect. **Note** You cannot transfer a call from a cell phone to a desk phone if the Remote Destination Profile Privacy specifies On, and the “Enforce Privacy Setting on Held Calls” service parameter specifies True.
Rerouting Calling Search Space	Choose a calling search space to be used to route Cisco Unified Mobility calls. **Note** Ensure that the gateway that is configured for routing mobile calls is assigned to the partition that belongs to the Rerouting Calling Search Space. Unified Communications Manager determines how to route calls based on the remote destination number and the Rerouting Calling Search Space. The Rerouting Calling Search Space setting applies only when you are routing calls to the remote destination or mobility identity, which specifies the outbound call leg toward the remote destination or mobility identity when a call comes in to the user enterprise number. Cisco Unified Mobility calls do not get routed to the dual-mode mobility identity number that corresponds to the dual-mode mobile phone number if the device associates with the enterprise WLAN and registers with Unified Communications Manager. Cisco Unified Mobility calls get routed to the dual-mode mobility identity number only when the device is outside the enterprise.

Field	Description
Calling Party Transformation CSS	Choose the calling search space for transformations. This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device. **Note** The partitions in the calling search space should contain only calling party transformations. Ensure the calling search space is not null because no transformations can apply to null partitions. The device takes on the attributes of the Calling Party Transformation Pattern because you assign the pattern to a partition where the Calling Party Transformation CSS exists. For example, when you configure the Calling Party Transformation CSS under **Call Routing** > **Class of Control** > **Calling Search Space**, you assign the CSS to a partition; when you configure the Calling Party Transformation CSS under **Call Routing** > **Transformation Pattern** > **Calling Party Transformation Pattern**, you choose the partition where the Calling Party Transformation CSS is assigned.
Use Device Pool Calling Party Transformation CSS	To use the Calling Party Transformation CSS that is configured in the device pool that is assigned to this device, check this check box. If you do not check this check box, the device uses the Calling Party Transformation CSS that you configured in the **Remote Destination Profile Configuration** window.
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 the users require information to display (on the phone) in any language other than English, verify that the locale installer is installed before you configure user locale. See the Unified Communications Manager Locale Installer documentation.
Network Locale	From the drop-down list, choose the locale to associate with the remote destination profile. The network locale contains a definition of the tones and cadences that the devices tied to the remote destination profile in a specific geographic area use. Select a network locale that is supported by all of the devices that use this remote destination profile. If you do not choose a network locale, the locale that is specified in the Unified Communications Manager clusterwide parameters as Default Network Locale applies. Choose only a network locale that is already installed and supported by the associated devices. The list contains all available network locales for this setting, but not all are necessarily installed.

Field	Description
Ignore presentation indicators (internal calls only)	Check the check box if you want to ignore the connected line ID presentation. Use this configuration for internal calls.
Associated Remote Destinations	
Add a New Remote Destination	Click this link to open the Remote Destination Configuration window, where you can configure a new remote destination to associate with this remote destination profile. By default, the current remote destination profile is selected in the **Remote Destination Profile** field of the new remote destination.
Name	For a remote destination that already exists and has been associated with this remote destination profile, this column displays the name of the remote destination.
Destination Number	For a remote destination that already exists and has been associated with this remote destination profile, this column displays the destination number of the remote destination.
Do Not Disturb	
Do Not Disturb	Check this check box to enable Do Not Disturb on the phone.
DND Option	This Call Reject option specifies that no incoming call information gets presented to the user. **Note** For mobile devices, dual-mode phones, and phones that are running SCCP, 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.

Associate a Directory Number with a Remote Destination Profile

After creating a remote destination profile, you must associate the DN record for the desk phone or phones for the user. Click the Add a New DN link on the Remote Destination Profile Configuration window and follow the instructions to configure a directory number in the *Cisco Unified Communications Manager Administration Guide*.

Note If the remote destination profile is dissociated on the Directory Number configuration window, you must check the Line Association check box for the DN on the Remote Destination window to re-associate it.

About Remote Destination Setup

After remote destination profiles and access lists are created, you can enter individual remote destinations and assign each to a profile. Each remote destination represents a mobile or other phone that can be configured to perform remote destination pickup (accept transfers from the desk phone of the user) and accept incoming Cisco Unified Mobility calls that come from the system as a result of the line that is shared with the desk phone.

After you save a new remote destination, the Association Information pane displays, which lists the desk phone numbers that have been assigned to the remote destination profile. You can click a link to open the associated Directory Number Information window.

This section describes how to access remote destination records by opening the Remote Destination Configuration window. You can also open an existing or new record in the Remote Destination Profile Configuration window by clicking the Add a New Remote Destination link at the bottom of the remote destination profile.

In Unified Communications Manager, use the **Device** > **Remote Destination** menu path to configure remote destinations.

Remote destinations represent phones that are available for Cisco Unified Mobility answer and pickup, plus locations that are used to reach Mobile Voice Access. Remote destinations may include any of the following devices:

- Single-mode mobile (cellular) phones
- Smartphones
- Dual-mode phones
- Enterprise IP phones that are not in the same cluster as the desk phone
- Home phone numbers in the PSTN.

Tips About Configuring Remote Destinations

End users can create their own remote destinations in the Cisco Unified Communications Self Care Portal. For information about how to perform this task, see the user guide for the phone model.

Be aware that the appropriate timer settings in the following table may be service-provider-specific. If difficulties in transferring calls by using the default timer settings occur, you may need to adjust the settings to be compatible with the service provider for the remote destination phone.

Check the Line Association check boxes for the desk phones that will be used with this remote destination. You must perform this step for Cisco Unified Mobility to work.

Note This step requires that a directory number has already been configured on the remote destination profile with which the remote destination associates.

Tips About Deleting Remote Destinations

To find out which items are using the remote destination, choose Dependency Records from the Related Links drop-down list box that is on the Remote Destination Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message.

Remote Destination Configuration Settings

Field	Description
Remote Destination Information	
Mobile Identity Information	

Field	Description
Name	Enter a name that identifies the remote destination or mobile identity.
Destination Number	Enter the PSTN telephone number for the destination. Include the area code and any additional digits that are required to obtain an outside line. Maximum field length equals 24 characters; individual characters can take the values 0-9, *, #, and +. Cisco recommends that you configure the caller ID of the remote destination. If the administrator configures the Incoming Calling Party settings in the Unified Communications Manager gateway, trunk, or device pool to globalize the incoming calling party number, configure the Destination Number of the remote destination in the E.164 format. Example: For a remote destination with US area code 408 and destination number 5552222, configure the Destination Number as +14085552222. Additionally, if globalized destination numbers are in use, set the Matching Caller ID with Remote Destination service parameter to Complete Match. **Note** Add the necessary translation pattern or route patterns to route the destination number. You can also enter a directory URI in this field. Keep in mind that if you enter a directory URI in this field, you must also configure a domain-based SIP route pattern. **Note** When you place a call from a remote destination, the caller ID of the destination phone displays the directory number that is associated with the calling directory URI rather than the directory URI.
Single Number Reach Voicemail Policy	Configures how mobile device users answer calls that terminate on a remote destination (RD). This feature provides users with a single enterprise voice mail box for their enterprise mobility if the RD call reaches an external voice mail system. Available options are as follows: • Use System Default • Timer Control • User Control **Note** For User Control to work, you must set the Enable Enterprise Feature Access service parameter to TRUE.
Dial-via-Office Reverse Voicemail Policy	Configures how dual mode device users answer Dial-via-Office Reverse (DVO-R) calls that terminate on the Mobile Identity (MI). This feature provides users with a single enterprise voicemail box for their enterprise mobility if the RD call reaches an external voice mail system. Available options are as follows: • Use System Default • Timer Control • User Control

Field	Description
Answer Too Soon Timer	Enter the minimum time in milliseconds that Unified Communications Manager requires the mobile phone to ring before answering the call. This setting accounts for situations where the mobile phone is switched off or is not reachable, in which case the network may immediately divert the call to the mobile phone voice mail. If the mobile phone is answered before this timer expires, Unified Communications Manager pulls the call back to the enterprise. Range: 0 - 10,000 milliseconds Default: 1,500 milliseconds
Answer Too Late Timer	Enter the maximum time in milliseconds that Unified Communications Manager allows for the mobile phone to answer. If this value is reached, Unified Communications Manager stops ringing the mobile phone and pulls the call back to the enterprise. Range: 0 and 10,000 - 300,000 milliseconds Default: 19,000 milliseconds If the value is set to zero, the timer is not started.
Delay Before Ringing Timer	Enter the time that elapses before the mobile phone rings when a call is extended to the remote destination. Range: 0 - 30,000 milliseconds Default: 4,000 milliseconds **Tip** When a hunt group is in use, the lines ring only for a short period of time. You may need to manipulate the Delay Before Ringing Timer setting and make it zero to allow a remote destination call to be established, ring, and answer, before the hunt list timer expires and pulls the call back.
Remote Destination Profile	From the drop-down list, choose the remote destination profile that you want to use for this remote destination.
Mobility Profile	From the drop-down list, choose the mobility profile that you want to use for this remote destination. To configure a mobility profile, use the **Call Routing** > **Mobility** > **Mobility Profile** menu option.
Dual Mode Phone	Displays a dual-mode phone with which this Mobility Identity associates. The field displays the device name. Click the Configure Device link to display the Phone Configuration window, where you can change the settings of the specified device.

Field	Description
Mobile Phone	Check the check box if you want calls that the desk phone answers to be sent to your mobile phone as the remote destination. Checking this check box ensures that, if Send Call to Mobile Phone is specified (by using the Mobility softkey for remote destination pickup), the call gets extended to this remote destination. **Note** This check box does not apply to dual-mode phones that are running SIP nor to dual-mode phones that are running SCCP, such as the Nokia S60.
Enable Mobile Connect	Check the check box to allow an incoming call to ring your desk phone and remote destination at the same time. For more information, see the "Cisco Mobility" and "Extend and Connect" chapters in the Feature Configuration Guide for Cisco Unified Communications Manager
When Cisco Unified Mobility Is Enabled	
Ring Schedule	
All the time	If the Enable Cisco Unified Mobility check box is checked for this remote destination, clicking this radio button allows this remote destination to ring all the time. This setting works in conjunction with the setting in the When receiving a call during the above ring schedule pane below.
As specified below	If the Enable Cisco Unified Mobility check box is checked for this remote destination, clicking this radio button allows this remote destination to ring according to the schedule that the subsequent rows specify. This setting works in conjunction with the setting in the When receiving a call during the above ring schedule pane below.
(day of week)	If the Enable Cisco Unified Mobility check box is checked and the As specified below radio button is selected, click the check box for each day of the week when the remote destination should receive calls. You can specify a ring schedule for each day of the week. (day of the week) - Check the check box for a day of the week, such as Monday, to specify the ring schedule for that day. All Day - Click this check box next to a day of the week to specify that the remote destination should ring at all hours of the day as specified by the setting in the When receiving a call during the above ring schedule pane below. (drop-down list box) to (drop-down list box) - For a particular day of the week, specify a ring schedule by choosing a starting time and ending time for that day. Specify the starting time by choosing a value in the drop-down list box that precedes to and specify the ending time by choosing a value in the drop-down list box that follows to. For a particular day, the default ring schedule specifies No Office Hours. The values that you specify in the drop-down list boxes relate to the time zone that you specify in the Time Zone field for the remote destination or mobile identity.

Field	Description
Time Zone	From the drop-down list, choose a time zone to use for this remote destination or mobile identity. **Note** The time-of-day access feature uses the time zone that you choose for this remote destination or mobile identity to allow or to block calls to this remote destination or mobile identity.
When receiving a call during the above ring schedule	
Always ring this destination	Click this radio button to cause incoming calls to always ring this remote destination according to the Ring Schedule that you specify. This setting applies only if the Enable Cisco Unified Mobility check box is checked for this remote destination.
Ring this destination only if caller is in	Click this radio button to allow incoming calls to ring this remote destination only if the caller belongs to the access list that is specified in the drop-down list box and according to the Ring Schedule that you specify in the Ring Schedule pane. This setting applies only if the Enable Cisco Unified Mobility check box is checked for this remote destination. From the drop-down list, choose an access list that applies to this setting. If you want to view the details of an access list, click the View Details link. (To modify an access list, you must use the **Call Routing** > **Class of Control** > **Access List** menu option.) Choosing an access list that contains no members equates to choosing to never ring this destination.
Do not ring this destination if caller is in	Click this radio button to prevent incoming calls from ringing this remote destination if the caller belongs to the access list that is specified in the drop-down list box and according to the Ring Schedule that you specify in the Ring Schedule pane. This setting applies only if the Enable Cisco Unified Mobility check box is checked for this remote destination. From the drop-down list box, choose an access list that applies to this setting. If you want to view the details of an access list, click the View Details link. (To modify an access list, you must use the **Call Routing** > **Class of Control** > **Access List** menu option.) Choosing an access list that contains no members equates to choosing the Always ring this destination radio button.
Association Information	
Line	This entry displays a line that can associate with this remote destination.
Line Association	Check this check box if you want to associate a particular line with this remote destination. You must check a line association check box for Cisco Unified Mobility to work for this remote destination. **Note** Be aware that the line association check box of a line must be checked for Cisco Unified Mobility calls to ring this remote destination when a call comes into the directory number that is assigned to that line.

FMC Over SIP Trunks Without Smart Client

Cisco Unified Communications Manager allows service providers to provide base PBX-extension features such as enterprise dialing, SNR, single VM, call move, and mid-call features via the trunk without a smart client on the mobile. Basic mobile features such as Single Number Reach, Deskphone pickup, Send Call to Mobile, Mobile Voice Access and Mid-call DTMF features are supported. Extension dialing is supported if it is implemented in the network and the network is integrated with Cisco Unified Communications Manager. These features can be provided by any type of trunk.

With previous versions of Cisco Unified Communications Manager, service providers used the Remote Destination feature to deliver network-based FMC including the enterprise dialing/DVO feature without a client. This version allows for a new device type called Carrier-Integrated Mobile to deliver network-based FMC via the trunk or gateway.

When configuring the new device type Carrier-Integrated Mobile, set the Owner User ID value to the mobile user identity. The mobile user identity does not appear on the configuration page. Only end users with mobility enabled will appear in the Owner User ID drop-down on the end user page. Only one line (DN) can be associated with an FMC device. Users should associate a mobile identity with the FMC. This can be done on the FMC device configuration page after the device has been added. For calls to be extended to the number of the mobile identity, users must enable Cisco Unified Mobility on the Mobile Identity window.

Cisco Unified Communications Manager can be configured in the Ring All Shared Lines service parameter so that the shared-line is rung when mobile DN is dialed.

Note The Reroute Remote Destination Calls to Enterprise Number feature must be enabled for Ring All Shared Lines to take effect. Reroute Remote Destination Calls to Enterprise Number is disabled by default.

IMS shared lines will ring solely based on the value of the Ring All Shared Lines parameter. In previous versions of Cisco Unified Communications Manager, IMS shared lines rang based on the value of Reroute Remote Destination Calls to Enterprise Number.

You can also migrate from the Remote Destination feature used in previous versions to this new device type.

Mobile Voice Access Directory Number Configuration

Use the Mobile Voice Access window under Media Resources to assign sets of localized user prompts for Mobile Voice Access.

This configuration is required for making calls with the Mobile Voice Access feature. After the gateway collects the required digits from the user to make a call, the call gets transferred to the DN that is configured in this window. This DN can be an internal DN to Cisco Unified Communications Manager and the end user does not need to know the DN. The administrator 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, as configured in the Inbound Calling Search Space for Remote Destination service parameter in the Clusterwide Parameters (System - Mobility) pane.

To assign localized users prompts for Mobile Voice Access, perform the following procedure:

Procedure

Step 1 In the menu bar, choose **Media Resources** > **Mobile Voice Access**.

Step 2 Enter values for the parameters that are described in Mobile Voice Access Configuration, on page 285.

Step 3 Click **Save.**

Mobile Voice Access Configuration

The following table describes the available settings in the Mobile Voice Access window.

Table 35: Mobile Voice Access Configuration Settings

Field	Description
Mobile Voice Access Information	
Mobile Voice Access Directory Number	Enter the internal DN to receive Mobile Voice Access calls from the gateway. Enter a value between 1 and 24 digits in length. You may use the following characters: 0 to 9. **Note** The Mobile Voice Access Directory Number field is required only for legacy Mobile Voice Access where the gateway provides the IVR resource. For native Mobile Voice Access, Cisco Unified Communications Manager provides the IVR. In this case, you do not need to configure a Mobile Voice Access Directory Number.
Mobile Voice Access Partition	From the drop-down list, choose a partition for Mobile Voice Access. The combination of directory number and partition makes the Mobile Voice Access directory number unique.
Mobile Voice Access Localization	
Available Locales	This pane displays the locales that have been configured. See the Unified Communications Manager Locale Installer documentation for details. Use the Down Arrow key to move the locales that you select to the Selected Locales pane. **Note** Cisco Unified Mobility supports a maximum of nine locales. If more than nine locales are installed for Unified Communications Manager, they will display 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 displays: “Update failed. Check constraint (informix.cc_ivruserlocale_orderindex) failed.”

Field	Description
Selected Locales	Use the arrows above this pane to move the locales that you want to select to or from this pane. **Note** Remember that you can select a maximum of nine locales, even if more locales are available in the system. Use the arrow keys to the right of this pane to reorder the locales that are listed in the pane. Choose a locale by clicking the locale name; then, use the arrow key to change the order of the chosen locale. **Note** Mobile Voice Access uses the first locale that displays in the Selected Locales pane in the Mobile Voice Access window when the IVR is used. For example, if English United States displays first in the Selected Locales pane, the Cisco Unified Mobility user receives English when the IVR is used during a call.

Gateway Configuration for Enterprise Feature Access

To configure H.323 or SIP gateways for Enterprise Feature Access, two options are available: configure an H.323 or SIP gateway, or configure an H.323 gateway for system remote.

Configure an H.323 or SIP Gateway

If you already have an H.323 or SIP gateway that is configured in Cisco Unified Communications Manager, you can use it to support system remote access. If you do not have an H.323 or SIP gateway, you must add and configure one. For more information, see the *Cisco Unified Communications Manager Administration Guide*.

Note When a Cisco Unified Mobility call is placed from an internal extension, the system presents only the internal extension as the caller ID. If an H.323 or SIP gateway is used, you can use translation patterns to address this issue.

To configure the gateway, follow these steps.

Procedure

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

Sample configuration:

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

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

Sample configuration:

- 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 Cisco Unified Communications Manager server (Publisher).

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

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

Sample configuration before IOS Version 12.3(12):

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

Note Although VXML was added in Version 12.2(11), Versions 12.3(8), 12.3(9), 12.3(14)T1, and 12.2(15) have VXML issues, and you should not use them.

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

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

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 (where 58888 represents the Mobile Voice Access number)

Step 5 Add a dial-peer to transfer the calls to the Mobile Voice Access DN that is configured in the Mobile Voice Access Directory Number Configuration, on page 284.

Sample configuration for primary Cisco Unified Communications Manager:

- dial-peer voice 101 voip
- preference 1

- destination-pattern <Mobile Voice Access DN>

  Note This specifies the Mobile Voice Access DN that is configured with the Media **Resources** > **Mobile Voice Access** menu option. If a generic dial-peer is already configured to terminate the calls and is consistent with the Mobile Voice Access DN, you do not need to perform this step.

- session target ipv4:10.1.30.3
- codec g711ulaw
- dtmf-relay h245-alphanumeric
- no vad

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

- dial-peer voice 102 voip
- preference 2
- destination-pattern <Mobile Voice Access DN>

  Note This specifies the Mobile Voice Access DN that is configured with the Media **Resources** > **Mobile Voice Access** menu option. If a generic dial-peer is already configured to terminate the calls and is consistent with the Mobile Voice Access DN, you do not need to perform this step.

- session target ipv4:10.1.30.4
- codec g711ulaw
- dtmf-relay h245-alphanumeric
- no vad

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 an H.323 Gateway for System Remote Access

If you do not have an H.323 gateway but want to use a H.323 gateway only to support System Remote Access, you must add and configure the gateway. For more information, see the *Cisco Unified Communications Manager Administration Guide*.

To configure the gateway, follow these steps.

Procedure

Step 1 Load the VXML application from the Cisco Unified Communications Manager server (Publisher).

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

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

Sample configuration before IOS Version 12.3(12):

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

Note Although VXML was added in Version 12.2(11), Versions 12.3(8), 12.3(9), 12.3(14)T1, and 12.2(15) have VXML issues, and you should not use them.

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

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>

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 DN that is configured in the Mobile Voice Access Directory Number Configuration, on page 284.

Sample configuration for primary Cisco Communications Manager:

- dial-peer voice 101 voip
- preference 1
- destination-pattern <Mobile Voice Access DN>

  Note This specifies the Mobile Voice Access DN that is configured with the **Media Resources** > **Mobile Voice Access** menu option. If a generic dial-peer is already configured to terminate the calls and is consistent with the Mobile Voice Access DN, you do not need to perform this step.

- session target ipv4:10.1.30.3
- voice-class h323 1
- codec g711ulaw
- dtmf-relay h245-alphanumeric
- no vad

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

- dial-peer voice 102 voip
- preference 2
- destination-pattern <Mobile Voice Access DN>

  Note This specifies the Mobile Voice Access DN that is configured with the **Media Resources** > **Mobile Voice Access** menu option. If a generic dial-peer is already configured to terminate the calls and is consistent with the Mobile Voice Access DN, you do not need to perform this step.

- session target ipv4:10.1.30.4
- voice-class h323 1
- codec g711ulaw
- dtmf-relay h245-alphanumeric
- no vad

Step 4 Configure hairpin.

- voice service voip
- allow-connections h323 to h323

Step 5 On the Cisco 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 gets created.

Configure Enterprise Feature Access Two-Stage Dialing

Use this procedure to configure enterprise feature access two-stage dialing.

When a caller calls the Enterprise Feature Access DID, Cisco Unified Communications Manager matches the calling number to the destination number that is configured in the Remote Destination Configuration window. In the scenario where Cisco Unified Communications Manager Administration inserts the digit 9 to get an outside line, the administrator can manipulate the quantity of digits of this number by modifying these service parameters in the Clusterwide Parameters (System - Mobility) section:

- Matching Caller ID with Remote Destination
- Number of Digits for Caller ID Partial Match

No IVR exists with this configuration, so callers do not receive a prompt.

See the User Guide of the remote phone model for the steps that users perform to make outbound calls and to use Mobile Voice Access. Keep in mind that, when you use Enterprise Feature Access, each entry must end with the # (octothorpe) character.

Note When calling the Mobile Voice Access DN or Enterprise Feature Access DN, the gateway device must present the exact number of digits that are configured as the Mobile Voice Access DN or Enterprise Feature Access DN. Translation patterns or other called number modification cannot be used to match the MVA or EFA numbers either by stripping digits or by adding digits to the number that the gateway presents. Because Cisco Unified Mobility intercepts the call at the gateway layer, the feature behaves thus by design.

Note Unlike Mobile Voice Access (MVA), Enterprise Feature Access (EFA) identifies the user based solely on caller ID. If the system receives no inbound caller ID or receives a value that does not match a remote destination, the EFA call fails. With MVA, if the caller ID does not match, the user gets prompted to enter the user remote destination number. EFA does not provide this capability because no IVR prompts exist. In both cases, after the user is identified, the user authenticates by using the same PIN number.

Procedure

Step 1 Choose **System** > **Service Parameters**.

Step 2 For the Cisco CallManager service, set the following service parameters in the Clusterwide Parameters (System - Mobility) area:

a) Set the Enable Enterprise Feature Access service parameter to True.
b) Set the Matching Caller ID for Remote Destination service parameter. Choose either Complete Match or Partial Match. If you choose Partial Match, proceed to set a value for the Number of Digits for Caller ID Partial Match service parameter.
c) If you set the Matching Caller ID for Remote Destination service parameter to Partial Match, set the Number of Digits for Caller ID Partial Match service parameter.

Step 3 To save the service parameter settings, click **Save.**

Step 4 Choose **Call Routing** > **Mobility** > **Enterprise Feature Access Configuration**.

Step 5 In the Mobility Enterprise Feature Access Configuration window, configure the Enterprise Feature Access DID by specifying a value in the (Access Number Information) Number field. (This field specifies the same DID that is called to invoke midcall features like Transfer and Conference.)

Step 6 Specify the partition by choosing a value for the Route Partition.

Step 7 To save the Mobility Enterprise Feature Access Configuration settings, click **Save.**

Step 8 Ensure that the outbound VOIP dial-peer that is used on the gateway for the initial call leg over to the remote destination (mobile phone) has DTMF-relay configuration in it, so the DTMF codes can get passed through to Cisco Unified Communications Manager.

Step 9 Configure dial-peers on the gateway that receives the second-stage inbound call to the Enterprise Feature Access DID, so the call gets forwarded to the Cisco Unified Communications Manager. Ensure that the VOIP dial-peer has the DTMF-relay configuration in it.

Note If a generic dial-peer is already configured to forward the calls to Cisco Unified Communications Manager and is consistent with the EFA DN, you do not need to perform this step. Ensure that the VOIP dial-peer for this call leg also has a configured DTMF-relay command.

See the *Cisco Unified Communications Solution Reference Network Design (SRND)* Based on Cisco Unified Communications Manager for the list of steps that you need to configure Enterprise Feature Access.

Mobility Enterprise Feature Configuration

This section provides information about mobility enterprise feature configuration.

About Mobility Enterprise Feature Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Mobility** > **Enterprise Feature Access Configuration** menu path to configure mobility enterprise feature configuration.

The Mobility Enterprise Feature Configuration window allows you to configure mobility enterprise feature access (EFA) numbers. These numbers can then associate with mobility profile(s) for use.

Mobility Enterprise Feature Configuration Settings

The following table describes the available settings in the Mobility Enterprise Feature Configuration window.

Table 36: Mobility Enterprise Feature Configuration Settings

Field	Description
Access Number Information	
Number	Enter the DID number that is required for enterprise feature access. This number supports transfer, conference, resume, and two-stage dialing from smartphones. **Note** Ensure that each DID number is unique.
Route Partition	From the drop-down list box, choose the partition of the DID that is required for enterprise feature access.

Field	Description
Description	Enter a description of the Mobility Enterprise Feature Access number.
Default Enterprise Feature Access Number	Check this box to make this Enterprise Feature Access number the default for this system.

Handoff Mobility Configuration

This section provides information about handoff mobility configuration.

About Handoff Mobility Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Mobility** > **Handoff Configuration** menu path to configure handoff mobility configuration.

The Handoff Mobility Configuration window allows you to configure a handoff number and/or partition for dual-mode phones between the Wi-Fi and Global System for Mobile communication (GSM) or Code Division Multiple Access (CDMA) networks.

Handoff Mobility Settings

The following table describes the available settings in the Handoff Mobility Configuration window.

Table 37: Handoff Mobility Configuration Settings

Field	Description
Handoff Configuration Information	
Handoff Number	Enter the DID number for handoff between the Wi-Fi and GSM or CDMA networks. The handoff feature requires this number. For numbers that start with the international escape character +, you must precede the + with a backslash (\). Example: \+15551234.
Route Partition	From the drop-down list box, choose the partition to which the handoff direct inward dial (DID) number belongs.

Mobility Profile Configuration

This section provides information about mobility profile configuration.

About Mobility Profile Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Mobility** > **Mobility Profile** menu path to configure mobility profiles.

Mobility profiles specify profiles where you can configure Dial-via-Office Forward or Dial-via-Office Reverse settings for a mobile client. After you configure a mobility profile, you can assign it to a user or to a group of users, such as the users in a region or location. You specify either DVO-F or DVO-R for a particular mobility profile, but you configure both the DVO-F and DVO-R settings for the mobility profile.

Mobility profiles can associate with a standalone mobile identity or with a dual-mode mobile identity. Standard, single-mode remote destinations cannot associate with a mobility profile.

Users cannot change the settings in a mobility profile.

Note If no mobility profile exists for a client and the client opts to let the server choose, the default DVO call type specifies Dial-via-Office Reverse (DVO-R).

Tips About Configuring Mobility Profiles

Before you start to configure mobility profiles, consider the design issues that follow.

If a client associates with a mobility profile and a DVO-R call is configured, the caller ID value in the 183 SIP message gets retrieved according to the following preference order:

1. DVO-R caller ID from the mobility profile (if this value is configured in the mobility profile)
2. EFA DN from mobility profile (if this value is configured in the mobility profile)
3. Default EFA DN

Note You must configure the caller ID value in at least one of the preceding settings for the DVO-R call to succeed.

If a client associates with a mobility profile and a DVO-F call is configured, the DID value in the 183 SIP message gets retrieved according to the following preference order:

1. DVO-F service access number from mobility profile (if this value is configured in the mobility profile)
2. DVO-F EFA DN from mobility profile (if this value is configured in the mobility profile)
3. Default service access number, which is configured in the Service Parameter Configuration window
4. Default EFA DN

Note For a DVO-F call, the client needs to make an incoming call to Cisco Unified Communications Manager that terminates at a particular DID. The administrator must configure this DID in at least one of the preceding settings for the DVO-F call to succeed.

Cisco Unified Communications Manager identifies an incoming PSTN call (made by the client) as DVO-F by matching the called number (that is, the DID number that was sent in the 183 SIP message) in the following priority order:

If a mobility profile associates with the client

1. DVO-F EFT DN from mobility profile (if this value is configured)
2. DVO-F service access number from mobility profile (if this value is configured)

If no mobility profile associates with the client:

3. Default EFA DN
4. Default service access number

Also consider the following requirements when you configure mobility profiles:

- You must configure the PSTN gateway so that matching of the called party can take place.
- EFA DN and service access number always comprise a pair: both of these values are retrieved from the mobility profile and must match in the mobility profile, or both default values are retrieved and the default values must match.

Mobility Profile Configuration Settings

The following table describes the available settings in the Mobility Profile Configuration window.

Table 38: Mobility Profile Configuration Settings

Field	Description
Mobility Profile Information	
Name	Enter a unique name for this mobility profile, up to 50 characters in length. Valid values specify upper- and lowercase letters, numeric digits (0 through 9), periods (.), dashes (-), underscores (_) and spaces ( ).
Description	Enter a description for this mobility profile.
Mobile Client Calling Option	From the drop-down list box, choose a mobile client calling option: • Dial via Office Reverse—Choose this option for the mobile client to make Dial-via-Office Reverse calls. • Dial via Office Forward—Choose this option for the mobile client to make Dial-via-Office Forward calls. **Note** The administrator configures either DVO-R or DVO-F for automatic selection by the client for any DVO calls that the user makes. Users can make the opposite type of DVO call than what the administrator has configured by explicitly choosing their DVO call type on their mobile devices.
Dial-via-Office Forward Configuration	

Field	Description
Service Access Number	Enter the DID number that is required for Dial-via-Office Forward feature access. This number supports transfer, conference, resume, and two-stage dialing from smartphones. This number gets returned in the 183 SIP message that Cisco Unified Communications Manager sends to the client. The client uses this value as a dial-in DID. Cisco Unified Communications Manager uses this value as the first preference to search when completing a DVO-F call. If this value is not configured, Cisco Unified Communications Manager uses the value in the Enterprise Feature Access Number/Partition field. **Note** Ensure that each DID number is unique.
Enterprise Feature Access Number/Partition	From the drop-down list box, choose the number or number and partition of the DID that is required for Dial-via-Office Forward call completion. After the client dials the Service Access Number, the gateways compare this value with the stripped digits that Cisco Unified Communications Manager sends. If the number is configured with a partition, both the number and the partition display in the drop-down list box. Cisco Unified Communications Manager uses this value as the second preference to search when completing a DVO-F call.
Dial-via-Office Reverse Callback Configuration	
Callback Caller ID	Enter a callback caller ID for dial-via-office reverse callback completion. If the client makes a DVO-R call, Cisco Unified Communications Manager send this value in the 183 SIP message, and this value becomes the caller ID value for the callback call that the client receives. This value displays in the client screen for DVO-R.

Toll Bypass Optimization for Handoff

The Least Cost Routing (LCR) and Dialed Number Identification Service (DNIS) pool features were introduced as part of the Cisco Unified Communications Manager 8.5 release. These features led to reduced costs for Dial Via Office (DVO) calls by providing call routing based on the area, location, and region. Cisco Unified Communications Manager release 8.6.(1) leverages the LCR-DNIS feature to invoke Handoff. Toll Bypass Optimization for Handoff uses the Enterprise Feature Access Number configured in the Mobility Profile associated with the Mobile Identity. Using this feature eliminates the need for a separate Handoff DID to be configured, which can also result in cost savings. When a user needs to invoke legacy Handoff, the client must dial the administrator configured Handoff DID number, which would be an international call placed to the Handoff DID number in roaming scenarios, which incurs additional costs to the enterprise.

Cisco Mobile Clients that are registered with a release previous to 8.6.(1) of Cisco Unified Communications Manager will continue to have the legacy Handoff invocation. For more information see, Session Handoff, on page 249.

Toll Bypass Optimization for Handoff Dial Via Office - Forward (DVO-F)

Enable DVO-F for all handoff calls between cellular and WiFi to leverage LCR policies for cost savings. Mid-call features can be triggered after handoff.

To configure LCR enabled handoff for DVO-F, perform the following procedures:

1. Configure an Enterprise Feature Access Number. For more information, see About Mobility Enterprise Feature Setup, on page 292.
2. Configure a Handoff DN. For more information, see Handoff Mobility Configuration, on page 293.
3. Create a Mobility Profile Associated with the Mobile Identity with the Mobile Client Calling Option set to DVO-F. For more information, see Mobility Profile Configuration, on page 293.

Toll Bypass Optimization for Handoff Dial Via Office - Reverse (DVO-R)

Enable DVO-R for all handoff calls between cellular and WiFi to leverage LCR policies for cost savings. Mid-call features can be triggered after handoff.

To configure LCR enabled handoff for DVO-R, perform the following procedures:

1. Configure an Enterprise Feature Access Number. For more information, see About Mobility Enterprise Feature Setup, on page 292.
2. Create a Mobility Profile Associated with the Mobile Identity the Mobile Client Calling Option set to DVO-R. For more information, see Mobility Profile Configuration, on page 293.

Unified Application Dial Rule Configuration for Mobility

Cisco Unified Communications Manager 8.5 and earlier versions, required that Application Dial Rules be configured locally on the client side for VoIP calls and separately in Cisco Unified Communications Manager for DVO calls. To simplify configuration for both VoIP and DVO calls, Cisco Unified Communications Manager 8.6(1) allows Application Dial Rule configuration to apply to DVO as well as VoIP calls, so that there is no separate client configuration required. This allows mobile users to make calls with both the enterprise dial plan or service provider dial plan regardless of the transports and provides a consistent way to manage dial plans. When a client makes a call in either VOIP or DVO mode, the same rule applies. Mobility uses the Application Dial Rules in such a way that the client can dial a 10-digit number in VoIP mode to call an external number as it does in DVO mode.

Note VoIP mode is applicable to only SIP based mobile clients using enbloc dialing and cannot be applied to SCCP based mobile clients using overlap dialing.

This feature uses existing Application Dial Rule configuration and Mobility is treated as an application. For more information about Dial Rules, see the Cisco Unified Communications Manager System Guide. For more information about Application Dial Rule configuration, see the Cisco Unified Communications Manager Administration Guide.

Application Dial rules are shared by all applications. Ensure that the Application Dial rules you configure for Mobility do not conflict with Application Dial rules shared among other applications.

Mobility Softkey Configuration

Note Do not configure the Mobility softkey and the MOVE softkey together.

Follow this procedure to configure a Mobility softkey for the phone user that uses Cisco Unified Mobility.

Procedure

Step 1 Choose **Device** > **Device Settings** > **Softkey Template**.

Step 2 To list the existing templates, click **Find**.

Step 3 To create the new template, click **Standard User** and then click **Copy**.

Step 4 Enter a name and description for the Softkey template and click **Save**.

Step 5 Select Configure Softkey Layout from the Go next to Related Link menu in the upper, right corner of the window and click **Go.**

Step 6 Select On Hook from the pull-down list box.

Step 7 Add Mobility to the selected Softkeys and click **Save**.

Step 8 Select Connected from the pull-down list box.

Step 9 Add Mobility to the selected Softkeys and click **Save**.

Step 10 Open the Phone Configuration window and associate the Softkey Template with the created Softkey template. See the Cisco Unified Communications Manager Administration Guide.

Step 11 Choose the Owner User ID for the Cisco Unified Mobility phone user.

Step 12 Click **Save**.

Cisco Jabber for Mobile

This chapter provides information about functionality for Cisco Mobile VoiP Clients which connect directly with Cisco Unified Communications Manager. This chapter discusses the features and the required configurations.

Cisco Mobile VoiP Clients register directly with Cisco Unified Communications Manager

Cisco Mobile is the name given to a family of clients that run on mobile devices. Different Cisco Mobile clients offer different features. Features may include the following:

- Direct connection from Cisco Unified Communications Manager to mobile client without proxy server

- Dial-via-Office (DVO) optimization settings for toll reduction
- Enable/disable Cisco Unified Mobility from mobile phone
- Dial-via-Office Reverse Callback
- Dial-via-Office Forward
- Ability to transfer active Dial-via-Office calls between the mobile device and the desktop phone

See the following documentation for details about configuring Cisco Unified Mobility and Cisco Mobile VoiP Clients:

- End-user guides for Cisco Mobile VoiP Clients.
- End-user guide for a particular Cisco Unified IP Phone for procedures that end users follow to configure the Cisco Unified Mobility settings for their phones by using the Cisco Unified Communications Self Care Portal windows.

Configuration for Cisco Mobile VoiP Clients

See the Cisco Mobility installation guide for complete configuration instructions for Cisco Mobile VoiP Clients.

For more information on Cisco Unified Mobility features that are available upon configuration of the Cisco Unified Mobility Advantage server, see the List of Cisco Mobile VoiP Client Features, on page 300.

Cisco Mobile VoIP Clients

This section provides information about Cisco Mobile VoIP clients.

Be aware that special configuration in Cisco Unified Communications Manager Administration is required for features that Cisco Mobile VoIP Clients provide.

Terminology

The following table provides definitions of terms that are related to Cisco Unified Mobility with Cisco Mobile VoiP Clients.

Table 39: Definitions

Term	Definition
Cisco Mobile 8.x	These direct-connect dual-mode clients support voice-over-Wi-Fi (for costing savings) in addition to cellular. They connect to Cisco Unified Communications Manager directly without the need of a proxy server.

List of Cisco Mobile VoiP Client Features

This section provides a list of Cisco Unified Mobility features that are available to mobile phone users when the Cisco Mobile VoiP Client has been configured. This material discusses configuration within Cisco Unified Communications Manager Administration.

The following entities and features require configuration of Cisco Unified Mobility in Cisco Unified Communications Manager Administration:

- Direct connection from Cisco Unified Communications Manager to mobile client without proxy server - This feature provides server-side support for Cisco Mobile VoiP Clients to connect to Cisco Unified Communications Manager directly and thus eliminate Cisco Unified Mobility Advantage in the deployment. Cisco Unified Communications Manager adjusts to support direct connection with the Cisco Mobile VoiP Client.
- DVO Optimization Settings for Toll Reduction - This feature supports a pre-configured policy to determine which mobile origination call (DVO-R or DVO-F) yields the least cost to the enterprise; this determination is typically based on locations. Administrators assign a profile based on the user location and any other available information. Least cost routing negotiates with Cisco Unified Communications Manager to determine whether DVO-R or DVO-F generates the least cost, then chooses the less costly method for making the call.
- Enable/Disable Cisco Unified Mobility From Mobile Phone - This feature allows the Cisco Mobile VoiP Client to change the Cisco Unified Mobility status dynamically and keep the Cisco Unified Mobility Status between Cisco Unified Communications Manager and the client in sync. This feature provides the flexibility to the end user: the end user can change the user Cisco Unified Mobility status from the user mobile phone, not just from the GUI website.

The following features, which were originally part of Cisco Unified MobilityManager, now reside in Cisco Unified Communications Manager:

- Cisco Unified Mobility
- Desktop Call Pickup
- Access List

Cisco Unified Communications Manager also supports the following Cisco Unified Mobility features:

- Midcall Enterprise Feature Support Using DTMF
- Dual-mode Phone Support
- Manual Handoff of Calls on a Dual-mode Phone
- Time-of-Day Access
- Directed Call Park via DTMF
- SIP URI Dialing

See topics related to the benefits of Cisco Unified Mobility features for a discussion of other benefits of Cisco Unified Mobility features, such as simultaneous desktop ringing, single enterprise voice mailbox, system remote access, caller ID, remote on/off control, call tracing, security and privacy for Cisco Unified Mobility calls, and smartphone support.

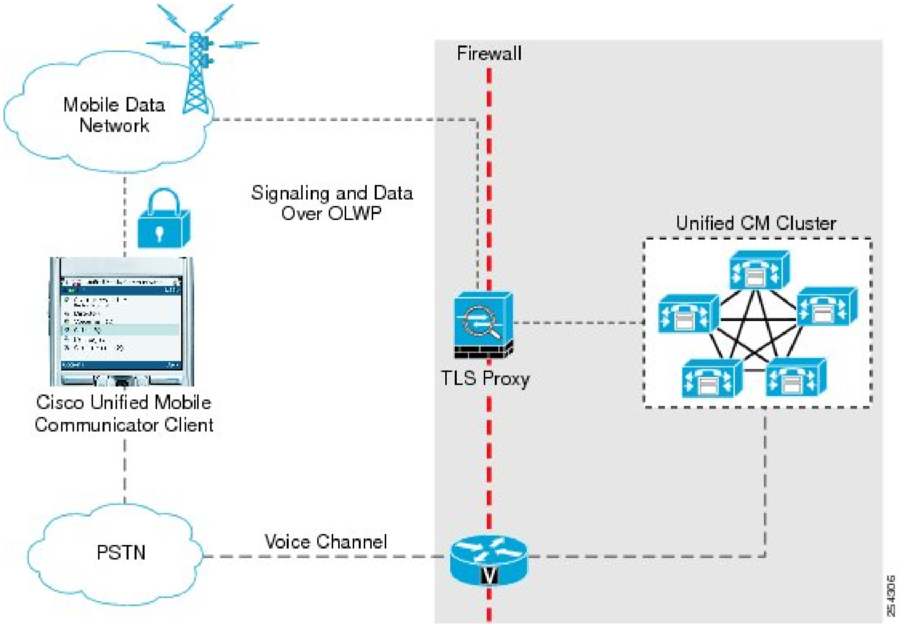
Related Topics

- Benefits of Cisco Unified Mobility Features, on page 238
- Cisco Unified Mobility, on page 233
- Direct Connection From CUCM to Mobile Client, on page 301
- DVO Optimization Settings, on page 302
- Enable or Disable Cisco Unified Mobility From Mobile Phone, on page 302
- Cisco Unified Mobility, on page 239

Direct Connection From CUCM to Mobile Client

Registration between the Cisco Mobile VoiP Client and Cisco Unified Communications Manager takes place over a separate TCP port. (The shared or pooled connection that was used by the Cisco Unified Mobility Advantage server is not used.) Keepalive messages between the Cisco Mobile VoiP Client and Cisco Unified Communications Manager remain the same as those passed between Cisco Unified Communications Manager and Cisco Unified Mobility Advantage. Cisco Mobile VoiP Client registration with Cisco Unified Communications Manager introduces no new alarms, and registration takes place over the SIP channel.

Figure 15: Cisco Mobile VoiP Client Registration with Cisco Unified Communications Manager



If the client is running on the iPhone and the Cisco Mobile VoiP Client is unable to complete the SIP dialog, the Cisco Unified Communications Manager retains the PSTN call. (The PSTN call does not drop even if the SIP stat times out.) For example, if Cisco Unified Communications Manager does not receive an ACK message after it sends a 200 OK message, the PSTN call gets retained.

Limitation for Direct Connection From Cisco Unified Communications Manager to Mobile Client

This feature specifies the following limitation:

- If the SIP dialog between Cisco Unified Communications Manager and the Cisco Mobile VoiP Client is not complete, the dialog cannot be used for further midcall feature invocations. The user can, however, invoke midcall features through the DTMF interface.

DVO Optimization Settings

This feature supports a pre-configured policy to determine which mobile origination call (DVO-R or DVO-F) yields the least cost to the enterprise; this determination is typically based on locations. This feature benefits the mobile user by allowing the user to find the least cost when making a mobile call. The DNIS pool provides a list of Direct Inward Dialing (DID) numbers so that the user, if roaming, can choose a non-international number for the mobile call. Least cost routing negotiates with Cisco Unified Communications Manager to determine whether DVO-R or DVO-F generates the least cost, then chooses the less costly method for making the call.

Reasons for Least Cost Routing and DNIS Pool

The following reasons make this feature desirable:

- Administrator can decide upon the DVO call type, DVO-F or DVO-R, for least cost call routing. In certain regions and with certain service providers, DVO-F can be more economical for mobile users; in other regions, DVO-R can be more economical. For example, in regions where incoming calls are free for mobile phone users, configuring a DVO-R call for mobile phone users achieves least cost call routing.
- Scalability - Multiple users in a given region can use a single mobility profile, which comprises region, service provider, location, and so forth. Here, “users” refers to the clients under actual end users. The administrator does not need to create a mobility profile for each end user.
- Single DID within a cluster for all DVO-F calls - For such DVO-F calls, the client makes an incoming call to Cisco Unified Communications Manager by using a particular DID.
- Multisite cluster - For a multisite cluster, a client in cluster A (such as the UK) uses the DID of cluster B (such as San Jose) for DVO-F calls, which incurs costs.
- DVO-R - Trunk allows calls that originate from a local DID. At times, when a client makes an outgoing DVO-R call, the client trunk may not allow an outgoing call if the caller ID does not lie in a specific range. For example, if a UK client invokes DVO-R, the callback call from the trunk at the San Jose cluster shows 408. When this call reaches the UK, the service provider trunk may not recognize the 408 and therefore not allow the call. Therefore, the caller IDs need to specify the local identifiable values.

Characteristics of DVO Optimization Settings for Toll Reduction

This feature involves the use of mobility profiles, which the administrator configures by using the Call Routing > Mobility > Mobility Profile menu path in Cisco Unified Communications Manager Administration. See the Mobility Profile Configuration, on page 293 for additional details about mobility profiles.

The DVO Optimization Settings for Toll Reduction feature does not change the alternate callback mechanism that DVO-R calls use: the client continues to control alternate callback.

Limitation of DVO Optimization Settings for Toll Reduction

The DVO Optimization Settings for Toll Reduction feature specifies the following limitation:

- Least Cost Routing (LCR) rules are applied after application dial rules. Called party transformations and call forward scenarios do not get considered for LCR.

Enable or Disable Cisco Unified Mobility From Mobile Phone

The Cisco Mobile VoiP Client can update its Cisco Unified Mobility status directly.

Interactions and Limitations

Be aware that most standard Cisco Unified Communications Manager features are fully compatible with Cisco Unified Mobility features. See the chapter for Cisco Unified Mobility for details of any exceptions.

Related Topics

Cisco Unified Mobility, on page 233

Interactions, on page 258

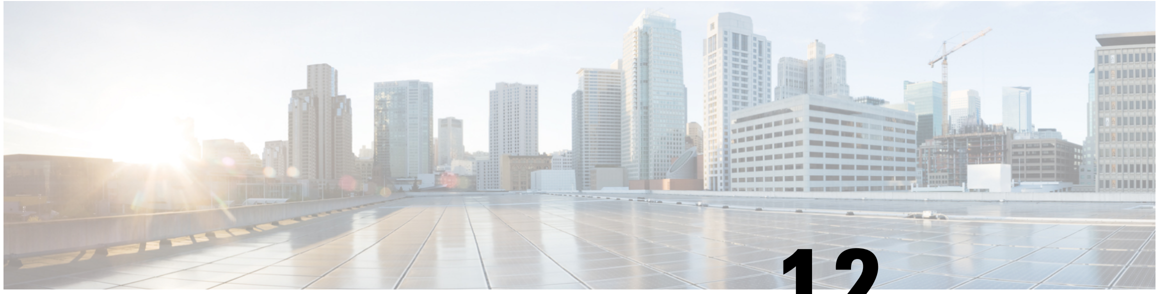
Limitations, on page 260

System Requirements

See the Cisco Mobile release notes for detailed system requirements.

Configure Cisco Mobile VoiP Clients

For details about configuring the Cisco Mobile VoiP Clients, see the configuration guides for Cisco Mobile VoiP Clients.



CHAPTER 12

Cisco Unified Communications Manager Assistant with Proxy Line Support

This chapter provides information about Cisco Unified Communications Manager Assistant feature which enables managers and their assistants to work together more effectively. Cisco Unified Communications Manager Assistant supports two modes of operation: proxy line support and shared line support.The Cisco IP Manager Assistant service supports both proxy line and shared line support simultaneously in a Cisco Unified Communications Manager server. For information about Cisco Unified Communications Manager Assistant with shared line support, see the Cisco Unified Communications Manager Assistant with Shared Line Support, on page 345.

Cisco Unified Communications Manager Assistant supports up to 3500 managers and 3500 assistants. To accommodate this number of users, the administrator configures up to three Cisco Unified Communications Manager Assistant applications in one Cisco Unified Communications Manager cluster and assigns managers and assistants to each instance of the application.

The feature comprises a call-routing service, enhancements to phone capabilities for the manager and the assistant, and assistant console interfaces that are primarily used by the assistant.

The service intercepts calls that are made to managers and routes them to selected assistants, to managers, or to other targets on the basis of preconfigured call filters. The manager can change the call routing dynamically; for example, by pressing a softkey on the phone, the manager can instruct the service to route all calls to the assistant and can receive status on these calls.

Cisco Unified Communications Manager Assistant users comprise managers and assistants. The routing service intercepts manager calls and routes them appropriately. An assistant user handles calls on behalf of a manager.

Configure Cisco Unified Communications Manager Assistant with Proxy Line Support

Cisco Unified Communications Manager Assistant, a plug-in that allows an assistant to handle calls on behalf of a manager, intercepts manager calls and routes them appropriately. When you configure Cisco Unified Communications Manager Assistant in proxy-line mode, the manager and assistant do not share a directory number. The assistant handles calls for a manager using a proxy number. The proxy number is not the directory number for the manager, but 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 Cisco Unified Communications Manager Assistant, which include default assistant selection, assistant watch, call filtering, and divert all calls.

Perform the following steps to configure Cisco Unified Communications Manager Assistant with proxy line support.

Procedure

Step 1 If you have not already done so, configure the phones and users and associate the devices to the users.

Step 2 In Cisco Unified Serviceability, activate the Cisco IP Manager Assistant service in the Service Activation window.

Step 3 Configure system administration parameters:

- Add three partitions.
- Add two calling search spaces.
- Add the CTI route point for Cisco Unified Communications Manager Assistant. You can have only one route point per server.
- Configure Cisco IP Manager Assistant service parameters.

Tip To automatically configure these system administration parameters, use the Cisco Unified Communications Manager Assistant Configuration Wizard.

- Add the partition of the manager line to the calling search space of the Message Waiting Indicator (MWI) on and off number (if MWI is required).
- If using the Cisco Unified Communications Manager intercom feature, add the Intercom partition, Intercom calling search space, Intercom directory number, and the Intercom translation pattern.

Step 4 If multiple Cisco Unified Communications Manager Assistant pools are required to support large numbers of assistants and managers, configure the following Cisco IP Manager Assistant clusterwide service parameters:

- Enable Multiple Active Mode
- Pool 2 and Pool 3 Cisco IPMA Server IP Address

Step 5 Configure the application user CAPF profile (optional).

Step 6 Configure Cisco IP Manager Assistant service parameters for security (optional).

Step 7 Using the Serviceability Control Center Feature Services, stop and start the Cisco IP Manager Assistant service.

Step 8 Configure phone parameters:

- Add Assistant Primary service as a Cisco Unified IP Phone service. If necessary, add Assistant Secondary service pointing to the Cisco Unified Communications Manager Assistant backup server as a Cisco Unified IP Phone service.
- Check the Enable check box to activate the service.
- Configure Cisco Unified IP Phone.

Step 9 Configure manager and assistant Cisco Unified IP Phone parameters:

- Set up manager phone.
- Set up assistant phone.

Step 10 Configure manager phone settings:

- Assign a softkey template.
- If using Do Not Disturb, configure the Do Not Disturb fields on the manager phone.
- Add a primary line.
- Set up voice-mail profile on primary line.
- Add intercom line.
- For Cisco Unified IP Phones 7940 and 7960, add speed dial for outgoing intercom targets.
- For Cisco Unified IP Phones 7942, 7945, 7962, 7965, and 7975 add the intercom capabilities.
- Subscribe to Cisco Unified IP Phone Service, Cisco Unified Communications Manager Assistant Primary Phone Service. If necessary, subscribe to Cisco Unified IP Phone Service, Cisco Unified Communications Manager Assistant Secondary Phone Service.
- Set user locale.
- Reset the phone.

Tip To automatically configure some of the manager phone settings, choose the automatic configuration check box on the Manager Configuration window.

Step 11 Configure assistant phone settings:

- Assign a softkey template.
- Add a Cisco Unified IP Phone Expansion Module (optional).
- Add a primary line.
- Add proxy lines for each configured manager. Add a voice-mail profile that is the same as the voice-mail profile on the manager primary line.
- Add incoming intercom line.
- For Cisco Unified IP Phones 7940 and 7960, add speed dial for outgoing intercom targets
- For Cisco Unified IP Phones 7942, 7945, 7962, 7965, and 7975 add the intercom capabilities.
- Set user locale.
- Reset the phone.

Tip To automatically configure some assistant phone settings, choose the Automatic Configuration check box on the Assistant Configuration window..

Step 12 Configure Cisco Unified Communications Manager Assistant application:

- Create a new manager.
- Configure lines for manager.
- Assign an assistant to a manager.
- Configure lines for the assistant.

- Configure intercom lines (optional).

Step 13 Configure the dial rules for the assistant.

Step 14 Install the Assistant Console application.

Step 15 Configure the manager and assistant console applications.

Related Topics

Cisco Unified Communications Manager Assistant with Proxy Line Support, on page 305
Calling Search Space and Partitions, on page 323
Cisco Unified Communications Manager Assistant CTI Route Point, on page 324
Cisco Unified Communications Manager Assistant Configuration, on page 320
Set the Service Parameters for Cisco Unified Communications Manager Assistant, on page 325
Configure Proxy Incoming Intercom and Primary Lines, on page 338
Intercom, on page 685
Configure Multiple Servers for Cisco Unified Communications Manager Assistant Scalability, on page 328
Security Considerations, on page 329
Start the Cisco IP Manager Assistant Service, on page 330
Cisco Unified IP Phone Service Configuration , on page 330
Manager and Assistant Phone Configuration, on page 330
Do Not Disturb, on page 413
Delete Cisco Unified Communications Manager Assistant Information From the Manager, on page 337
Dial Rules Configuration, on page 341
Install the Assistant Console Plug-In, on page 342

Cisco Unified Communications Manager Assistant Feature

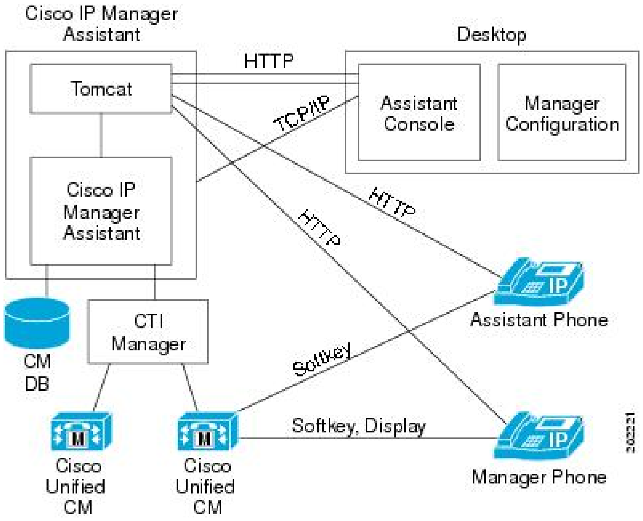
Cisco Unified Communications Manager Assistant, a plug-in that allows an assistant to handle calls on behalf of a manager, intercepts manager calls and routes them appropriately. When you configure Cisco Unified Communications Manager Assistant in proxy-line mode, the manager and assistant do not share a directory number. The assistant handles calls for a manager using a proxy number. The proxy number is not the directory number for the manager, but 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 Cisco Unified Communications Manager Assistant, which include default assistant selection, assistant watch, call filtering, and divert all calls.

Cisco Unified Communications Manager Assistant Overview

The Cisco Unified Communications Manager Assistant feature architecture comprises the Cisco IP Manager Assistant service, the assistant console interfaces, and the Cisco Unified IP Phone interfaces. See the following figure.

Cisco IP Manager Assistant service routes calls that are presented to a CTI route point that is defined in the Cisco IP Manager Assistant service parameters. See the Set the Service Parameters for Cisco Unified Communications Manager Assistant, on page 325.

Figure 16: Cisco Unified Communications Manager Assistant Architecture



Cisco IP Manager Assistant Service

Cisco Tomcat loads the Cisco IP Manager Assistant service, a servlet. Cisco Tomcat gets installed at Cisco Unified Communications Manager installation.

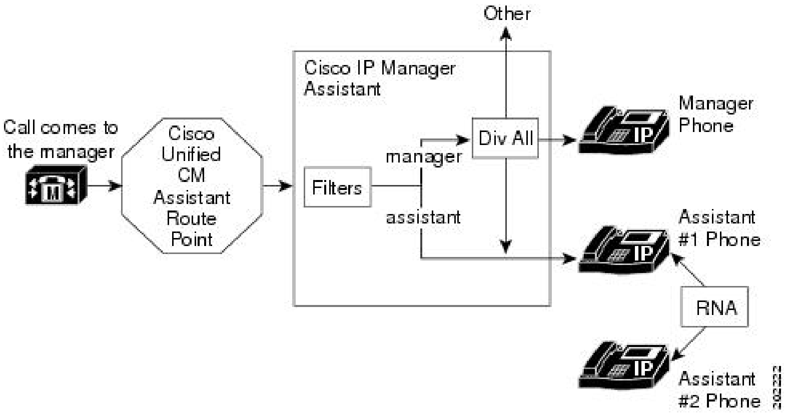
The Cisco IP Manager Assistant service gets installed on all Cisco Unified Communications Manager nodes. After installation, the administrator activates the service from Serviceability, which automatically starts Cisco Unified Communications Manager Assistant. The Cisco IP Manager Assistant service checks to see whether it is one of the Cisco Unified Communications Manager Assistant nodes that is configured in the clusterwide service parameter, Cisco IPMA Server (Primary) IP Address. If it is, the Cisco IP Manager Assistant service attempts to become the active Cisco IP Manager Assistant service.Currently, Cisco Unified Communications Manager supports only one active Cisco IP Manager Assistant service.

The Cisco IP Manager Assistant service performs the following tasks:

- Hosts the HTTP services that run on the manager phone.
- Hosts the web pages that the manager uses for configuration.
- Contains the routing logic that applies filters on an incoming call for a manager. See the following figure.
- Communicates to Cisco Unified Communications Manager through the Cisco CTIManager for third-party call control. Cisco Unified Communications Manager Assistant requires only one CTI connection.
- Accesses data from the database.
- Supports the Assistant Console application.

Cisco Unified Communications Manager supports redundancy of the Cisco IP Manager Assistant service. To achieve redundancy, you must configure a second Cisco IP Manager Assistant service in the same cluster.

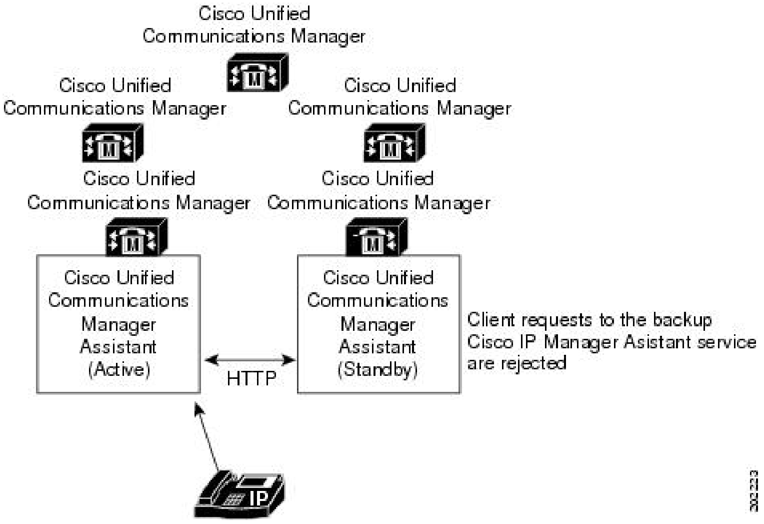
Figure 17: Cisco Unified Communications Manager Assistant Routing Logic for Proxy Line Support



Cisco Unified Communications Manager Assistant implements redundancy by using an active/standby node model. At any time, only one Cisco Unified Communications Manager Assistant node remains active and servicing all assistant console applications and phones. The other node stays in a standby mode and will detect failures on the active node. When it detects a failure, the backup node takes over and becomes the active node. All connections that were active get restored on the new node, and service continues uninterrupted to the users.

If the active node fails, the Assistant Console application fails over automatically to the backup node. The Cisco IPMA Assistant Console Heartbeat Interval service parameter (see the Set the Service Parameters for Cisco Unified Communications Manager Assistant, on page 325) determines the time that the application takes to detect failure. A shorter heartbeat interval leads to faster failover. See the following figure.

Figure 18: Cisco Unified Communications Manager Assistant Redundancy


Cisco Unified Communications Manager
Cisco Unified Communications Manager
Cisco Unified Communications Manager
Cisco Unified Communications Manager
Cisco Unified Communications Manager
Cisco Unified Communications Manager Assistant (Active)
HTTP
Cisco Unified Communications Manager Assistant (Standby)
Client requests to the backup Cisco IP Manager Asistant service are rejected
202223

The Cisco IP Manager Assistant service includes built-in security to help prevent unauthorized access to its services. The user ID and password that are collected at the assistant console get encrypted before they are sent over the network. The Assistant Console blocks nonauthorized users who are posing as assistants.

Assistant Console Interface

Cisco Unified Communications Manager Assistant supports the following assistant console interfaces for managers and assistants:

- Assistant Console (used for call control, log on, assistant preferences, monitoring managers call activity, keyboard shortcuts)
- Manager configuration (used to configure send all calls target, immediate divert target, and filters)

Administrators use Cisco Unified Communications Manager Administration, End User Configuration, to configure Cisco Unified Communications Manager Assistant for managers and assistants. See Cisco Unified Communications Manager Assistant Administration Interface, on page 313.

Cisco Unified Communications Manager makes all Cisco Unified Communications Manager Assistant manager features available through the Cisco Unified IP Phone, except manager configuration, which is available by using a browser. Assistants use the Cisco Unified IP Phone and the assistant console application. See Manager Interfaces, on page 311 and Assistant Interfaces, on page 312.

For more information about how to use the Cisco Unified Communications Manager Assistant features, see the Cisco Unified Communications Manager Assistant User Guide.

Cisco Unified IP Phone Interface

Managers and assistants use softkeys and the Cisco Unified IP Phone Services button to access the Cisco Unified Communications Manager Assistant features. For more information about how to use the Cisco Unified Communications Manager Assistant phone features, see the Cisco Unified Communications Manager Assistant User Guide.

See Manager Interfaces, on page 311 and Assistant Interfaces, on page 312.

Cisco Unified Communications Manager Assistant Database Access Architecture

The database stores all Cisco Unified Communications 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.

Manager Interfaces

The manager phone makes all manager features available with the exception of Manager Configuration. Cisco Unified Communications Manager Assistant automatically logs in a manager when the Cisco IP Manager Assistant service starts.

The manager can change selected assistants by using the Cisco Unified IP Phone **Services** button.

The manager accesses the Cisco Unified Communications Manager Assistant features Assistant Watch, Intercept Call, and Transfer to Voice Mail from the Cisco Unified IP Phone softkeys.

Note Managers also have access to Cisco Unified Communications Manager features such as Do Not Disturb and iDivert.

The state of the features Assistant Watch, Do Not Disturb, Divert All Calls, and Filtering displays in the Status Window on the Cisco Unified IP Phone.

You can enable filtering and choose filter mode by using the Cisco Unified IP Phone **Services** button. Configuration of the filters occurs by using Manager Configuration. You can access the Manager Configuration on the assistant console by using a web browser (see the Manager Configuration, on page 344).

See the Cisco Unified Communications Manager Assistant User Guide for more information.

Assistant Interfaces

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, an application, provides call-control functions such as answer, divert, transfer, and hold. The assistant uses the Assistant Console to log on and log off, to set up assistant preferences, and to display the manager configuration window that is used to configure manager preferences.

The Assistant Console displays the assistant lines and the manager proxy lines. A proxy line specifies a phone line that appears on the assistant Cisco Unified IP Phone. Assistants use the proxy lines to manage calls that are intended for a manager. For more information on setting up proxy lines, see the Configure Proxy Incoming Intercom and Primary Lines, on page 338.

When the assistant logs in from the Assistant Console, the softkeys Redirect and Transfer to Voice Mail become active for the proxy lines. See the Cisco Unified Communications Manager Assistant User Guide for more information.

Softkeys

The Cisco Unified Communications Manager Assistant feature supports softkeys such as Redirect, Transfer to Voice Mail, and Do Not Disturb on the Cisco Unified IP Phone. Softkeys appear in their appropriate call state; for example, Transfer to Voice Mail does not appear if no active calls exist.

Cisco Unified Communications 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

Additionally, the system makes call-processing (such as hold and dial) softkeys available with the Standard User template. The administrator configures the appropriate softkey template for the devices that managers and assistants use.

Note The default process assigns call-processing softkey templates to devices.

Administrators can create custom softkey templates in addition to using the standard softkey templates that are included in Cisco Unified Communications Manager. Use Softkey Template configuration in Cisco Unified Communications Manager Administration to associate softkey templates with Cisco Unified Communications Manager Assistant devices and to create custom softkey templates. See Configure Proxy Incoming Intercom and Primary Lines, on page 338 in the Cisco Unified Communications Manager Administration Guide.

Cisco Unified Communications Manager Assistant Administration Interface

The administrator uses the End User Configuration window in Cisco Unified Communications Manager Administration to configure the manager and assistant. The administrator chooses the device for the manager and assistant, configures an intercom line for the manager and assistant, and assigns a proxy line for a manager on the assistant phone.

See the Manager and Assistant Configuration, on page 334.

System Requirements for Cisco Unified Communications Manager Assistant with Proxy Line Support

Cisco Unified Communications Manager Assistant with proxy line support requires the following software components to operate:

- Cisco Unified Communications Manager
- Supported Browsers and platform:
  - Cisco Unified Communications Manager Assistant administration (using Cisco Unified Communications Manager Administration) and the Assistant Console are supported on Microsoft Internet Explorer (IE) 7.0 or later, Firefox 3.x or later, and Safari 4.x or later. (See the Interactions and Restrictions, on page 314 for more information.)
  - On a computer running Windows XP, Windows Vista, Windows 7, or Apple MAC OS X, a customer can open one of the browsers specified above.
- Cisco Unified Communications Manager Bulk Administration Tool (BAT) if bulk adding of managers and assistants is planned.

Because Cisco Unified Communications Manager Assistant installs automatically on the same server with Cisco Unified Communications Manager, an additional server is not required.

To determine which Cisco Unified IP Phones support Cisco Unified Communications Manager Assistant, see the Determine Device Support for Cisco Unified Communications Manager Assistant, on page 313.

Determine Device Support for Cisco Unified Communications Manager Assistant

Use the Cisco Unified Reporting application to generate a complete list of IP Phones that support Cisco Unified Communications Manager Assistant. To do so, follow these steps:

1. Start Cisco Unified Reporting by using any of the methods that follow.

   The system uses the Cisco Tomcat service to authenticate users before allowing access to the web application. You can access the application

   - by choosing Cisco Unified Reporting in the Navigation menu in Cisco Unified Communications Manager Administration and clicking **Go**.
   - by choosing **File** > **Cisco Unified Reporting** at the Cisco Unified Real Time Monitoring Tool (RTMT) menu.

- by entering `https://<server name or IP address>:8443/cucreports/` and then entering your authorized username and password.

2. Click **System Reports** in the navigation bar.
3. In the list of reports that displays in the left column, click the **Unified CM Phone Feature List** option.
4. Click the Generate a new report link to generate a new report, or click the Unified CM Phone Feature List link if a report already exists.
5. To generate a report of all IP Phones that support Cisco Unified Communications Manager Assistant, choose these settings from the respective drop-down list boxes and click **Submit**:

   Product: All

   Feature: IPMA

   The List Features pane displays a list of all devices that support the Cisco Unified Communications Manager Assistant feature. You can click on the Up and Down arrows next to the column headers (Product or Protocol) to sort the list.

For additional information about the Cisco Unified Reporting application, see the *Cisco Unified Reporting Administration Guide*.

Interactions and Restrictions

This section describes the interactions and restrictions for Cisco Unified Communications Manager Assistant with proxy line support.

Interactions

This section describes how Cisco Unified Communications Manager Assistant with proxy line support interacts with Cisco Unified Communications Manager applications and call processing.

Bulk Administration Tool

The administrator can use the Bulk Administration Tool (BAT) to add many users (managers and assistants) at once instead of adding users individually. See the Cisco Unified Communications Manager Bulk Administration Guide for more information.

The BAT templates that are created by the Cisco Unified Communications Manager Assistant Configuration Wizard for Cisco Unified IP Phones support only the Cisco Unified Communications Manager intercom lines.

Calling Party Normalization

Cisco Unified Communications Manager Assistantautomatically supports localized and globalized calls if you configure the calling party normalization feature. Cisco Unified Communications Manager Assistant can display localized calling party numbers on the user interfaces. In addition, for an incoming call to the manager, Cisco Unified Communications Manager Assistant can display localized and globalized calling party numbers when filter pattern matching occurs. For information on configuring calling party normalization, see the Calling Party Normalization, on page 193.

Extension Mobility

A manager who uses the Cisco Extension Mobility feature can simultaneously use Cisco Unified Communications Manager Assistant. The manager logs into the Cisco Unified IP Phone by using extension mobility, and Cisco Unified Communications Manager Assistant service then automatically gets enabled on that phone. The manager can then access the Cisco Unified Communications Manager Assistant features.

To have access to Cisco Extension Mobility with Cisco Unified Communications Manager Assistant, the administrator checks the Mobile Manager check box in the Manager Configuration window in Cisco Unified Communications Manager Administration (which is accessed from the End User Configuration window). See the Configure a Manager and Assign an Assistant for Proxy Line Mode, on page 335. For more information about configuring device profiles, see the Cisco Unified Communications Manager Administration Guide. For more information about Cisco Unified Communications Manager Extension Mobility, see Extension Mobility, on page 463

Internet Protocol Version 6 (IPv6)

Cisco Unified Communications Manager Assistant does not support IPv6, so you cannot use phones with an IP Addressing Mode of IPv6 Only with Cisco Unified Communications Manager Assistant. If you want to use Cisco Unified Communications Manager Assistant with the phone, make sure that you configure the phone with an IP Addressing Mode of IPv4 Only or IPv4 and IPv6. For more information on IPv6, see the Internet Protocol Version 6 (IPv6), on page 739.

Reporting Tools

Cisco Unified Communications 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 following sections describe these reporting tools.

CDR Analysis and Reporting

Cisco Unified Communications Manager Assistant supports call-completion statistics for managers and assistants and inventory reporting for managers and assistants. The CDR Analysis and Reporting (CAR) tool supports call-completion statistics. Cisco Unified Serviceability supports inventory reporting. See the Cisco Unified Serviceability Administration Guide and the Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide for more information.

IPMA_ChangeLog

The administrator can view a summary of changes that are made to the Manager or Assistant Configurations. A manager can change defaults by accessing the Manager Configuration from a URL.

An assistant can change the manager defaults from the Assistant Console.

Note See the Cisco Unified Communications Manager Assistant User Guide for information about the URL and Manager Configuration.

When changes are made, the information gets sent to a log file that is called ipma_changeLogxxx.log. The log file resides on the server that runs the Cisco IP Manager Assistant service at the following location:

file get activelog tomcat/logs/ipma/log4j

The administrator can download this file from the server by using the Trace Collection Tool in the Cisco Unified Real Time Monitoring Tool. See the Cisco Unified Real Time Monitoring Tool Administration Guide for more information.

The log file contains the following fields:

- LineNumber - The line in the log file with information about changes
- TimeStamp - The time that the configuration changed
- for Manager/Assistant - Designation of whether the change is for the manager or the assistant
- for Userid - The userid of the manager or assistant that is being changed
- by Manager/Assistant - Designation of whether the manager or the assistant made the change
- by Userid - The userid of the manager or assistant who made the change
- Parameter Name - What changed; for example, divert target number
- Old Value - The value of the information before the change
- New Value - The value of the information after the change

Because the information in the log file is comma delimited, the administrator can open the log file by using a spreadsheet application such as Microsoft Excel. Use the following procedure to save the log file contents to the Microsoft Excel application.

Procedure

Step 1 Start the Microsoft Excel application.

Step 2 To open the ConfigChange*.log file, choose **File** > **Open.**

Step 3 Choose the Original data type, file type as Delimited, and click **Next.**

Step 4 Choose Delimiters as Comma and click **Next.**

Step 5 When complete, click **Finish.**

Multilevel Precedence and Preemption (MLPP)

The following points describe the interactions between Cisco Unified Communications Manager Assistant with proxy line support and MLPP:

- Cisco Unified Communications Manager Assistant preserves call precedence in the handling of calls. For example, when an assistant diverts a call to a manager, Cisco Unified Communications Manager Assistant 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 Cisco Unified Communications Manager Assistant does not perceive the precedence of a call, it does not provide any additional indication of the precedence of a call on the assistant console.

Time-of-Day Routing

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 voice-messaging service.

Partitions specify the time schedule and time zone that Time-of-Day routing uses. Cisco Unified Communications Manager Assistant partitions and partitions in Cisco Unified Communications Manager Assistant calling search spaces support Time-of-Day routing.

For more information about Time-of-Day routing, see the Cisco Unified Communications Manager System Guide.

Message Waiting Indicator

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. For more information on configuring message waiting indicators, see the Cisco Unified Communications Manager Administration Guide.

Intercom

Cisco Unified Communications Manager Assistant supports the following intercom features:

- Cisco Unified Communications Manager Assistant intercom (used with Cisco Unified IP Phones 7940 and 7960). This intercom feature gets configured by using the DN configuration and end user (manager and assistant) configuration windows.
- Cisco Unified Communications Manager intercom (used with Cisco Unified IP Phones 7900 except 7940 and 7960). This intercom feature gets configured by using the intercom partition, intercom calling search space, intercom directory number, intercom translation pattern, DN, and end user (manager and assistant) configuration windows.

IPMA Configuration Wizard

The following interactions are applicable to IPMA configuration wizard:

- The **Assistant Route Point** status is **Unknown** before service parameters configuration
- Configuring Dial Rules in a shared line mode results in same number for Manager and Assistant phones
- Configuring Dial Rules in a proxy line mode results in different numbers for Manager and Assistant phones
- Sofkeys are available only in virtual environment with OVA templates

IPMA Phone Compatibility

The following procedure describes how to identify phones compatible for IPMA:

Procedure

Step 1 In the Cisco Unified Reporting, click **System Reports**

Step 2 Click **Unified CM Phone Feature List**

Step 3 From the **Product** drop down list, choose **default**

Step 4 From the **Feature** drop down list, choose **IPMA**

Step 5 Click **Submit**
The list of all the phones supporting IPMA displays.

Restrictions

The following restrictions apply to Cisco Unified Communications Manager Assistant:

- Cisco Unified Communications Manager Assistant supports SIP on Cisco Unified IP Phones 7900 series except the Cisco Unified IP Phone 7940 and 7960.
- Cisco Unified Communications Manager Assistant supports up to 3500 managers and 3500 assistants by configuring multiple Cisco IP Manager Assistant servers (pools). When multiple pools are enabled, a manager and all configured assistants for that manager should belong to the same pool.
- One manager can have up to 10 assigned assistants.
- One assistant can support up to 33 managers (if each manager has one Cisco Unified Communications Manager Assistant—Controlled Line).
- Cisco Unified Communications Manager Assistant supports up to 3500 managers and 3500 assistants per Cisco Unified Communications Manager cluster when you are using the MCS 7845 server.
- Cisco Unified Communications Manager Assistant is not supported in the single sign on environment.
- The Assistant Console does not support hunt groups/queues.
- The Assistant Console does not support record and monitoring.
- The Assistant Console does not support onhook transfer (the ability to transfer a call by pressing the Transfer softkey and going on hook to complete the transfer).
- The Assistant Console does not support the one-touch Call Pickup feature.
- Cisco Unified IP Phones 7940, 7942, and 7945 support only two lines or speed-dial buttons.
- When an upgrade to Cisco Unified Communications Manager Release 8.5.(1) occurs, existing Cisco Unified Communications Manager Assistant users that use the incoming intercom line do not get upgraded automatically to the Cisco Unified Communications Manager Intercom feature.
- The system does not support calls between the Cisco Unified Communications Manager Intercom feature and regular lines (which may be configured as Cisco Unified Communications Manager Assistant Intercom lines).
- Cisco Unified IP Phones 7960 and 7940 support only the Cisco Unified Communications Manager Assistant Intercom lines feature. Cisco Unified IP Phones 7900 (except 7940 and 7960) support only the Cisco Unified Communications Manager intercom feature.
- To install the Assistant Console application on a computer with Microsoft Internet Explorer 7 (or later) on Windows XP, install the Microsoft Java Virtual Machine (JVM) with Windows XP Service Pack 1 before the Assistant Console installation.

Install and Activate Cisco Unified Communications Manager Assistant

Cisco Tomcat loads the Cisco Unified Communications Manager Assistant, a servlet. Cisco Tomcat gets installed and started at Cisco Unified Communications Manager installation. For more information, see the Cisco Unified Communications Manager Assistant Overview, on page 308.

The administrator performs three steps after installation to make Cisco Unified Communications Manager Assistant available for system use:

1. Use Cisco Unified Serviceability Service Activation, located on the **Tools** menu, to activate the Cisco IP Manager Assistant service. See the Cisco Unified Serviceability Administration Guide.
2. Configure the applicable service parameters for the Cisco IP Manager Assistant service. See the Set the Service Parameters for Cisco Unified Communications Manager Assistant, on page 325.
3. Use the Serviceability Control Center Feature Service window to stop and start the Cisco IP Manager Assistant service. See the Start the Cisco IP Manager Assistant Service, on page 330.

Note If the managers and assistants will require Cisco Unified Communications Manager Assistant features to display (on the phone and assistant console) in any language other than English, verify that the locale installer is installed before configuring Cisco Unified Communications Manager Assistant. See the Cisco Unified Communications Operating System Administration Guide for information on locale installers.

Configure Cisco Unified Communications Assistant with Proxy Line Support

For successful configuration of Cisco Unified Communications Manager Assistant, review the steps in the configuration checklist, perform the system, user, and device configuration requirements, and configure the managers and assistants.

Note Cisco Unified Communications Manager Assistant with proxy line support coexists in the same Cisco Unified Communications Manager node with Cisco Unified Communications Manager Assistant with shared line support.

Tip Before you configure the Cisco Unified Communications Manager Assistant with proxy line support, review the summary task to configure Cisco Unified Communications Manager Assistant with proxy line support.

Related Topics

Configure Cisco Unified Communications Manager Assistant with Proxy Line Support, on page 306
Cisco Unified Communications Manager Assistant with Shared Line Support Configuration, on page 357

System Configuration with Proxy Line Support

Because the Cisco IP Manager Assistant service intercepts calls that are made to managers who are using proxy line mode, it requires configuration of partitions, calling search spaces, and route points. For more information on configuring Cisco Unified Communications Manager Assistant , see the **System Configuration with Proxy Line Support**.

You must perform the following configurations before you configure devices and users for Cisco Unified Communications Manager Assistant :

- Calling Search Space and Partitions, on page 323
- Cisco Unified Communications Manager Assistant CTI Route Point, on page 324

Cisco Unified Communications Manager Assistant provides a one-time-use configuration wizard that helps the administrator configure partitions, calling search spaces, a route point, and the Cisco Unified Communications Manager Assistant phone service. The Cisco Unified Communications Manager Assistant Configuration Wizard also creates the Cisco IP Manager Assistant service parameters in the Clusterwide Parameters (IPMA Device Configuration Defaults for Proxy Mode) section. For more information on the Cisco Unified Communications Manager Assistant Configuration Wizard, see the Cisco Unified Communications Manager Assistant Configuration, on page 320.

Note This document provides specific information about Cisco Unified Communications Manager Assistant configuration. For more information about configuring Calling Search Spaces, Partitions, and CTI Route Points, see the Cisco Unified Communications Manager Administration Guide.

Cisco Unified Communications Manager Assistant Configuration

Cisco Unified Communications Manager Assistant, a plug-in that allows an assistant to handle calls on behalf of a manager, intercepts manager calls and routes them appropriately. Perform the following steps to configure Cisco Unified Communications Manager Assistant with proxy line support.

With the Cisco Unified Communications Manager Assistant Configuration Wizard, configuration takes less time and eliminates errors. The partitions, calling search spaces, and route point automatically get created when the administrator successfully runs and completes the configuration wizard. The wizard also creates BAT templates for the manager phone, the assistant phone, and all other user phones. The administrator can use the BAT templates to configure the managers, assistants, and all other users. See the Cisco Unified Communications Manager Bulk Administration Guide.

Note The Cisco Unified Communications Manager Assistant Configuration Wizard only creates the Cisco IP Manager Assistant service parameters in the Clusterwide Parameters (IPMA Device Configuration Defaults for Proxy Mode) section of the Service Parameters Configuration window. You must enter the remaining service parameters manually. For service parameter information, see the Set the Service Parameters for Cisco Unified Communications Manager Assistant, on page 325.

The Cisco Unified Communications Manager Assistant Configuration Wizard provides windows for each configuration parameter. The windows provide the administrator with preconfigured information. If the administrator prefers to use other configuration information (for example, partition names), the administrator can change the preconfigured information to the appropriate information.

Perform the following procedure to configure the Cisco Unified Communications Manager Assistant system parameters by using the Cisco Unified Communications Manager Assistant Configuration Wizard.

Before you begin

Ensure that the configuration wizard runs from the same server (the Cisco Unified Communications Manager server) as the Bulk Administration Tool (BAT).

You can run the wizard only one time.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Application** > **Cisco Unified CM Assistant Configuration Wizard**.

The Cisco Unified Communications Manager Assistant Configuration Wizard Overview window displays and provides a description of the configuration wizard process.

Step 2 To begin the Cisco Unified Communications Manager Assistant Configuration wizard process, click the **Next** button.

The Partition for Managers window displays.

Step 3 Enter a name in the partition name field and provide a description; otherwise, use the default partition name and description.

Step 4 Click the **Next** button.

The Partition for CTI Route Point window displays.

Step 5 Enter a name in the CTI route point name field and provide a description; otherwise, use the default CTI route point name.

Step 6 Click the **Next** button.

The Partition for All Users window displays.

Step 7 Enter a name in the partition name field and provide a description; otherwise, use the default partition name and description.

Step 8 Click the **Next** button.

The Intercom Partition window displays.

Step 9 Enter a name in the name field and provide a description; otherwise, use the default Intercom Partition name.

Step 10 Click the **Next** button.

The Assistant Calling Search Space window displays.

Step 11 Enter a name in the name field and provide a description; otherwise, 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. If the defaults that are provided are not wanted, the administrator 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 12 Click the **Next** button.

The Everyone Calling Search Space window displays.

Step 13 Enter a name in the name field and provide a description; otherwise, use the default calling search space name and description.

The Available Partitions and Selected Partitions boxes under the Additional Route Partitions for This Calling Search Space automatically list Partitions for the Everyone Calling Search Space. If the defaults that are provided are not wanted, the administrator 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 14 Click the **Next** button.

If you have existing calling search spaces that are configured in the system, the Existing Calling Search Spaces window displays; otherwise, the Existing Calling Search Spaces window does not display (proceed to the next step).

Cisco Unified Communications Manager Assistant requires that 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 15 Click the **Next** button.

The CTI Route Point window displays.

Step 16 Enter a name in the CTI route point name field; otherwise, use the default CTI route point name.

Step 17 From the drop-down selection list box, choose the appropriate device pool.

Step 18 Enter a route point directory number; otherwise, use the default route point directory number.

Step 19 From the drop-down selection list box, choose the appropriate numbering plan.

Step 20 Click the **Next** button.

The Phone Services window displays.

Step 21 Enter the Primary Phone Service Name; otherwise, use the default Phone Service name.

Step 22 From the drop-down list box, choose the Primary Cisco Unified Communications Manager Assistant server or enter a server name or IP address.

Step 23 Enter the Secondary Phone Service Name; otherwise, use the default Phone Service name.

Step 24 From the drop-down list box, choose the secondary Cisco Unified Communications Manager Assistant server or enter a server name or IP address.

Step 25 Click the **Next** button.

The Confirmation window displays. It provides all the information that the administrator chose while using the configuration wizard. If the information is not correct, the administrator can cancel the configuration process or return to the previous configuration windows by pressing the **Back** button.

Step 26 To allow the configuration process to execute, click the **Finish** button; otherwise, to cancel the configuration process, click the **Cancel** button.

Upon completion, a final status window displays. The window shows the success or failure of each part of the wizard.

Any errors that the configuration wizard generates get sent to a trace file. Access this file by using the following CLI command:

```
file get activelog tomcat/logs/ccmadmin/log4j
```

With the data that is collected from the configuration windows, the wizard automatically creates the partitions, calling search spaces, a route point, and the Cisco Unified Communications Manager Assistant phone services. The wizard populates the Cisco IP Manager Assistant service parameters in the Clusterwide Parameters (IPMA Device Configuration Defaults for Proxy Mode) section of the Service Parameters Configuration window. Additionally, the wizard creates the manager phone template, the assistant phone template, and the Everyone phone template that BAT uses to configure phones for use with Cisco Unified Communications Manager Assistant. See the Cisco Unified Communications Manager Bulk Administration Guide for information about configuring the manager and assistant devices.

Calling Search Space and Partitions

A Cisco Unified Communications Manager Assistant route point (called CTI route point) intercepts calls for the managers and determines where to route them; therefore, all calls for the managers should flow through the route point first.

To accomplish the call flow, Cisco Unified Communications Manager Assistant uses calling search spaces. Calls from lines that the Cisco IP Manager Assistant service must route or act upon should have a calling search space that has the route point partition (you can call this partition CTI Route Point) that is configured as the primary partition, and you can call the secondary partition the Everyone partition. See the following example.

Note For a manager who has multiple lines and who uses proxy line support, those lines must fall in the range that is covered by the route point (for example, a route point of 1xxx means that manager lines must fall in 1000 - 1999 range).

Example

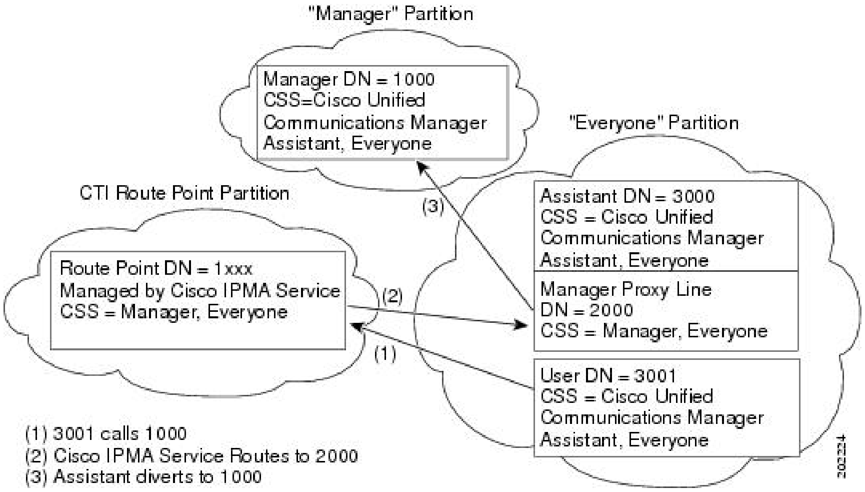
A user (in Everyone partition) places a call to a manager primary line (in Manager partition). Because the partition for the originating call does not include the manager primary line, the manager line number gets searched through the calling search space. The order of priority of the partitions in the calling search space provides basis for the search. Because the user line has a calling search space that comprises CTI Route Point and Everyone, the search for the manager primary line begins with the CTI route point partition. Because the CTI route point matches the manager primary number, the call gets presented to the route point. The Cisco IP Manager Assistant service that is monitoring the route point gets the call and routes the call by using the manager settings.

All lines that have calls that should go through a route point should have a calling search space that is called Cisco Unified Communications Manager Assistant and Everyone. Examples of lines that require this calling search space configuration include manager primary and private lines, assistant primary line, and all other user lines.

All lines that have calls that should go directly to the manager without having the routing logic applied on them should have a calling search space that is called Managers and Everyone. Examples of lines that require this calling search space configuration include Cisco CTI route point and assistant proxy lines.

See the following figure for an example of the calling search space and partition configuration.

Figure 19: Cisco Unified Communications Manager Assistant Calling Search Space and Partition Configuration Example for Proxy Line Support



Configuration Tips

- Create three partitions that are called CTI Route Point, Manager, and Everyone.
- Create a calling search space that is called CSS-M-E, which contains the partitions Manager and Everyone.
- Create a calling search space that is called CSS-I-E, which contains the partitions CTI Route Point and Everyone.
- Configure the manager primary and private directory numbers (DN) in the partition that is called Manager.
- Configure all assistants lines and other users lines in the partition that is called Everyone.
- Configure the Cisco Unified Communications Manager Assistant route point in the partition that is called CTI Route Point.
- Configure the MWI On/Off numbers with a calling search space CSS-M-E.

Cisco Unified Communications Manager Assistant CTI Route Point

You can have only one Cisco Unified Communications Manager Assistant CTI route point for each node. The directory numbers of CTI route points must match the primary and private directory numbers of the manager; otherwise, the Cisco IP Manager Assistant service routes calls inappropriately. Cisco recommends the use of wild cards to satisfy this condition.

When you add directory number ranges for the CTI route point, the caller search space must not contain the Manager partition because Cisco Unified Communications Manager always matches on the most specific match regardless of partition order; for example, the manager line is 1000, and the directory number range that is added to the route point is 1xxx. If a caller search space includes the Manager partition, even when the CTI Route Point partition is at the top, the more specific match applies for the manager directory number, and the call does not get routed by Cisco Unified Communications Manager Assistant but gets sent directly to the manager extension. For Cisco Unified Communications Manager Assistant to route the call when using directory number ranges on the route point, the caller search space must include the CTI Route Point partition but not the Manager partition.

Configuration Tips

- Create a CTI route point that is called Assistant_RP.
- Configure the directory numbers of the route point to match the primary and private directory numbers of the managers (for example, for managers whose primary directory numbers are 1000-1999, create a route point DN as 1xxx for line 1; for managers whose primary directory numbers are 2000-2999, create a route point DN as 2xxx for line 2). Configure the directory numbers in the CTI Route Point partition with a calling search space of CSS-M-E.
- Configure Call Forward No Answer with Destination Internal/External as Route Point DN (for example, CFNA as 1xxx for the Route Point DN 1xxx) with a calling search space of CSS-M-E. Call Forward No Answer forwards the call to the manager if the Cisco IP Manager Assistant service is not available.

Set the Service Parameters for Cisco Unified Communications Manager Assistant

Service parameters for the Cisco IP Manager Assistant service comprise two categories: general and clusterwide. Specify clusterwide parameters once for all Cisco IP Manager Assistant services. Specify general parameters for each Cisco IP Manager Assistant service that is installed.

Set the Cisco IP Manager Assistant service parameters by using Cisco Unified Communications Manager Administration to access the service parameters (**System** > **Service Parameters**). Choose the node where the Cisco Unified Communications Manager Assistant application resides and then choose the Cisco IP Manager Assistant service.

Cisco IP Manager Assistant includes the following service parameters that must be configured:

- Clusterwide
    - Cisco IPMA Server (Primary) IP Address - No default. Administrator must manually enter this IP address. Administrator can assign up to 2500 managers and assistants to this address. To avoid potential high CPU usage, enter the address of the local CTIManager server where the IPMA process is running when you configure the Cisco IP Manager Assistant CTIManager (Primary) IP Address service parameter.
    - Cisco IPMA Server (Backup) IP Address - No default. Administrator must manually enter this IP address.
    - Cisco IPMA Server Port - Default specifies Port 2912.
    - Cisco IPMA Assistant Console Heartbeat Interval - Default specifies 30 seconds. This interval timer specifies how long it takes for the failover to occur on the assistant console.
    - Cisco IPMA Assistant Console Request Timeout - Default specifies 30 seconds.
    - Cisco IPMA RNA Forward Calls - Default specifies False. If the parameter is set to True, an assistant phone that does not get answered will forward to another assistant phone.
    - Cisco IPMA RNA Timeout - Default specifies 10 seconds. RNA timeout specifies how long an assistant phone can go unanswered before the call is forwarded to another assistant phone. If Call Forward No Answer (CFNA) and RNA timeout are both configured, the first timeout occurrence takes precedence.
    - CTIManager Connection Security Flag has the following two options:

Nonsecure - The security mode specifies nonsecure.

Use Cluster Default - Cisco IP Manager Assistant service fetches the security mode for the cluster. If the cluster security mode is detected as mixed, Cisco Unified Communications Manager Assistant will open a secure connection to CTI Manager by using the Application CAPF profile. To make the secure connection succeed, configure both the “CTI Manager Connection Security Flag” and the “CAPF Profile Instance ID for Secure Connection to CTI Manager” parameters.

Use Cluster Default - Cisco IP Manager Assistant service fetches the security mode for the Cisco Unified Communications Manager node. If the Cisco Unified Communications Manager node security mode is detected as mixed, Cisco Unified Communications Manager Assistant will open a secure connection to CTI Manager by using the Application CAPF profile. To make the secure connection succeed, configure both the “CTI Manager Connection Security Flag” and the “CAPF Profile Instance ID for Secure Connection to CTI Manager” parameters.

- Advanced Clusterwide
  - Enable Multiple Active Mode - The default specifies False. When set to True, the administrator can configure up to 7000 managers and assistants by using multiple pools.

    Note Configure unique IP addresses for each pool so that the same Cisco IPMA server IP address does not appear in more than one pool.

  - Pool 2: Cisco IPMA Server (Primary) IP Address - No default. Administrator must manually enter this IP address. Administrator can assign up to 2500 managers and assistants to this address.
  - Pool 2: Cisco IPMA Server (Backup) IP Address - No default. Administrator must manually enter this IP address.
  - Pool 3: Cisco IPMA Server (Primary) IP Address - No default. Administrator must manually enter this IP address. Administrator can assign up to 2500 managers and assistants to this address.
  - Pool 3: Cisco IPMA Server (Backup) IP Address - No default. Administrator must manually enter this IP address.
- Cisco IPMA Service Parameters.
  - CTIManager (Primary) IP Address - No default. Enter the IP address of the primary CTIManager that will be used for call control.
  - CTIManager (Backup) IP Address - No default. Administrator must manually enter this IP address.
  - Route Point Device Name for Proxy Mode - No default. Choose the Cisco Unified Communications Manager Assistant route point device name (that you configure by using **Device** > **CTI Route Point**).
  - 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 Cisco Unified Communications Manager Assistant node will use to open a secure connection to CTIManager. You must configure this parameter if CTIManager Connection Security Flag is enabled.

Note If you change the IPMASecureSysUser password, you must then go to the **IPMASecureSysUser config** > **CAPF Profile config** window for the profile that was selected on the IPMA Service Parameters window, change the Certificate Operation to “Install/Upgrade”, provide the authentication string, and restart the IPMA service.

Cisco Unified Communications Manager Assistant includes the following clusterwide parameters that must be configured if you want to use the Cisco Unified Communications Manager Assistant automatic configuration for managers and assistants:

- Softkey Templates
    - Assistant Softkey Template - Default specifies Standard Assistant softkey template. This parameter specifies the softkey template that is assigned to the assistant device during assistant automatic configuration.
    - Manager Softkey Template for Proxy Mode - Default specifies Standard Manager softkey template. This parameter specifies the softkey template that is assigned to the manager device during manager automatic configuration.
    - Manager Softkey Template for Shared Mode - Default specifies Standard Shared Mode Manager. This service parameter does not apply to proxy line support.
- IPMA Device Configuration Defaults
    - Manager Partition - No default. This parameter specifies the partition that the automatic configuration assigns to the manager line(s) that Cisco Unified Communications Manager Assistant handles on the manager device. Enter a partition that exists in the system. If you run the Cisco Unified Communications Manager Assistant Configuration Wizard, the wizard populates this value.
    - All User Partition - No default. This parameter specifies the partition that the automatic configuration assigns to the proxy line(s) and the intercom line on the assistant device as well as the intercom line on the manager device. Enter a partition that exists in the system. If you run the Cisco Unified Communications Manager Assistant Configuration Wizard, the wizard populates this value.
    - IPMA Calling Search Space - No default. This parameter specifies the calling search space that the automatic configuration assigns to the manager line(s) that Cisco Unified Communications Manager Assistant handles and the intercom line on the manager device as well as the assistant intercom line on the assistant device. Enter a calling search space that exists in the system. If you run the Cisco Unified Communications Manager Assistant Configuration Wizard, the wizard populates this value.
    - Manager Calling Search Space - No default. This parameter specifies the calling search space that the automatic configuration assigns to the proxy line(s) on the assistant device. Enter a calling search space that exists in the system. If you run the Cisco Unified Communications Manager Assistant Configuration Wizard, the wizard populates this value.
    - Cisco IPMA Phone Service - No default. This parameter specifies the IPMA phone service that the automatic configuration assigns to the manager device. If you run the Cisco Unified Communications Manager Assistant Configuration Wizard, the wizard populates this value.

  - IPMA Secondary Phone Service - No default. This parameter specifies a secondary IPMA phone service that the automatic configuration assigns to the manager device if the primary service is not available.

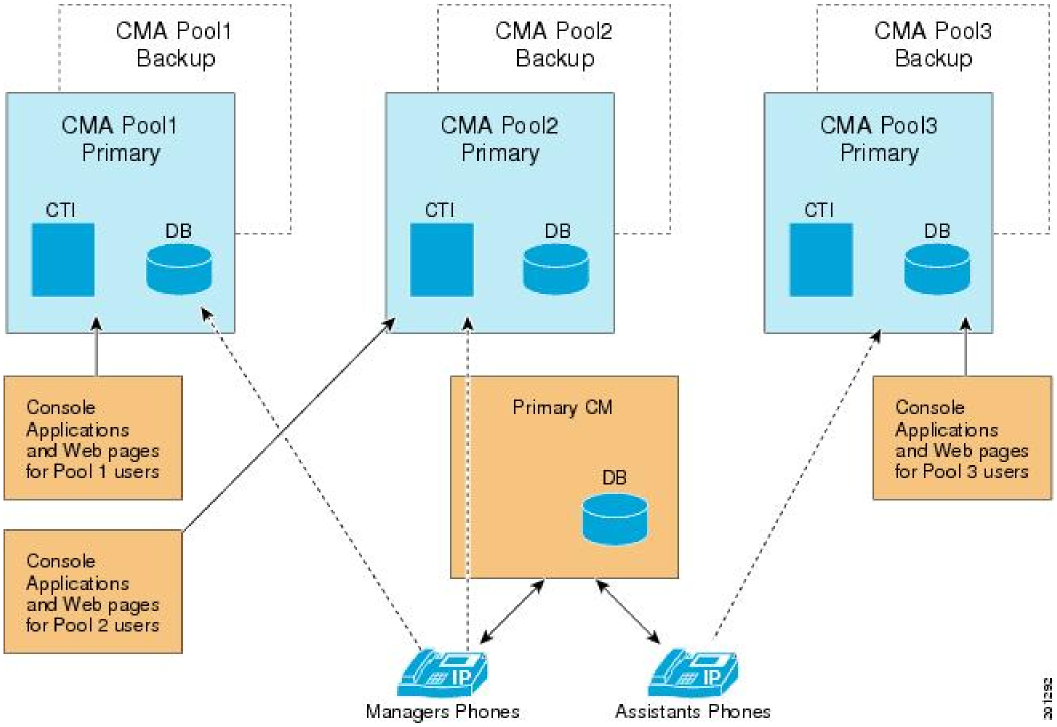
- Proxy Directory Number Range
  - Starting Directory Number - No default. The Starting Directory Number and the Ending Directory Number parameters provide a range of proxy numbers that are available for the assistant configuration. The Starting Directory Number parameter specifies the first directory number in the range. The next available number in the range displays in the Proxy Line field in the End User Configuration window when you are configuring an assistant.
  - Ending Directory Number - No default. The Starting Directory Number and the Ending Directory Number parameters provide a range of proxy numbers that are available for the assistant configuration. The Ending Directory Number parameter specifies the last directory number in the range. If you enter a smaller value in the Ending Directory Number field than you do in the Starting Directory Number field, a message displays when you access the Assistant Configuration in the End User Configuration window.

- Proxy Directory Number Prefix
  - Number of Characters to be Stripped from Manager Directory Number - Default specifies 0. This parameter specifies the number of characters that Cisco Unified Communications Manager strips from a manager directory number (DN) in the process of generating a proxy DN. You can use this parameter along with the Prefix for Manager Directory Number parameter to generate a proxy DN. For example, if you strip 2 digits from a manager DN of 2002 and add a prefix of 30 (specified in the Prefix for Manager Directory Number service parameter), Cisco Unified Communications Manager generates a proxy DN of 3002. You can strip 0 to 24 characters.
  - Prefix for Manager DN - No default. This parameter specifies the prefix that Cisco Unified Communications Manager adds to a manager DN in the process of generating the proxy DN. For example, if manager DN is 1001, number of characters to be stripped is 0, and the prefix is *, Cisco Unified Communications Manager generates a proxy DN of *1001. The maximum prefix length equals 24.

Configure Multiple Servers for Cisco Unified Communications Manager Assistant Scalability

Cisco Unified Communications Manager supports up to 3500 managers and 3500 assistants for a total of 7000 users. To support 7000 users, the administrator must configure multiple active Cisco IP Manager Assistant servers by enabling and setting service parameters. Administrators can configure up to three active Cisco IP Manager Assistant servers, each managing up to 2500 managers and assistants. Each server can also have a backup server. Configure the Cisco IP Manager Assistant servers by using the Advanced Service Parameters, Enable Multiple Active Mode, Pool 2: Cisco IPMA Server, and Pool3: Cisco IPMA Server. See the Set the Service Parameters for Cisco Unified Communications Manager Assistant, on page 325 for more information. See the following figure.

Figure 20: Scalability Architecture



1. Activate IPMA service (see the Install and Activate Cisco Unified Communications Manager Assistant, on page 318)
2. Enable multiple active mode (see the Set the Service Parameters for Cisco Unified Communications Manager Assistant, on page 325)
3. Provide IP addresses for multiple pools (see the Set the Service Parameters for Cisco Unified Communications Manager Assistant, on page 325)
4. Add the pool to the manager/assistant from the End User Configuration window (see the Configure a Manager and Assign an Assistant for Proxy Line Mode, on page 335)

Migration Considerations

If you are migrating from a release previous to Cisco Unified Communications Manager Release 8.0(2), all managers and assistants will get migrated to Pool 1 (the default).

Security Considerations

Cisco Unified Communications Manager Assistant supports a secure connection to CTI (transport layer security connection).

The administrator must configure a CAPF profile (one for each Cisco Unified Communications Manager Assistant node) by choosing **User Management** > **Application User CAPF Profile**. From the Application User drop-down list box that is on the Application User CAPF Profile Configuration window, the administrator chooses **IPMASecureSysUser.**

For more information about configuring security for Cisco Unified Communications Manager Assistant, see the information on the CTIManager Connection Security Flag and the CAPF Profile Instance Id for Secure Connection to CTIManager service parameters in the Set the Service Parameters for Cisco Unified Communications Manager Assistant, on page 325.

The Cisco Unified Communications Manager Security Guide provides detailed security configuration procedures for CTI applications.

Start the Cisco IP Manager Assistant Service

The Cisco IP Manager Assistant service runs as an application on Cisco Tomcat. To start or stop the Cisco IP Manager Assistant service, use the Serviceability Control Center Feature Services window.

Cisco Unified IP Phone Service Configuration

Add the Cisco IP Manager Assistant service as a new Cisco Unified IP Phone Service. Configure a name, description, and the URL for the Cisco IP Manager Assistant service. The name and description that you enter should be in the local language because it displays on the manager Cisco Unified IP Phone. For more information, see the Cisco Unified Communications Manager Administration Guide.

Provide a URL by using the format

http://<server-ipaddress>:8080/ma/servlet/MAService?cmd=doPhoneService&Name=#DEVICENAME#

For example

http://123.45.67.89:8080/ma/servlet/MAService?cmd=doPhoneService&Name=#DEVICENAME#

Configuration Tips

To provide redundancy for the Cisco Unified IP Phone Service, create a Cisco Unified IP Phone Service that uses the host name rather than the IP address. The host name in DNS should resolve to both Cisco Unified Communications Manager Assistant primary and backup IP addresses. The phone functionality for softkeys and filtering, as well as the phone service, will fail over automatically in the case of a failover.

Manager and Assistant Phone Configuration

You must configure devices for each manager and assistant. Before you begin, complete the following tasks, depending on the phone type.

Cisco Unified IP Phone 7940, 7942, 7945, 7960, 7962, 7965, and 7975 (SCCP and SIP)

- Add a Cisco Unified IP Phone 7900 series for each manager and assistant that will be using Cisco Unified Communications Manager Assistant. To add these phones, use one of the following methods:
  - Manually (**Device** > **Phone**)
  - Auto registration
  - BAT
- Assign the Standard Assistant or Standard Manager softkey template.

Cisco Unified IP Phone 7940

You can use the Cisco Unified IP Phone 7940, 7942, or 7945 for Cisco Unified Communications Manager Assistant, but certain restrictions apply.

- Add a Cisco Unified IP Phone 7940, 7942, or 7945 for each manager with the following items configured:
    - Two lines, one for the primary line and one for the intercom
    - Softkey template for manager with shared line support
- Add a Cisco Unified IP Phone 7940 for each assistant with the following items configured:
    - Two lines, one for the primary line and one for the intercom
    - Softkey template for assistant

Note Cisco recommends the Cisco Unified IP Phones 7960, 7962, 7965, and 7975 because they provide more functionality.

Note Cisco Unified IP Phones 7940 and 7960 support only the Cisco Unified Communications Manager Assistant intercom feature.

After you complete these tasks, continue to configure the phones.

Manager Phones

The following section describes the Cisco Unified Communications Manager Assistant requirements and tips for configuring a manager phone.

Manager Phone Configuration

Configure the manager Cisco Unified IP Phones with the following settings:

- Standard Manager softkey template
- Primary line
- Additional lines if required
- Voice-messaging profile on primary line
- If using the Cisco Unified IP Phone 7900 series, except Cisco Unified IP Phone 7940 or 7960, configure the intercom feature
- If using the Cisco Unified IP Phone 7940 or 7960, configure the incoming intercom line to support the auto answer with speakerphone or headset option
- If using the Cisco Unified IP Phone 7940 or 7960, configure the speed dial for outgoing intercom targets
- Subscribe to Cisco Unified IP Phone Service, Assistant Primary Phone Service. If necessary, subscribe to Cisco Unified IP Phone Service, Assistant Secondary Phone Service.

- Set user locale

You can automate some of these settings by choosing the Automatic Configuration check box on the Manager Configuration window when you configure the manager. Automatic Configuration sets the following items for the manager device or device profile:

- Softkey template
- Subscription to Cisco Unified Communications Manager Assistant phone service
- Calling search space and partition for Cisco Unified Communications Manager Assistant-controlled selected lines and intercom line (applies only to Cisco Unified IP Phone7940 and 7960)
- Auto answer with speakerphone for intercom line (applies only to Cisco Unified IP Phone 7940 and 7960)

Before you can automatically configure a manager phone, you must set the Cisco IP Manager Assistant service parameters in the Clusterwide Parameters (IPMA Device Configuration Defaults for Proxy Mode) section. These parameters specify information such as which partition and calling search space to use for a manager line. You can enter these parameters manually, or you can populate the parameters by using the Cisco Unified Communications Manager Assistant Configuration Wizard. For more information about these parameters, see the Set the Service Parameters for Cisco Unified Communications Manager Assistant, on page 325. For more information on the Cisco Unified Communications Manager Assistant Configuration Wizard, see the Cisco Unified Communications Manager Assistant Configuration, on page 320.

After you enter the appropriate service parameters, you can automatically configure a manager phone by choosing the Automatic Configuration check box on the Manager Configuration window and clicking Save. For step-by-step instructions, see the Configure a Manager and Assign an Assistant for Proxy Line Mode, on page 335.

Configuration Tips for Manager

- Do not configure Call Forward All Calls on the manager primary DN because the manager cannot intercept calls that are routed to the assistant proxy DN when Call Forward All Calls is set.
- Configure primary lines (Cisco Unified Communications Manager Assistant-controlled lines) and assign DNs; use the Managers partition and the CSS-I-E calling search space for these lines if you are not using the automatic configuration.
- If the manager is using the Cisco Unified IP Phone 7940 or 7960, configure an incoming intercom line and assign a DN; use the Everyone partition and the CSS-I-E calling search space if you are not using the automatic configuration.
- If the manager is using the Cisco Unified IP Phone 7900 series (except Cisco Unified IP Phone 7940 and 7960) and requires intercom, add the intercom DN and choose the applicable intercom partition and intercom calling search space.

Cisco Unified Communications Manager Assistant supports the Cisco Unified IP Phone 7940, 7942, and 7945. For more information, see the Manager and Assistant Phone Configuration, on page 330.

Assistant Phones

The following section describes the Cisco Unified Communications Manager Assistant requirements and provides tips for configuring an assistant phone.

Assistant Phone Configuration

Configure the assistant Cisco Unified IP Phones with the following settings:

- Standard Assistant softkey template
- Default expansion module (optional)
- Standard Assistant phone button template (if using an expansion module)
- Primary line
- Proxy lines for each configured manager with a voice-mail profile that is the same as the manager voice-mail profile
- Incoming intercom line to support the auto answer with speakerphone or headset option (applies only to Cisco Unified IP Phone 7940 and 7960)
- Speed dial to incoming intercom line for each configured manager (applies only to Cisco Unified IP Phone 7940 and 7960)
- Set user locale
- Subscribe to Cisco Unified IP Phone Service, Assistant Primary Phone Service. If necessary, subscribe to Cisco Unified IP Phone Service, Assistant Secondary Phone Service.

You can automate some settings by choosing the Automatic Configuration check box on the Assistant Configuration window when you configure the assistant. Automatic Configuration sets the following items for the assistant device or device profile:

- Softkey template
- Phone button template
- Calling search space and partition for existing proxy lines and intercom line
- Auto answer with speakerphone for intercom line
- Autogenerated proxy lines creation, if chosen

Before you can automatically configure an assistant phone, you must set the Cisco IP Manager Assistant service parameters in the Clusterwide Parameters (IPMA Device Configuration Defaults for Proxy Mode) section. These parameters specify information such as which partition and calling search space to use for assistant proxy and intercom lines. You can enter these parameters manually, or you can populate the parameters by using the Cisco Unified Communications Manager Assistant Configuration Wizard. For more information about these parameters, see the Set the Service Parameters for Cisco Unified Communications Manager Assistant, on page 325. For more information on the Cisco Unified Communications Manager Assistant Configuration Wizard, see the Cisco Unified Communications Manager Assistant Configuration, on page 320.

After you have entered the appropriate service parameters, you can automatically configure an assistant phone by choosing the Automatic Configuration check box on the Assistant Configuration window. For step-by-step instructions, see the Configure Proxy Incoming Intercom and Primary Lines, on page 338.

Automatic configuration allows you to create a proxy line automatically (with the required calling search space and partition information) on the assistant phone. The autogenerated proxy numbers get generated from the values that you enter for the Proxy Directory Number Range and Proxy Directory Number Prefix service parameters as described in the Set the Service Parameters for Cisco Unified Communications Manager Assistant, on page 325.

Autogenerated numbers appear along with lines on the assistant device in the Proxy Line drop-down list box on the Assistant Configuration window when you configure the assistant. “Line” appears before existing lines on the assistant phone. “Auto” appears before each autogenerated number until the system adds that proxy line to an assistant phone. The system sets the calling search space and partition for the proxy line and the intercom line, if any, on the basis of the Cisco IP Manager Assistant service parameter settings. For step-by-step instructions, see the Configure Proxy Incoming Intercom and Primary Lines, on page 338.

Configuration Tips for Assistant

- If the assistant is using the Cisco Unified IP Phone 7940 or 7960, configure an incoming intercom line and assign a DN; use the Everyone partition and the CSS-I-E calling search space if you are not using the automatic configuration.
- If the assistant is using the Cisco Unified IP Phone 7900 series (except 7940 and 7960) and requires intercom, add the intercom DN and choose the applicable intercom partition and intercom calling search space.
- Configure a proxy line and assign a DN for each manager that the assistant will support; use the Everyone partition and the CSS-M-E calling search space if you are not using the automatic configuration.

Cisco Unified Communications Manager Assistant supports the Cisco Unified IP Phone 7940, 7942, and 7945. For more information, see the Manager and Assistant Phone Configuration, on page 330.

Nonmanager and Nonassistant Phones

In addition to configuring manager and assistant devices, configure all other users in Cisco Unified Communications Manager. Proper configuration allows managers and assistants to make calls to and receive calls from all other users in the system.

Configuration Tips for Nonmanager and Nonassistant

- Use the Everyone partition for all other users.
- Use the CSS-I-E calling search space for all other users.
- If you use auto registration, perform the following tasks:
  - On the Device Pool Configuration window (**System** > **Device Pool**), choose CSS-I-E from the Calling Search Space for Auto-registration field.
  - On the Cisco Unified CM Configuration window (**System** > **Cisco Unified Communications Manager**), choose **Everyone** from the Partition field.
- If you use BAT, you can use the Everyone template that the Cisco Unified Communications Manager Assistant Configuration Wizard created to add phones in the Everyone partition and the CSS-I-E calling search space.

Manager and Assistant Configuration

From the Cisco Unified Communications Manager End User Configuration window, configure the settings for the managers and assistants who use the Cisco Unified Communications Manager Assistant feature. You can configure Cisco Unified Communications Manager Assistant in proxy line or shared line mode.

From the End User Configuration window, perform the following functions:

- Choose manager and assistant devices.
- Automatically configure a manager or assistant device, if you want one.
- Choose the local language in which the End User Configuration window displays.
- Choose the Manager Configuration or Assistant Configuration window to configure the following Cisco Unified Communications Manager Assistant settings:
    - Set up primary and incoming intercom lines for intercom capability. For example, configure extension 3102 as the intercom line for the manager. This line will receive intercom calls from the assistant; for example, the assistant line 1 (1102) and line 2 (1103) display on the assistant console, and the assistant answers them.

      Note The intercom line that you choose will be the one that you created by using the Cisco Unified Communications Manager intercom feature (applicable only to Cisco Unified IP Phones 7942, 7945, 7962, 7965, and 7975) or by using speed dials (applicable only to Cisco Unified IP Phones 7940 and 7960).

    - Configure assistant information for managers.
    - Set up proxy lines for each manager on the assistant phone. For example, assistant lines 4 and 5 take calls from manager lines 1102 and 1103.

Configure a Manager and Assign an Assistant for Proxy Line Mode

Perform the following procedure to configure a manager and assign an assistant to the manager. To configure a new user, see topics related to end user configuration settings in the *Cisco Unified Communications Manager Administration Guide*.

Tip Configure manager information before configuring assistant information.

Procedure

Step 1 To configure the manager and to assign an assistant to an existing user, choose **User Management** > **End User**.

Step 2 To find the user that will be the Cisco Unified Communications Manager Assistant manager, click the **Find** button or enter the user name in the Search Options field and click the **Find** button.

Step 3 To display user information for the chosen manager, click the user name.

The End User Configuration window displays.

Step 4 To configure Cisco Unified Communications Manager Assistant information for the manager, choose Manager Configuration from the Related Links drop-down list box and click **Go**.

Step 5 The Manager Configuration window displays and contains manager information, assistant information, and controlled lines information for the chosen user.

Tip To view existing assistant configuration information, click the assistant name in the Associated Assistants list and click the View Details link. The Assistant Configuration information displays. To return to the manager configuration information, click the manager name in the Associated Managers list and click the View Details link.

Step 6 To associate a device name or device profile with a manager, choose the device name or device profile from the Device Name/Profile drop-down list box. Extension mobility can optionally use device profiles.

Note If the manager telecommutes, click the Mobile Manager check box and optionally choose Device Profile. When Device Profile is chosen, the manager must log on to the phone by using extension mobility before accessing Cisco Unified Communications Manager Assistant.

Step 7 From the Intercom Line drop-down list box, choose the intercom line appearance for the manager, if applicable.

Note The chosen intercom line applies to the Cisco Unified Communications Manager Assistant and Cisco Unified Communications Manager intercom features.

Step 8 From the Assistant Pool drop-down list box, choose the appropriate Pool number (1 to 3).

Step 9 To assign an assistant to the manager, choose an assistant from the Available Assistants list and click the down arrow to move the chosen assistant to the Associated Assistants list.

Step 10 From the Available Lines selection box, choose a line that you want Cisco Unified Communications Manager Assistant to control and click the down arrow to make the line display in the Selected Lines selection box. Configure up to five Cisco Unified Communications Manager Assistant-controlled lines.

To remove a line from the Selected Lines selection box and from Cisco Unified Communications Manager Assistant control, click the up arrow.

Step 11 To automatically configure the softkey template, subscription to the Cisco Unified Communications Manager Assistant phone service, calling search space and partition for Cisco Unified Communications 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, check the Automatic Configuration check box.

Note Automatic Configuration for intercom applies only when using the Cisco Unified Communications Manager Assistant intercom feature for the Cisco Unified IP Phones 7940 and 7960.

Step 12 Click the **Save** button.

The update takes effect immediately.

If you checked the Automatic Configuration check box and the service parameters are invalid, a message displays.

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.

Related Topics

Extension Mobility, on page 315

IPMA Service Restarts

Previously, the IPMA service did not reflect changes that were made in the Unified CM Admin user interface or in the directory until the service got restarted. This was the case for:

- User name changes
- User locale changes
- User ID changes

Each time the IPMA service got restarted, all assistants got logged out.

Because of changes that were made in Cisco Unified Communications Manager, it is not necessary to restart the IPMA service in the above cases.

If a restart does occur, IPMA now preserves the authentication state and availability status of the user.

Delete Cisco Unified Communications Manager Assistant Information From the Manager

Perform the following procedure to delete Cisco Unified Communications Manager Assistant information for a manager. To delete non-Cisco Unified Communications Manager Assistant information for a manager, see topics related to end user configuration settings in the *Cisco Unified Communications Manager Administration Guide*.

Procedure

Step 1 To search for the manager for whom you want to delete Cisco Unified Communications Manager Assistant information, choose **User Management** > **End User** from Cisco Unified Communications Manager Administration.

Step 2 From the Find and List Users window, click the **Find** button or enter the user name in the Search Options field and click the **Find** button.

A list of configured users displays.

Step 3 Choose the manager whose information you want to delete.

Step 4 From the Related Links drop-down list box, click **Manager Configuration**.

The Manager Configuration window displays and contains manager configuration information.

Step 5 Click the **Delete** button.

The update takes effect immediately.

Update the Manager Cisco Unified Communications Manager Assistant Configuration

Perform the following procedure to update Cisco Unified Communications Manager Assistant information for a manager. To update non-Cisco Unified Communications Manager Assistant information for a manager, see the Cisco Unified Communications Manager Administration Guide.

Procedure

Step 1 To search for the manager for whom you want to update Cisco Unified Communications Manager Assistant information, choose **User Management** > **End User** from Cisco Unified Communications Manager Administration.

Step 2 From the Find and List Users window, click the **Find** button or enter the user name in the Search Options field and click the **Find** button.

A list of configured users displays.

Step 3 Choose the manager whose information you want to update.

Step 4 From the Related Links drop-down list box, click **Manager Configuration**.

The Manager Configuration window displays and contains manager configuration information.

Step 5 Update the information that you want changed such as device name, controlled lines, assistant, or intercom line appearance.

Note When the Automatic Configuration check box is checked, the system automatically configures the softkey template, subscription to the Cisco Unified Communications Manager Assistant phone service, calling search space and partition for Cisco Unified Communications 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.

Step 6 Click the **Save** button.

The update takes effect immediately.

Note When non-Cisco Unified Communications Manager Assistant changes such as name, user locale, or PIN are made to a user, the user (manager or assistant) must log out of Cisco Unified Communications Manager Assistant and log in for the changes to occur.

Configure Proxy Incoming Intercom and Primary Lines

Use the Assistant Configuration of the End User Configuration window to configure the following items:

- Device name of the assistant phone
- Intercom line that the assistant uses to answer the incoming intercom call (optional)
- Primary line to make outgoing calls (optional)
- Proxy line of the assistant phone that is associated with the manager, the manager name, and the manager line. For example, the assistant phone line 3 gets used to answer manager Mary Smith phone line 2.

A proxy line specifies a phone line that appears on the assistant Cisco Unified IP Phone. Cisco Unified Communications Manager Assistant uses proxy lines to manage calls that are intended for a manager; for example, manager1. If the call-routing software determines that the call should be presented to the assistant because manager1 cannot accept the call, the call routes to the proxy line that is configured for manager1 on the assistant Cisco Unified IP Phone.

You can manually configure a line on the assistant phone to serve as the proxy line, or you can use automatic configuration to generate a DN and to add the line to the assistant phone.

For information about configuring shared and intercom lines for Cisco Unified Communications Manager Assistant with shared line mode, see the Configure Shared and Incoming Intercom Lines, on page 367.

When you display Cisco Unified Communications Manager Assistant information for the assistant, the system generates DNs on the basis of Cisco IP Manager Assistant service parameter entries in the Proxy Directory Number Range and Proxy Directory Number Prefix sections. For more information about these service parameters, see the Set the Service Parameters for Cisco Unified Communications Manager Assistant, on page 325.

Perform the following procedure to configure the proxy and incoming intercom line appearances for an assistant. To configure a new user, see the Set the Service Parameters for Cisco Unified Communications Manager Assistant, on page 325 section in the Cisco Unified Communications Manager Administration Guide.

Tip Before configuring the Cisco Unified Communications Manager Assistant information for an assistant, you must configure the manager information and assign an assistant to the manager. See Configure a Manager and Assign an Assistant for Proxy Line Mode, on page 335.

Before you begin

If you want to automatically configure the proxy line on the assistant phone, configure the service parameters in the Proxy Directory Number Range and Proxy Directory Number Prefix sections.

Procedure

Step 1 To configure an assistant and assign proxy and incoming intercom lines, choose **User Management** > **End User**.

Step 2 To find the user that will be the assistant, click the **Find** button or enter the user name in the Search Options field and click the **Find** button.

Step 3 To display user information for the chosen assistant, click the user name.

The End User Configuration window displays.

Step 4 To configure Cisco Unified Communications Manager Assistant information for the assistant, choose **Assistant Configuration** from the Related Links drop-down list box and click Go.

The Assistant Configuration window displays.

Step 5 From the Device Name drop-down list box, choose the device name to associate with the assistant.

Step 6 From the Intercom Line drop-down list box, choose the incoming intercom line appearance for the assistant.

Step 7 From the Primary Line drop-down list box, choose the primary line appearance for the assistant.

Step 8 Use the selection boxes in the Manager Association to Assistant Line area to assign and associate manager line numbers to the assistant line numbers.

In the Available Lines selection box, choose the assistant line. The word “Auto” precedes the autogenerated proxy lines. If you want Cisco Unified Communications Manager to create an autogenerated proxy line on the assistant phone, choose an autogenerated proxy line and ensure that the Automatic Configuration check box is checked.

Note The system automatically sets the softkey template as well as the calling search space and partition for existing proxy lines and intercom line on the basis of the Cisco IP Manager Assistant service parameter settings when the Automatic Configuration check box is checked. Additionally, the system sets auto answer with speakerphone for intercom line.

Step 9 In the Manager Names selection box, choose the manager for whom this proxy line will apply.

Step 10 In the Manager Lines selection box, choose the manager line for which this proxy line will apply.

Step 11 Click the **Save** button.

The update takes effect immediately. If you chose automatic configuration, the assistant device automatically resets.

Delete the Cisco Unified Communications Manager Assistant Information

Perform the following procedure to delete Cisco Unified Communications Manager Assistant information for an assistant. To delete non-Cisco Unified Communications Manager Assistant information for an assistant, see the Cisco Unified Communications Manager Administration Guide.

Procedure

Step 1 To search for the assistant for whom you want to delete Cisco Unified Communications Manager Assistant information, choose **User Management** > **End User** from Cisco Unified Communications Manager Administration.

Step 2 From the Find and List Users window, click the **Find** button or enter the user name in the Search Options field and click the **Find** button.

A list of configured users displays.

Step 3 Choose the assistant whose information you want to delete.

Step 4 From the Related Links drop-down list box, click **Assistant Configuration**.

The Assistant Configuration window displays.

Step 5 Click the **Delete** button.

The update takes effect immediately.

Note When non-Cisco Unified Communications Manager Assistant changes such as name, user locale, or PIN, are made to a user, the user (manager or assistant) must log out of Cisco Unified Communications Manager Assistant and log in before the changes occur.

Update the Cisco Unified Communications Manager Assistant Configuration

Perform the following procedure to update Cisco Unified Communications Manager Assistant information for an assistant. To update non-Cisco Unified Communications Manager Assistant information for an assistant, see the Cisco Unified Communications Manager Administration Guide.

Procedure

Step 1 To search for the assistant for whom you want to update information, choose **User Management** > **End User** from Cisco Unified Communications Manager Administration.

Step 2 From the Find and List Users window, click the **Find** button or enter the user name in the Search Options field and click the **Find** button.

A list of configured users displays.

Step 3 Choose the assistant whose information you want to update.

Step 4 From the Related Links drop-down list box, click **Assistant Configuration**.

The Assistant Configuration window displays.

Step 5 Update the information such as device name, intercom line, or manager association information that you want changed.

Note The system automatically configures the softkey template, subscription to the Cisco Unified Communications Manager Assistant phone service, calling search space and partition for Cisco Unified Communications 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 when the Automatic Configuration check box is checked.

Step 6 Click the **Save** button.

The update takes effect immediately.

Note When non-Cisco Unified Communications Manager Assistant changes such as name, user locale, or PIN, are made to a user, the user (manager or assistant) must log out of Cisco Unified Communications Manager Assistant and log in before the changes can occur.

Dial Rules Configuration

The administrator uses dial rules configuration to add and sort the priority of dialing rules. Dial rules for Cisco Unified Communications Manager Assistant automatically strip numbers from or add numbers to telephone numbers that the assistant dials from the directory search window in the Assistant Console. For example, a dial rule can automatically add the digit 9 in front of a 7-digit telephone number to provide access to an outside line.

The Cisco Unified Communications Manager System Guide provides additional information on application dial rules.

Provide Information to Cisco Unified Communications Manager Assistant Managers and Assistants

Install the assistant console application for Cisco Unified Communications Manager Assistant by accessing a URL. The administrator sends the URL, in the Install the Assistant Console Plug-In, on page 342, to the assistant.

Note The assistant console application installation program supports Microsoft Internet Explorer 7, Internet Explorer 8, FireFox 3.x and Safari 4.x.

Install the Assistant Console Plug-In

The assistant console plug-in installation supports Internet Explorer 7, FireFox 3.x and Safari 4.x. You can install the application on a PC that runs Windows 7, Windows XP, Windows Vista or Apple MAC OS X.

Note If you use Cisco Unified Communications Manager release 8.5(1) or earlier and want to install the assistant console on a Windows 7 operating system, you must download a new plug-in installer from Cisco.com that supports Windows 7. The plug-in that is available for previous versions of Cisco Unified Communications Manager does not support Windows 7.

Note In addition, if you are upgrading the assistant console you must uninstall the previous version to proceed with the new installation. The new plug-in detects any older version of assistant console (which uses the previous plug-in) and displays an alert message to uninstall the previous version before performing the upgrade.

A previous 5.x or 6.x version of the assistant console application works with Cisco Unified Communications Manager 7.1, but if you decide to install the 7.1 plug-in, you must uninstall the previous 5.x or 6.x version of the assistant console application before you install the plug-in.

Previous versions of the assistant console application do not work with Windows Vista. If the PC runs Windows Vista, install the plug-in.

After you upgrade from Cisco Unified CallManager Release 4.x to Cisco Unified Communications Manager 7.1, you must install the assistant console plug-in. Before you install the plug-in, uninstall the 4.x version of the assistant console application.

To uninstall previous versions of the assistant console application (6.0(1), 4.x, or any 5.x version before 5.1(3)), choose Start> ...Programs > Cisco Unified CallManager Assistant > Uninstall Assistant Console.

To uninstall a 5.1(3) or 6.1(x) assistant console application, go to the Control Panel and remove it.

Tip The assistant console application requires that JRE1.4.2_05 exist in C:\Program Files\Cisco\Cisco Unified Communications Manager.

To install the assistant console application, perform the following procedure:

Procedure

Step 1 From the PC where you want to install the assistant console application, browse to Cisco Unified Communications Manager Administration and choose **Application** > **Plugins**.

Step 2 For the Cisco Unified Communications Manager Assistant plug-in, click the Download link; save the executable to a location that you will remember.

Step 3 Locate the executable and run it.

Tip If you install the application on a Windows Vista PC, a security window may display. Allow the installation to continue.

The installation wizard displays.

Step 4 In the Welcome window, click **Next.**

Step 5 Accept the license agreement and click **Next.**

Step 6 Choose the location where you want the application to install. After you choose the location for the installation, click **Next.**

Tip By default, the application installs in C:\Program Files\Cisco\ Unified Communications Manager Assistant Console.

Step 7 To install the application, click **Next.**

The installation begins.

Step 8 After the installation completes, click **Finish.**

Tip To launch the assistant console, click the desktop icon or choose **Cisco Unified Communications Manager Assistant** > **Assistant Console** in the Start...Programs menu.

Tip Before the assistant logs in to the console, give the assistant the port number and the IP address or hostname of the Cisco Unified Communications Manager server where the Cisco IP Manager Assistant service is activated. 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.

Tip Before the assistant logs in to the console, give the assistant the user name and password that is required to log in to the console.

Tip The Advanced tab in the Cisco Unified Communications Manager Assistant Settings window allows you to enable trace for the assistant console.

Assistant Console Dialog Options

The assistant console displays a dialog that contains the following options:

- Location to Install - The path of the directory where the assistant console software gets installed. The default specifies following path:

  c:\Program Files\Cisco\Cisco Unified Communications Manager Assistant Console

- Create Desktop Shortcut - Default specifies true. This parameter determines whether a shortcut is created on the assistant console.
- Create StartMenu Shortcut - Default specifies true. This parameter determines whether a shortcut is created in the Start menu (**Start** > **Programs** > **Cisco Unified Communications Manager Assistant** > **Assistant Console**).
- Install JRE - Default specifies true. This parameter determines whether JRE is installed along with assistant console. If this option is turned off, the following configuration must exist on the assistant console:
  - Install JRE 1.4.2_05 (international version) on the assistant console.

- Create an environment variable - Assistant_JRE on the assistant console, which gives the path to the JRE; for example, c:\Program Files\Jave\j2re1.4.2_05.

Manager Configuration

Managers can customize their feature preferences from the Manager Configuration window by using the following URL:

```
https://<Cisco Unified Communications Manager Assistant
node>:8443/ma/desktop/maLogin.jsp
```

where

Cisco Unified Communications Manager Assistant node specifies the IP address of the node on which the Cisco IP Manager Assistant service is running.

The administrator must send this URL to the manager.

CHAPTER 13

Cisco Unified Communications Manager Assistant with Shared Line Support

This chapter provides information about Cisco Unified Communications Manager Assistant feature which enables managers and their assistants to work together more effectively. Cisco Unified Communications Manager Assistant supports two modes of operation: proxy line support and shared line support. The Cisco IP Manager Assistant service supports both proxy line and shared line support simultaneously.

The feature comprises enhancements to phone capabilities for the manager and the assistant console application that are primarily used by the assistant.

Cisco Unified Communications Manager Assistant supports up to 3500 managers and 3500 assistants. To accommodate this number of users, the administrator configures up to three Cisco Unified Communications Manager Assistant applications in one Cisco Unified Communications Manager cluster and assigns managers and assistants to each instance of the application.

Cisco Unified Communications Manager users comprise managers and assistants. An assistant user handles calls on behalf of a manager. Cisco Unified Communications Manager Assistant comprises features for managers and features for assistants.

Configure Cisco Unified Communications Manager Assistant with Shared Line Support

Cisco Unified Communications Manager Assistant, a plug-in that allows an assistant to handle calls on behalf of a manager, intercepts manager calls and routes them appropriately. If you configure Cisco Unified Communications 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 rings.

The Cisco Unified Communications 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. The assistant phone does not have the softkey for the divert all feature. The manager phone does not have the softkeys for assistant watch, call intercept, or divert all feature.

Perform the following steps to configure the Cisco Unified Communications Manager Assistant with shared line support.

Procedure

Step 1 If you have not already done so, configure the phones and users and associate the devices to the users. Additionally, for shared line appearances between managers and assistants, configure the same directory number on the manager primary line and assistant secondary line, if you have not already done so.

Step 2 In Cisco Unified Serviceability, activate the Cisco IP Manager Assistant service in the Service Activation window.

Step 3 Configure Cisco IP Manager Assistant service parameters for shared line support.

Step 4 If using the Cisco Unified Communications Manager intercom feature, add the Intercom partition, Intercom calling search space, Intercom directory number, and the Intercom translation pattern.

Step 5 If multiple Cisco Unified Communications Manager Assistant pools are required to support large numbers of assistants and managers, configure the following Cisco IP Manager Assistant clusterwide service parameters:

- Enable Multiple Active Mode
- Pool 2 and Pool 3 Cisco IPMA Server IP Address

Step 6 Configure the application user CAPF profile (optional).

Step 7 Configure Cisco IP Manager Assistant service parameters for security (optional).

Step 8 Using the Serviceability Control Center Feature Services, stop and start the Cisco IP Manager Assistant service.

Step 9 Add the appropriate Cisco Unified IP Phone phone button template.

Step 10 Configure manager and assistant Cisco Unified IP Phone parameters:

- Set up manager phone.
- Set up assistant phone.

Step 11 Configure manager phone settings:

- Assign the softkey template for shared line mode.
- If using Do Not Disturb, configure the Do Not Disturb fields on the manager phone.
- Add primary lines. (Use the same DN and partition for the assistant secondary line DN.)
- Set up voice-mail profile on primary line.
- Add incoming intercom line (optional).
- For Cisco Unified IP Phones 7940 and 7960, add speed dial for outgoing intercom targets.
- For Cisco Unified IP Phones 7942, 7945, 7962, 7965, and 7975 add the intercom capabilities.
- Set user locale.
- Reset the phone.

Tip To automatically configure some manager phone settings, choose the automatic configuration check box on the Manager Configuration window when you are configuring the manager. For more information, see the Manager Phones, on page 362.

Step 12 Configure assistant phone settings:

- Assign a softkey template.
- Add an expansion module (optional).
- Assign the phone button template.
- Add a primary line.
- Add shared lines for each configured manager. (Use the same DN and partition for the assistant secondary line and manager primary line.)
- Add incoming intercom line (optional).
- For Cisco Unified IP Phones 7940 and 7960, add speed dial for outgoing intercom targets.
- For Cisco Unified IP Phones 7942, 7945, 7962, 7965, and 7975, add the intercom capabilities.
- Set user locale.
- Reset the phone.

Tip To automatically configure some assistant phone settings, choose the Automatic Configuration check box on the Assistant Configuration window when you are configuring the assistant. For more information, see the Assistant Phones, on page 363.

Step 13 Configure Cisco Unified Communications Manager Assistant:

- Create a new manager.
- Configure shared lines for manager.
- Assign an assistant to a manager.
- Configure lines for the assistant.
- Configure intercom lines (optional)

Step 14 Configure the dial rules for the assistant.

Step 15 Install the Assistant Console application.

Step 16 Configure the manager and assistant console applications.

Related Topics

Set the Service Parameters for Cisco Unified Communications Manager Assistant, on page 357

Intercom, on page 685

Configure Shared and Incoming Intercom Lines, on page 367

Configure Multiple Servers for Cisco Unified Communications Manager Assistant Scalability, on page 360

Security Considerations, on page 361

Starting the Cisco IP Manager Assistant Service, on page 361

Manager and Assistant Phone Configuration, on page 361

Do Not Disturb, on page 413

Configure a Manager and Assign an Assistant for Shared Line Mode, on page 364

Install the Assistant Console Plug-In, on page 370

Cisco Unified Communications Manager Assistant Feature

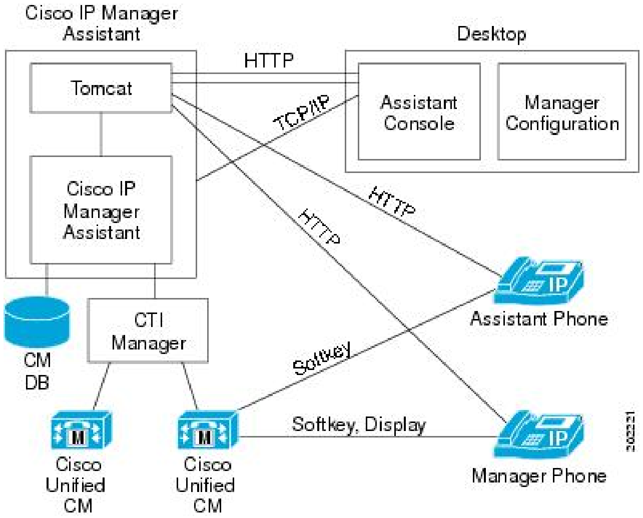
Cisco Unified Communications Manager Assistant, a plug-in that allows an assistant to handle calls on behalf of a manager, intercepts manager calls and routes them appropriately. If you configure Cisco Unified Communications Manager Assistant in shared-line mode, the manager and assistant share a directory 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 rings.

The Cisco Unified Communications 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. The assistant phone does not have the softkey for the divert all feature. The manager phone does not have the softkeys for assistant watch, call intercept, or divert all feature.

Cisco Unified Communications Manager Assistant Overview

The Cisco Unified Communications Manager Assistant feature architecture comprises the Cisco IP Manager Assistant service, the assistant console application, and the Cisco Unified IP Phone interfaces. See the following figure.

Figure 21: Cisco Unified Communications Manager Assistant Architecture



Cisco IP Manager Assistant Service

Cisco Tomcat loads the Cisco IP Manager Assistant service, a servlet. Cisco Tomcat gets installed at Cisco Unified Communications Manager installation.

The Cisco IP Manager Assistant service gets installed on the Cisco Unified Communications Manager node. After installation, the administrator activates the service from Serviceability, which automatically starts Cisco Unified Communications Manager Assistant. The Cisco IP Manager Assistant service checks to see whether it is one of the Cisco Unified Communications Manager Assistant nodes that is configured in the clusterwide service parameter, Cisco IPMA Server (Primary) IP Address. If it is, the Cisco IP Manager Assistant service attempts to become the active Cisco IP Manager Assistant service. Currently, Cisco Unified Communications Manager supports only one active Cisco IP Manager Assistant service.

The Cisco IP Manager Assistant service performs the following tasks:

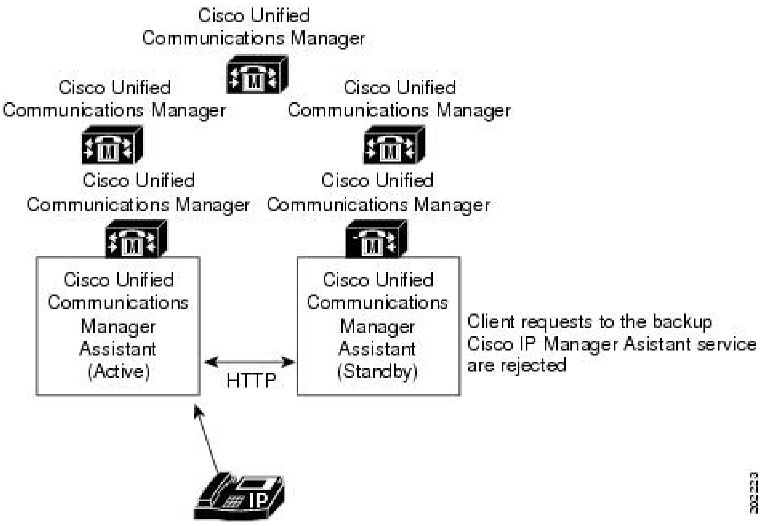
- Hosts the HTTP services that run on the manager phone.
- Hosts the web pages that the manager uses for configuration.
- Communicates to Cisco Unified Communications Manager through the Cisco CTIManager for third-party call control. Cisco Unified Communications Manager Assistant requires only one CTI connection.
- Accesses data from the database.
- Supports the Assistant Console application.

Cisco Unified Communications Manager supports redundancy of the Cisco IP Manager Assistant service. To achieve redundancy, you must configure a second Cisco IP Manager Assistant service in the same cluster.

Cisco Unified Communications Manager Assistant implements redundancy by using an active/standby node model. At any time, only one Cisco Unified Communications Manager Assistant node remains active and servicing all assistant console applications and phones. The other node stays in a standby mode and will detect failures on the active node. When the backup node detects a failure, it takes over and becomes the active node. All connections that were active get restored on the new node, and service continues uninterrupted to the users.

If the active node fails, the Assistant Console application fails over automatically to the backup node. The Cisco IPMA Assistant Console Heartbeat Interval service parameter (see the Set the Service Parameters for Cisco Unified Communications Manager Assistant, on page 357) determines the time that the application takes to detect failure. A shorter heartbeat interval leads to faster failover. See The following figure.

Figure 22: Cisco Unified Communications Manager Assistant Redundancy


Cisco Unified Communications Manager
Cisco Unified Communications Manager
Cisco Unified Communications Manager
Cisco Unified Communications Manager
Cisco Unified Communications Manager
Cisco Unified Communications Manager Assistant (Active)
HTTP
Cisco Unified Communications Manager Assistant (Standby)
Client requests to the backup Cisco IP Manager Asistant service are rejected
IP
202223

The Cisco IP Manager Assistant service includes built-in security to help prevent unauthorized access to its services. The user ID and password that are collected at the assistant console get encrypted before they are sent over the network. The Assistant Console blocks nonauthorized users who are posing as assistants.

Assistant Console Interface

Cisco Unified Communications Manager Assistant supports the following assistant console interfaces for managers and assistants:

- Assistant Console (used for call control, log on, assistant preferences, monitoring managers call activity, keyboard shortcuts)
- Manager configuration (used for configuring the immediate divert target)

Administrators use Cisco Unified Communications Manager Administration, End User Configuration, to configure Cisco Unified Communications Manager Assistant for managers and assistants. See Cisco Unified Communications Manager Assistant Administration Interface, on page 351.

Cisco Unified Communications Manager makes the Cisco Unified Communications Manager Assistant manager features available through the Cisco Unified IP Phone. Use a browser to access Manager configuration. Assistants use the Cisco Unified IP Phone and the assistant console application. See Manager Interfaces, on page 350 and Assistant Interfaces, on page 351.

For more information about how to use the assistant console features, see the Cisco Unified Communications Manager Assistant User Guide.

Cisco Unified IP Phone Interface

Assistants and managers use softkeys to access Cisco Unified Communications Manager Assistant features. For more information about how to use the Cisco Unified Communications Manager Assistant phone features, see the Cisco Unified Communications Manager Assistant User Guide.

See Manager Interfaces, on page 350 and Assistant Interfaces, on page 351.

Cisco Unified Communications Manager Assistant Database Access Architecture

The database stores all Cisco Unified Communications 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.

Manager Interfaces

The manager phone makes available the manager features with the exception of Manager Configuration. Cisco Unified Communications Manager Assistant automatically logs a manager into the Cisco IP Manager Assistant service when the Cisco IP Manager Assistant service starts.

The manager accesses the Cisco Unified Communications Manager Assistant features Assistant Watch, Intercept Call, and Transfer to Voice Mail from the Cisco Unified IP Phone softkeys.

Note Managers also have access to Cisco Unified Communications Manager features such as Do Not Disturb and i-Divert.

The state of the Do Not Disturb feature displays in the Status Window on the Cisco Unified IP Phone.

See the Cisco Unified Communications Manager Assistant User Guide for more information.

Assistant Interfaces

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, an application, provides call-control functions such as answer, divert, transfer, and hold. The assistant uses the Assistant Console to log on and log off, to set up assistant preferences, and to display the manager configuration window that is used to configure manager preferences.

The Assistant Console displays the assistant lines and the manager shared lines. Assistants access the shared lines to manage calls that are intended for a manager.

You can access Intercom and Distinctive Ringing on the assistant Cisco Unified IP Phone. When the assistant logs in from the Assistant Console, the softkeys Redirect and Transfer to Voice Mail become active for the shared lines. See the Cisco Unified Communications Manager Assistant User Guide for more information.

Softkeys

The Cisco Unified Communications Manager Assistant feature supports softkeys such as Redirect, Transfer to Voice Mail, and Do Not Disturb on the Cisco Unified IP Phone. Softkeys only appear in their appropriate call state; for example, Transfer to Voice Mail does not appear if no active calls exist.

Cisco Unified Communications 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

Additionally, the system makes call-processing (such as hold and dial) softkeys available with the Standard User template. The administrator configures the appropriate softkey template for the devices that managers and assistants use.

Note The default process assigns call-processing softkey templates to devices.

Administrators can create custom softkey templates in addition to using the standard softkey templates that are included in Cisco Unified Communications Manager. Use Softkey Template configuration in Cisco Unified Communications Manager Administration to associate softkey templates with Cisco Unified Communications Manager Assistant devices and to create custom softkey templates. See Assistant Interfaces, on page 351 in the Cisco Unified Communications Manager Administration Guide.

Cisco Unified Communications Manager Assistant Administration Interface

The administrator uses the End User Configuration window of Cisco Unified Communications Manager Administration to configure the manager and assistant. The administrator chooses the device for the manager and assistant and optionally chooses an intercom line for the manager and assistant. The administrator sets up the shared line for the manager, which gets configured for the assistant.

See the Manager and Assistant Configuration, on page 363.

System Requirements for Cisco Unified Communications Manager Assistant with Shared Line Support

Cisco Unified Communications Manager Assistant with shared line support requires the following software components to operate:

- Cisco Unified Communications Manager
- Supported Browsers and platform:
  - Cisco Unified Communications Manager Assistant administration (using Cisco Unified Communications Manager Administration) and the Assistant Console are supported on Microsoft Internet Explorer (IE) 5.5 or later, Firefox 3.x or later, and Safari 4.x or later. (See the Interactions and Restrictions, on page 353 for more information.).
  - On a computer running Microsoft Windows 2000 or later, a customer can open one of the browsers specified above.
    - Cisco Unified Communications Manager Bulk Administration Tool (BAT) if bulk adding of managers and assistants is planned.

Because Cisco Unified Communications Manager Assistant installs automatically on the same server with Cisco Unified Communications Manager, an additional server is not required.

To determine which Cisco Unified IP Phones support Cisco Unified Communications Manager Assistant, see the Determine Device Support for Cisco Unified Communications Manager Assistant, on page 352.

Determine Device Support for Cisco Unified Communications Manager Assistant

Use the Cisco Unified Reporting application to generate a complete list of IP Phones that support Cisco Unified Communications Manager Assistant. To do so, follow these steps:

1. Start Cisco Unified Reporting by using any of the methods that follow.

   The system uses the Cisco Tomcat service to authenticate users before allowing access to the web application. You can access the application

   - by choosing Cisco Unified Reporting in the Navigation menu in Cisco Unified Communications Manager Administration and clicking **Go.**
   - by choosing **File** > **Cisco Unified Reporting** at the Cisco Unified Real Time Monitoring Tool (RTMT) menu.
   - by entering `https://<server name or IP address>:8443/cucreports/` and then entering your authorized username and password.

2. Click System Reports in the navigation bar.
3. In the list of reports that displays in the left column, click the **Unified CM Phone Feature List** option.

4. Click the Generate a new report link to generate a new report, or click the **Unified CM Phone Feature List** link if a report already exists.
5. To generate a report of all IP Phones that support Cisco Unified Communications Manager Assistant, choose these settings from the respective drop-down list boxes and click the **Submit** button:

   Product: All

   Feature: IPMA

   The List Features pane displays a list of all devices that support the Cisco Unified Communications Manager Assistant feature. You can click on the Up and Down arrows next to the column headers (Product or Protocol) to sort the list.

For additional information about the Cisco Unified Reporting application, see the *Cisco Unified Reporting Administration Guide*.

Interactions and Restrictions

This section describes the interactions and restrictions for Cisco Unified Communications Manager Assistant.

Interactions

This section describes how Cisco Unified Communications Manager Assistant interacts with Cisco Unified Communications Manager applications.

Bulk Administration Tool

The administrator can use the Bulk Administration Tool (BAT) to add many users (managers and assistants) at once instead of adding users individually. See the Cisco Unified Communications Manager Bulk Administration Guide for more information.

The BAT templates that the Cisco Unified Communications Manager Assistant Configuration Wizard creates for Cisco Unified IP Phones support only the Cisco Unified Communications Manager intercom lines.

Calling Party Normalization

Cisco Unified Communications Manager Assistantautomatically supports localized and globalized calls if you configure the calling party normalization feature. Cisco Unified Communications Manager Assistant can display localized calling party numbers on the user interfaces. In addition, for an incoming call to the manager, Cisco Unified Communications Manager Assistant can display localized and globalized calling party numbers when filter pattern matching occurs. For information on configuring calling party normalization, see the Calling Party Normalization, on page 193.

Extension Mobility

A manager who uses the Cisco Extension Mobility feature can simultaneously use Cisco Unified Communications Manager Assistant. The manager logs into the Cisco Unified IP Phone by using extension mobility, and Cisco IP Manager Assistant service automatically gets enabled on that phone. The manager can then access the Cisco Unified Communications Manager Assistant features.

To have access to Cisco Extension Mobility with Cisco Unified Communications Manager Assistant, the administrator checks the Mobile Manager check box in the Manager Configuration window in Cisco Unified

Communications Manager Administration (accessed from the End User Configuration window). See the Configure a Manager and Assign an Assistant for Shared Line Mode, on page 364. For more information about configuring device profiles, see the Cisco Unified Communications Manager Administration Guide. For more information about Cisco Extension Mobility, see Extension Mobility, on page 463

Internet Protocol Version 6 (IPv6)

Cisco Unified Communications Manager Assistant does not support IPv6, so you cannot use phones with an IP Addressing Mode of IPv6 Only with Cisco Unified Communications Manager Assistant. If you want to use Cisco Unified Communications Manager Assistant with the phone, make sure that you configure the phone with an IP Addressing Mode of IPv4 Only or IPv4 and IPv6. For more information on IPv6, see the Internet Protocol Version 6 (IPv6), on page 739.

Reporting Tools

Cisco Unified Communications 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 following sections describe these reporting tools.

CDR Analysis and Reporting

Cisco Unified Communications Manager Assistant supports call-completion statistics for managers and assistants and inventory reporting for managers and assistants. The CDR Analysis and Reporting (CAR) tool supports call-completion statistics. Cisco Unified Serviceability supports inventory reporting. See the Cisco Unified Communications Manager System Guide, the Cisco Unified Serviceability Administration Guide, and the Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide for more information.

Unified CM AssistantChangeLog*.txt

The administrator can view a summary of changes that are made to the Manager or Assistant Configurations. A manager can change defaults by accessing the Manager Configuration from a URL.

An assistant can change the manager defaults from the Assistant Console.

Note See the Cisco Unified Communications Manager Assistant User Guide for information about the URL and Manager Configuration.

When changes are made, the information gets sent to a log file that is 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/
```

The administrator can download this file from the server by using the Trace Collection Tool in the Cisco Unified Real Time Monitoring Tool (RTMT). See the Cisco Unified Real Time Monitoring Tool Administration Guide for more information.

The log file contains the following fields:

- LineNumber - The line in the log file with information about changes
- TimeStamp - The time that the configuration changed
- for Manager/Assistant - Designation of whether the change is for the manager or the assistant
- for Userid - The userid of the manager or assistant that is being changed

- by Manager/Assistant - Designation of whether the change was made by the manager or the assistant
- by Userid - The userid of the manager or assistant who made the change
- Parameter Name - What changed; for example, divert target number
- Old Value - The value of the information before the change
- New Value - The value of the information after the change

Because the information in the log file is comma delimited, the administrator can open the log file by using a spreadsheet application such as Microsoft Excel. Use the following procedure to save the log file contents to the Microsoft Excel application.

Procedure

Step 1 Start the Microsoft Excel application.

Step 2 Choose **File** > **Open** to open the Unified CM Assistant.txt file.

Step 3 Choose the Original data type, file type as Delimited and click **Next.**

Step 4 Choose Delimiters as Comma and click **Next.**

Step 5 When complete, click **Finish.**

Multilevel Precedence and Preemption (MLPP)

The following points describe the interactions between Cisco Unified Communications Manager Assistant with shared line support and MLPP:

- The system preserves call precedence in the handling of calls by Cisco Unified Communications Manager Assistant. For example, when an assistant diverts a call, the system preserves the precedence of the call.
- Because Cisco Unified Communications Manager Assistant does not have knowledge of the precedence of a call, it does not provide any additional indication of the precedence of a call on the assistant console.

Intercom

Cisco Unified Communications Manager Assistant supports the following two types of intercom:

- Cisco Unified Communications Manager Assistant intercom (used with Cisco Unified IP Phones 7940 and 7960). This intercom feature gets configured by using the DN configuration and end user (manager and assistant) configuration windows.
- Cisco Unified Communications Manager intercom (used with Cisco Unified IP Phones 7942, 7945, 7962, 7965, 7975). This intercom feature gets configured by using the intercom partition, intercom calling search space, intercom directory number, intercom translation pattern, DN, and end user (manager and assistant) configuration windows.

Restrictions

The following restrictions apply to Cisco Unified Communications Manager Assistant:

- Cisco Unified Communications Manager Assistant supports SIP on Cisco Unified IP Phones 7900 series except the Cisco Unified IP Phone 7940 and 7960.

- Cisco Unified Communications Manager Assistant supports up to 3500 managers and 3500 assistants by configuring multiple Cisco IP Manager Assistant servers (pools). When multiple pools are enabled, a manager and all configured assistants for that manager should belong to the same pool.
- One manager can have up to 10 assigned assistants.
- One assistant can support up to 33 managers (if each manager has one Cisco Unified Communications Manager-controlled line).
- Only one assistant at a time can assist a manager.
- Cisco Unified Communications Manager Assistant supports up to 3500 managers and 3500 assistants per Cisco Unified Communications Manager cluster when you are using the MCS 7845 server.
- Cisco Unified Communications Manager Assistant is not supported in the single sign on environment.
- The Assistant Console does not support hunt groups/queues.
- The Assistant Console does not support record and monitoring.
- The Assistant Console does not support on-hook transfer (the ability to transfer a call by pressing the Transfer softkey and going on hook to complete the transfer).
- The Assistant Console does not support the one-touch Call Pickup feature.
- Cisco Unified IP Phones 7940, 7942, and 7945 support only two lines or speed-dial buttons.
- When an upgrade to Cisco Unified Communications Manager Release 8.0(2) (or higher) occurs, existing Cisco Unified Communications Manager Assistant users that use the incoming intercom line do not get upgraded automatically to the Cisco Unified Communications Manager Intercom feature.
- The system does not support calls between the Cisco Unified Communications Manager Intercom feature and regular lines (which may be configured as Cisco Unified Communications Manager Assistant Intercom lines).
- Cisco Unified IP Phones 7960 and 7940 support only the Cisco Unified Communications Manager Assistant Intercom lines feature. Cisco Unified IP Phones 7900 (except 7940 and 7960) support only the Cisco Unified Communications Manager intercom feature.
- To install the Assistant Console application on a computer with Microsoft Internet Explorer 7 (or later) on Windows XP, install the Microsoft Java Virtual Machine (JVM) with Windows XP Service Pack 1 before the Assistant Console installation.

Install and Activate Cisco Unified Communications Manager Assistant

Cisco Tomcat loads the Cisco Unified Communications Manager Assistant, a servlet. Cisco Tomcat gets installed and started at Cisco Unified Communications Manager installation. For more information, see the Cisco IP Manager Assistant Service, on page 348.

The administrator performs the following three steps after installation to make Cisco Unified Communications Manager Assistant available for system use:

1. Use Cisco Unified Serviceability Service Activation, located on the Tools menu, to activate the Cisco IP Manager Assistant service. See the Cisco Unified Serviceability Administration Guide.

2. Configure the applicable service parameters for the Cisco IP Manager Assistant service. See the Set the Service Parameters for Cisco Unified Communications Manager Assistant, on page 357.

3. Use Serviceability Control Center Feature Service to stop and start the Cisco IP Manager Assistant service. See the Starting the Cisco IP Manager Assistant Service, on page 361.

Note If the managers and assistants will require Cisco Unified Communications Manager Assistant features to display (on the phone and assistant console) in any language other than English, verify that the locale installer is installed before configuring Cisco Unified Communications Manager Assistant. See the Cisco Unified Communications Operating System Administration Guide.

Cisco Unified Communications Manager Assistant with Shared Line Support Configuration

For successful configuration of Cisco Unified Communications Manager Assistant, review the steps in the configuration checklist, perform the user and device configuration requirements, and configure the managers and assistants.

Note Cisco Unified Communications Manager Assistant with shared line support coexists in the same Cisco Unified Communications Manager system with Cisco Unified Communications Manager Assistant with proxy line support.

Tip Before you configure Cisco Unified Communications Manager Assistant with shared line support, review the task related to configuring CUCM Assistant with shared line support.

Related Topics

Cisco Unified Communications Manager Assistant with Proxy Line Support, on page 305
Configure Cisco Unified Communications Manager Assistant with Shared Line Support, on page 345

Set the Service Parameters for Cisco Unified Communications Manager Assistant

Service Parameters for the Cisco IP Manager Assistant service comprise three categories: general, clusterwide, and clusterwide parameters that must be configured if you want to use the Cisco Unified Communications Manager Assistant automatic configuration for managers and assistants. Specify clusterwide parameters once for all Cisco IP Manager Assistant services. Specify general parameters for each Cisco IP Manager Assistant service that is installed.

Set the Cisco IP Manager Assistant service parameters by using Cisco Unified Communications Manager Administration to access the service parameters (System > Service Parameters). Choose the server where the

Cisco Unified Communications Manager Assistant application resides and then choose the Cisco IP Manager Assistant service.

Cisco IP Manager Assistant includes the following service parameters that must be configured:

- Clusterwide Parameters That Apply to All Servers
    - Cisco IPMA Server (Primary) IP Address - No default. Administrator must manually enter this IP address. Administrator can assign up to 2500 managers and assistants to this address. To avoid potential high CPU usage, enter the address of the local CTIManager server where the IPMA process is running when you configure the Cisco IP Manager Assistant CTIManager (Primary) IP Address service parameter.
    - Cisco IPMA Server (Backup) IP Address - No default. Administrator must manually enter this IP address.
    - Cisco IPMA Server Port - Default specifies Port 2912.
    - Cisco IPMA Assistant Console Heartbeat Interval - Default specifies 30 seconds. This interval timer specifies how long it takes for the failover to occur on the assistant console.
    - Cisco IPMA Assistant Console Request Timeout - Default specifies 30 seconds.
    - Cisco IPMA RNA Forward Calls - Default specifies False. This service parameter does not apply to shared line support.
    - Cisco IPMA RNA Timeout - Default specifies 10 seconds. This service parameter does not apply to shared line support.
    - CTIManager Connection Security Flag has the following two options:

      Nonsecure - The security mode specifies nonsecure.

      Use Cluster Default - Cisco IP Manager Assistant service fetches the security mode for the cluster. If the cluster security mode is detected as mixed, Cisco Unified Communications Manager Assistant will open a secure connection to CTI Manager by using the Application CAPF profile. To make the secure connection succeed, configure both the “CTI Manager Connection Security Flag” and the “CAPF Profile Instance ID for Secure Connection to CTI Manager” parameters.

      Use Cluster Default - Cisco IP Manager Assistant service fetches the security mode for the Cisco Unified Communications Manager server. If the Cisco Unified Communications Manager server security mode is detected as mixed, Cisco Unified Communications Manager Assistant will open a secure connection to CTI Manager by using the Application CAPF profile. To make the secure connection succeed, configure both the “CTI Manager Connection Security Flag” and the “CAPF Profile Instance ID for Secure Connection to CTI Manager” parameters.
- Advanced Clusterwide
    - Enable Multiple Active Mode - The default specifies False. When this parameter is set to True, the administrator can configure up to 7000 managers and assistants by using multiple pools.
    - Pool 2: Cisco IPMA Server (Primary) IP Address - No default. Administrator must manually enter this IP address. Administrator can assign up to 2500 managers and assistants to this address.
    - Pool 2: Cisco IPMA Server (Backup) IP Address - No default. Administrator must manually enter this IP address.

  - Pool 3: Cisco IPMA Server (Primary) IP Address - No default. Administrator must manually enter this IP address. Administrator can assign up to 2500 managers and assistants to this address.
  - Pool 3: Cisco IPMA Server (Backup) IP Address - No default. Administrator must manually enter this IP address.

  Note Configure unique IP addresses for each pool so that the same Cisco IPMA server IP address does not appear in more than one pool.

- Cisco IPMA Service Parameters
  - CTIManager (Primary) IP Address - No default. Enter the IP address of the primary CTIManager that will be used for call control.
  - CTIManager (Backup) IP Address - No default. Administrator must manually enter this IP address.
  - Route Point Device Name for Proxy Mode - Not applicable for shared line support.
  - 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 Cisco Unified Communications Manager Assistant server will use to open a secure connection to CTIManager. You must configure this parameter if CTIManager Connection Security Flag is enabled.

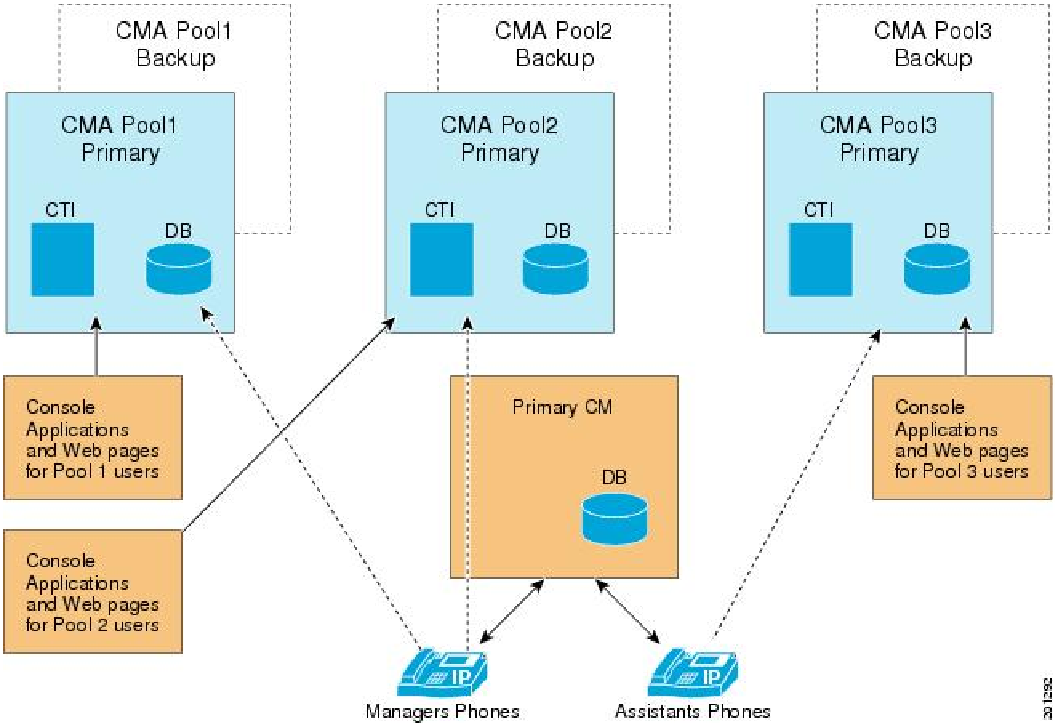
Cisco Unified Communications Manager Assistant includes the following clusterwide parameters that must be configured if you want to use the Cisco Unified Communications Manager Assistant automatic configuration for managers and assistants:

- Clusterwide Parameters for Softkey Templates
  - Assistant Softkey Template - Default specifies Standard Assistant softkey template. This parameter specifies the softkey template that is assigned to the assistant device during assistant automatic configuration.
  - Manager Softkey Template for Proxy Mode - This service parameter does not apply to shared line support.
  - Manager Softkey Template for Shared Mode - Default specifies Standard Shared Mode Manager. Set this parameter to specify the shared mode softkey template that is assigned to the manager device during manager automatic configuration.
- IPMA Device Configuration Defaults for Proxy Mode - These parameters do not apply for Cisco Unified Communications Manager Assistant with shared line support.
- Proxy Directory Number Range for Proxy Mode - These parameters do not apply for Cisco Unified Communications Manager Assistant with shared line support.
- Proxy Directory Number Prefix for Proxy Mode - These parameters do not apply for Cisco Unified Communications Manager Assistant with shared line support.

Configure Multiple Servers for Cisco Unified Communications Manager Assistant Scalability

Cisco Unified Communications Manager supports up to 3500 managers and 3500 assistants for a total of 7000 users. To support 7000 users, the administrator must configure multiple active Cisco IP Manager Assistant servers by enabling and setting service parameters. Administrators can configure up to three active Cisco IP Manager Assistant servers, with each managing up to 2500 pairs of managers and assistants. Each server can also have a backup server. Configure the Cisco IP Manager Assistant servers by using the Advanced Service Parameters, Enable Multiple Active Mode, Pool 2: Cisco IPMA Server, and Pool3: Cisco IPMA Server. See the Set the Service Parameters for Cisco Unified Communications Manager Assistant, on page 357 for more information. See the following figure.

Figure 23: Scalability Architecture



1. Activate IPMA service (see the Install and Activate Cisco Unified Communications Manager Assistant, on page 356)

2. Enable multiple active mode (see the Set the Service Parameters for Cisco Unified Communications Manager Assistant, on page 357)

3. Provide IP addresses for multiple pools (see the Set the Service Parameters for Cisco Unified Communications Manager Assistant, on page 357)

4. Add pool to the manager/assistant from the End User Configuration window (see the Configure a Manager and Assign an Assistant for Shared Line Mode, on page 364)

Migration Considerations

If you are migrating from a release previous to Cisco Unified Communications Manager Release 8.0(2), all managers and assistants will get migrated to Pool 1 (the default).

Security Considerations

Cisco Unified Communications Manager Assistant supports a secure connection to CTI (transport layer security connection).

The administrator must configure a CAPF profile (one for each Cisco Unified Communications Manager Assistant node) by choosing **User Management** > **Application User CAPF Profile**. From the Application User drop-down list box that is on the Application User CAPF Profile Configuration window, the administrator chooses IPMASecureSysUser.

For more information about configuring security for Cisco Unified Communications Manager Assistant, see the information on the CTIManager Connection Security Flag and the CAPF Profile Instance Id for Secure Connection to CTIManager service parameters in the Set the Service Parameters for Cisco Unified Communications Manager Assistant, on page 357.

The Cisco Unified Communications Manager Security Guide provides detailed security configuration procedures for CTI applications.

Starting the Cisco IP Manager Assistant Service

The Cisco IP Manager Assistant service runs as an application on Cisco Tomcat. To start or stop the Cisco IP Manager Assistant service, use the Serviceability Control Center Feature Services window.

Manager and Assistant Phone Configuration

You must configure and associate devices for each Cisco Unified Communications Manager Assistant manager and assistant. Before you begin, complete the following tasks, depending on the phone type.

Cisco Unified IP Phone 7940, 7942, 7945, 7960, 7962, 7965, and 7975 (SCCP and SIP)

- Add a Cisco Unified IP Phone for each manager and assistant that will be using Cisco Unified Communications Manager Assistant. To add these phones, use one of the following methods:
  - Manually (**Device** > **Phone**)
  - Auto registration
  - BAT
- Assign the Standard Assistant or Standard Shared Mode Manager softkey template.

Cisco Unified IP Phone 7940

You can use the Cisco Unified IP Phone 7940 for Cisco Unified Communications Manager Assistant, but certain restrictions apply:

- Add a Cisco Unified IP Phone 7940 for each manager with the following items configured:
  - Two lines, one for the primary line and one for the intercom

  - Softkey template for manager with shared line support

- Add a Cisco Unified IP Phone 7940 for each assistant with the following items configured:
  - Two lines, one for the primary line and one for the intercom
  - Softkey template for assistant

Note Cisco recommends the Cisco Unified IP Phones 7960, 7962, 7965, and 7975 because they provide more functionality.

Note Cisco Unified IP Phone 7940/60 supports only the Cisco Unified Communications Manager Assistant intercom feature.

After you complete these tasks, proceed to configure the phones.

Manager Phones

The following section describes the Cisco Unified Communications Manager Assistant requirements and tips for configuring a manager phone.

Manager Phone Configuration

Configure the manager Cisco Unified IP Phones with the following settings:

- Standard Shared Mode Manager softkey template
- Primary line
- Additional lines for shared line support (optional)
- Voice-mail profile on primary line
- If using the Cisco Unified IP Phone 7900 series, except Cisco Unified IP Phone 7940 or 7960, configure the intercom feature
- If using the Cisco Unified IP Phone 7940 or 7960, configure the incoming intercom line to support the auto answer with speakerphone or headset option
- If using the Cisco Unified IP Phone 7940 or 7960, configure the speed dial for outgoing intercom targets.
- User locale

You can automate some of these settings by choosing the Automatic Configuration check box on the End User Configuration window when you configure the manager. For step-by-step instructions, see the Configure a Manager and Assign an Assistant for Shared Line Mode, on page 364.

Automatic Configuration sets the following items for the manager device or device profile:

- Softkey template

- Auto answer with speakerphone for intercom line (applies only to Cisco Unified IP Phone 7940 and 7960)

Cisco Unified Communications Manager Assistant supports the Cisco Unified IP Phone 7940. For more information, see the Manager and Assistant Phone Configuration, on page 361.

Assistant Phones

The following section describes the requirements for configuring an assistant phone and provides tips on configuring an assistant phone. For step-by-step instructions, see the Configure Shared and Incoming Intercom Lines, on page 367.

Assistant Phone Configuration

Configure the assistant Cisco Unified IP Phones with the following settings:

- Standard Assistant softkey template (must include the Redirect and Transfer to Voice Mail softkeys)
- Default 14-button expansion module (optional)
- Primary line
- Shared lines for each configured manager (Use the same DN and partition as the manager primary line.)
- Incoming intercom line to support the auto answer with speakerphone or headset option (applies only to Cisco Unified IP Phone 7940 and 7960)
- Speed dial to incoming intercom line for each configured manager (applies only to Cisco Unified IP Phone 7940 and 7960)
- User locale

Cisco Unified Communications Manager Assistant supports the Cisco Unified IP Phone 7940. For more information, see the Manager and Assistant Phone Configuration, on page 361.

Nonmanager and Nonassistant Phones

In addition to configuring manager and assistant devices, configure all other users in Cisco Unified Communications Manager. Proper configuration allows managers and assistants to make calls to and receive calls from all other users in the system.

Manager and Assistant Configuration

From the Cisco Unified Communications Manager End User Configuration window, configure the settings for the managers and assistants who use the Cisco Unified Communications Manager Assistant feature. From this window, perform the following functions:

- Choose manager and assistant devices.
- Automatically configure a manager or assistant device, if desired.
- From the Manager Configuration or Assistant Configuration window that is accessed from the End User Configuration window, configure the following settings:

- Set up primary and incoming intercom lines for intercom capability. For example, extension 3102 serves as the intercom line for the manager. This line will receive intercom calls from the assistant. The assistant line 1 (1102) and line 2 (1103) display on the console, and the assistant answers them.

  Note The intercom line that you choose will be the one that you created by using the Cisco Unified Communications Manager intercom feature (applicable only to Cisco Unified IP Phones 7942, 7945, 7962, 7965, and 7975) or by using speed dials (applicable only to Cisco Unified IP Phones 7940 and 7960).

- Configure assistants for managers.

Note When the shared lines for the manager and assistant are configured (using the Directory Number Configuration window in Cisco Unified Communications Manager Administration), the assistant configuration gets updated appropriately.

- Choose the local language in which the End User Configuration window displays.

Configure a Manager and Assign an Assistant for Shared Line Mode

Perform the following procedure to configure a Cisco Unified Communications Manager Assistant manager and assign an assistant to the manager. To configure a new user and associate the device to the user, see the Cisco Unified Communications Manager Administration Guide. To configure the same directory number for the manager primary line and assistant secondary line, see the Cisco Unified Communications Manager Administration Guide.

Tip Configure manager information before configuring Cisco Unified Communications Manager Assistant information for an assistant.

Procedure

Step 1 To configure the manager and to assign an assistant to an existing user, choose **User Management** > **End User**. From the Find and List Users window, click the **Find** button. The window displays all of the end users that are configured in Cisco Unified Communications Manager.

Step 2 To display user information for the chosen manager, click the user name.

The End User Configuration window displays.

Step 3 To configure Cisco Unified Communications Manager Assistant information for the manager, choose Manager Configuration from the Related Links drop-down list box and click **Go.**

Step 4 The Manager Configuration window displays and contains manager information, assistant information, and controlled lines information.

Step 5 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, check the Automatic Configuration check box.

Note Automatic Configuration for intercom applies only when the Cisco Unified Communications Manager Assistant intercom feature is used for the Cisco Unified IP Phones 7940 and 7960.

Step 6 Click the Uses Shared Lines check box.

Step 7 To associate a device name or device profile with a manager, choose the device name or device profile from the Device Name/Profile drop-down list box. (Extension mobility uses device profiles.) For information about using Cisco Extension Mobility with Cisco Unified Communications Manager Assistant, see the Extension Mobility, on page 353.

Note If the manager telecommutes, click the Mobile Manager check box and optionally choose Device Profile. When Device Profile is chosen, the manager must log on to the phone by using extension mobility before accessing Cisco Unified Communications Manager Assistant.

Step 8 From the Intercom Line drop-down list box, choose the intercom line appearance for the manager, if applicable.

Note The chosen intercom line applies to the Cisco Unified Communications Manager Assistant and Cisco Unified Communications Manager intercom features.

Step 9 If applicable, from the Assistant Pool drop-down list box, choose the appropriate Pool number (1 to 3).

Step 10 To assign an assistant to the manager, choose the name of the assistant from the Available Assistants list and move it to the Associated Assistants list box by clicking the down arrow.

Tip You can go to the Assistant Configuration window by highlighting the assistant name and clicking the View Details link.

Step 11 To configure the Cisco Unified Communications Manager Assistant controlled lines, choose the appropriate line from the Available Lines list box and move it to the Selected Lines list box by clicking the down arrow.

Note Ensure the controlled line is always the shared line DN.

To remove a line from the Selected Lines selection box and from Cisco Unified Communications Manager Assistant control, highlight the line and click the up arrow.

Step 12 Click the Save button.

If you checked the Automatic Configuration check box and the service parameters are invalid, a message displays.

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.

Note When non-Cisco Unified Communications Manager Assistant changes such as name, user locale, or PIN, are made to a user, the user (manager or assistant) must log out of Cisco Unified Communications Manager Assistant and log in before the changes occur.

Delete CUCM Assistant Information for the Manager

Perform the following procedure to delete Cisco Unified Communications Manager Assistant information for a manager. To delete non-Cisco Unified Communications Manager Assistant information for a manager, see the Extension Mobility, on page 353 section in the Cisco Unified Communications Manager Administration Guide.

Procedure

Step 1 To search for the manager for whom you want to delete Cisco Unified Communications Manager Assistant information, choose **User Management** > **End User** from Cisco Unified Communications Manager Administration.

Step 2 From the Find and List Users window, click the **Find** button. The window displays all of the end users that are configured in Cisco Unified Communications Manager.

Step 3 From the Find and List Users window, choose the manager whose information you want to delete. The End User Configuration window displays.

Step 4 From the Related Links drop-down list box, choose Manager Configuration and click **Go.**

The Manager Configuration window displays for the user that you chose.

Step 5 Click the **Delete** button.

The update takes effect immediately.

Update the Manager CUCM Assistant Configuration

Perform the following procedure to update Cisco Unified Communications Manager Assistant information for a manager. To update non-Cisco Unified Communications Manager Assistant information for a manager, see the Cisco Unified Communications Manager Administration Guide.

Procedure

Step 1 To search for the manager for whom you want to update information, choose **User Management** > **End User** from Cisco Unified Communications Manager Administration.

Step 2 From the Find and List Users window, click the **Find** button. The window displays all the end users that are configured in Cisco Unified Communications Manager.

Step 3 From the Find and List Users window, choose the manager whose information you want to update. The End User Configuration window displays.

Step 4 From the Related Links drop-down list box, choose Manager Configuration and click **Go.**

The Manager Configuration window displays for the user that you chose.

Step 5 Update the information that you want changed such as device name, controlled lines, or intercom line appearance.

Step 6 Click the **Save** button.

The update takes effect immediately.

Note The system automatically configures the softkey template and auto answer with speakerphone for intercom line for the manager phone on the basis of the Cisco IP Manager Assistant service parameters when the Automatic Configuration check box is checked.

Note When non-Cisco Unified Communications Manager Assistant changes such as name, user locale, or PIN, are made to a user, the user (manager or assistant) must log out of Cisco Unified Communications Manager Assistant and log in for the changes to occur.

Configure Shared and Incoming Intercom Lines

Use the Assistant Configuration of the End User Configuration window to configure the following items:

- Device name of the assistant phone
- Intercom line that the assistant uses to answer the manager calls (optional)
- Shared line of the manager to which the assistant phone gets associated (this gets done automatically when the manager and assistant share the same DN).

Administrators can set up one or more lines with a shared line appearance. The Cisco 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.

In a shared line appearance, for example, you can set up a shared line, so a directory number appears on line 1 of a manager phone and also on line 2 of an assistant phone.

Perform the following procedure to configure the manager shared line and incoming intercom line appearances for an assistant. To configure a new user and associate devices, see the Cisco Unified Communications Manager Administration Guide.

Tip Before configuring the Cisco Unified Communications Manager Assistant information for an assistant, you must configure the manager information and assign an assistant to the manager. See Configure a Manager and Assign an Assistant for Shared Line Mode, on page 364.

Procedure

Step 1 To search for the assistant for whom you want to configure Cisco Unified Communications Manager Assistant information, choose **User Management** > **End User** from Cisco Unified Communications Manager Administration.

Step 2 From the Find and List Users window, click the **Find** button. The window displays all the end users that are configured in Cisco Unified Communications Manager.

Step 3 To display user information for the chosen assistant, click the user name.

The End User Configuration window displays.

Step 4 To configure information for the assistant, choose Assistant Configuration from the Related Links drop-down list box and click **Go.**

The Assistant Configuration window displays for the user that you chose.

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. Additionally, the system sets auto answer with speakerphone for intercom line.

Step 5 From the Device Name drop-down list box, choose the device name to associate with the assistant.

Step 6 From the Intercom Line drop-down list box, choose the incoming intercom line appearance for the assistant.

Step 7 From the Primary Line drop-down list box, choose the primary line for the assistant.

In the Associated Manager selection list box, the name of the previously configured manager displays.

Tip To view existing manager configuration information, highlight the manager name in the Associated Managers list and click the View Details link. The Manager Configuration window displays. To return to the Assistant Configuration window, highlight the assistant name and click the View Details link on the Manager Configuration window.

Step 8 To associate the manager line to the assistant line, perform the following steps from the Manager Association to the Assistant Line selection box:

a) In the Available Lines drop-down list box, choose the assistant line that will be associated with the manager line.
b) In the Manager Names drop-down list box, choose the preconfigured manager name with which the assistant is associated.
c) In the Manager Lines drop-down list box, choose the manager line that will be associated with the assistant line.

Step 9 Click the **Save** button.

The update takes effect immediately. If you chose automatic configuration, the assistant device automatically resets.

Delete the CUCM Assistant Information

Perform the following procedure to delete Cisco Unified Communications Manager Assistant information for an assistant. To delete non-Cisco Unified Communications Manager Assistant information for an assistant, see the Cisco Unified Communications Manager Administration Guide.

Procedure

Step 1 To search for the assistant for whom you want to delete information, choose **User Management** > **End User** from Cisco Unified Communications Manager Administration.

Step 2 From the Find and List Users window, click the **Find** button. The window displays all the end users that are configured in Cisco Unified Communications Manager.

Step 3 From the Find and List Users window, choose the assistant whose information you want to delete. The End User Configuration window displays.

Step 4 From the Related Links drop-down list box, choose Assistant Configuration and click **Go.**

The Assistant Configuration window displays for the user that you chose.

Step 5 Click the **Delete** button.

The update takes effect immediately.

Note When non-Cisco Unified Communications Manager Assistant changes such as name, user locale, or PIN, are made to a user, the user (manager or assistant) must log out of Cisco Unified Communications Manager Assistant and log in before the changes occur.

Update the CUCM Assistant Configuration

Perform the following procedure to update Cisco Unified Communications Manager Assistant information for an assistant. To update non-Cisco Unified Communications Manager Assistant information for an assistant, see topics related to end user configuration settings in the *Cisco Unified Communications Manager Administration Guide*.

Procedure

Step 1 To search for the assistant for whom you want to update t information, choose **User Management** > **End User** from Cisco Unified Communications Manager Administration.

Step 2 From the Find and List Users window, click the **Find** button. The window displays all the end users that are configured in Cisco Unified Communications Manager.

Step 3 From the Find and List Users window, choose the assistant whose information you want to update. The End User Configuration window displays.

Step 4 From the Related Links drop-down list box, choose Assistant Configuration and click **Go.**

The Assistant Configuration window displays for the user that you chose.

Step 5 Update the information that you want changed such as device name, intercom line, or associated manager information.

Step 6 Click the **Save** button.

The update takes effect immediately.

Note During automatic configuration, the system automatically sets the softkey template and intercom line on the basis of the Cisco IP Manager Assistant service parameter settings and sets auto answer with speakerphone for intercom line. If you do not want to use automatic configuration, uncheck the Automatic Configuration check box.

Note When non-Cisco Unified Communications Manager Assistant changes such as name, user locale, or PIN, are made to a user, the user (manager or assistant) must log out of Cisco Unified Communications Manager Assistant and log in before the changes occur.

Dial Rules Configuration

The administrator uses dial rules configuration to add and sort the priority of dialing rules. Dial rules for Cisco Unified Communications Manager Assistant automatically strip numbers from or add numbers to telephone numbers that the assistant dials. For example, a dial rule can automatically add the digit 9 in front of a 7-digit telephone number to provide access to an outside line.

The *Cisco Unified Communications Manager System Guide* provides additional information on application dial rules.

Provide Information to Cisco Unified Communications Manager Assistant Managers and Assistants

Install the assistant console application for Cisco Unified Communications Manager Assistant by accessing a URL. The administrator sends the URL, in the Install the Assistant Console Plug-In, on page 370, to the assistant.

Note The assistant console application installation program supports Microsoft Internet Explorer 7, and Internet Explorer 8, FireFox 3.x and Safari 4.x.

Install the Assistant Console Plug-In

The assistant console application installation supports Internet Explorer 7, Microsoft Internet Explorer 8, FireFox 3.x and Safari 4.x. You can install the application on a PC that runs Windows 7, Windows XP or Windows Vista.

A previous 5.x or 6.x version of the assistant console application works with Cisco Unified Communications Manager 7.1, but if you decide to install the 7.1 plug-in, you must uninstall the previous 5.x or 6.x version of the assistant console application before you install the plug-in.

Previous versions of the assistant console application do not work with Windows Vista. If the PC runs Windows Vista, install the plug-in.

After you upgrade from Cisco Unified CallManager Release 4.x to Cisco Unified Communications Manager 7.1, you must install the assistant console plug-in. Before you install the plug-in, uninstall the 4.x version of the assistant console application.

To uninstall previous versions of the assistant console application (6.0(1), 4.x, or any 5.x version before 5.1(3)), choose **Start** > **Programs** > **Cisco Unified CallManager Assistant** > **Uninstall Assistant Console**.

To uninstall a 5.1(3) or 6.1(x) assistant console application, go to the Control Panel and remove it.

Tip The assistant console application requires that JRE1.4.2_05 exist in C:\Program Files\Cisco\Cisco Unified Communications Manager.

To install the assistant console application, perform the following procedure:

Procedure

Step 1 From the PC where you want to install the assistant console application, browse to Cisco Unified Communications Manager Administration and choose **Application** > **Plugins.**

Step 2 For the Cisco Unified Communications Manager Assistant plug-in, click the Download link; save the executable to a location that you will remember.

Step 3 Locate the executable and run it.

Tip If you install the application on a Windows Vista PC, a security window may display. Allow the installation to continue.

The installation wizard displays.

Step 4 In the Welcome window, click **Next.**

Step 5 Accept the license agreement and click **Next.**

Step 6 Choose the location where you want the application to install. After you choose the location for the installation, click **Next.**

Tip By default, the application installs in C:\Program Files\Cisco\ Unified Communications Manager Assistant Console.

Step 7 To install the application, click **Next.**

The installation begins.

Step 8 After the installation completes, click **Finish.**

Tip To launch the assistant console, click the desktop icon or choose **Cisco Unified Communications Manager Assistant** > **Assistant Console** in the Start...Programs menu.

Tip Before the assistant logs in to the console, give the assistant the port number and the IP address or hostname of the Cisco Unified Communications Manager server where the Cisco IP Manager Assistant service is activated. 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.

Tip Before the assistant logs in to the console, give the assistant the user name and password that is required to log in to the console.

Tip The Advanced tab in the Cisco Unified Communications Manager Assistant Settings window allows you to enable trace for the assistant console.

Assistant Console Dialog Options

The assistant console displays a dialog that contains the following options:

- Location to Install - The path of the directory where the assistant console software gets installed. The default specifies following path:

  c:\Program Files\Cisco\Unified Communications Manager Assistant Console

- Create Desktop Shortcut - Default specifies true. This parameter determines whether a shortcut is created on the assistant console.

- Create StartMenu Shortcut - Default specifies true. This parameter determines whether a shortcut is created in the Start menu (**Start** > **Programs** > **Cisco Unified Communications Manager Assistant** > **Assistant Console**).
- Install JRE - Default specifies true. This parameter determines whether JRE is installed along with Unified CM Assistant assistant console. If this option is turned off, you need to ensure that the following configuration is on the assistant console:
    - Install JRE 1.4.2_05 (international version) on the assistant console
    - Create an environment variable - Assistant_JRE on the assistant console, which gives the path to the JRE; for example, c:\Program Files\Jave\j2re1.4.2_05

Manager Configuration

Managers can customize their feature preferences from the Manager Configuration window by using the following URL:

https://<Cisco Unified Communications Manager Assistant server>:8443/ma/desktop/maLogin.jsp

where

Cisco Unified Communications Manager Assistant server specifies the IP address of the server that has the Cisco IP Manager Assistant service running on it.

Note The Manager Configuration only supports Microsoft Internet Explorer 6.0 or later.

The administrator must send this URL to the manager.

CHAPTER 14

Cisco Unified Communications Manager Auto-Attendant

This chapter provides information about Cisco Unified Communications Manager Auto-Attendant, a simple automated attendant, which allows callers to locate people in your organization without talking to a receptionist. You can customize the prompts that are played for the caller, but you cannot customize how the software interacts with the customer.

Configure Auto-Attendant

Cisco Unified Communications Manager Auto-Attendant, a simple automated 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, but you cannot customize how the software interacts with the customer.

Perform the following steps to configure Cisco Unified Communications Manager Auto-Attendant.

Procedure

Step 1 Install and configure Cisco Unified Communications Manager.

Step 2 Configure Cisco Unified Communications Manager users.

Step 3 Configure the Cisco Customer Response Solutions (CRS) Engine. You must install and configure Cisco CRS before you can use Cisco Unified Communications Manager Auto-Attendant. The Cisco CRS Engine controls the software and its connection to the telephony system.

- Set up the cluster, if applicable.
- Set up the server.
- Add a Unified CM telephony call control group.
- Provision a Cisco media termination subsystem.
- Add a new Cisco Unified Communications Manager Auto-Attendant.

- Configure a Unified CM telephony trigger.

Step 4 Customize Cisco Unified Communications Manager Auto-Attendant, so its prompts are meaningful to the way that you are using the automated attendant.

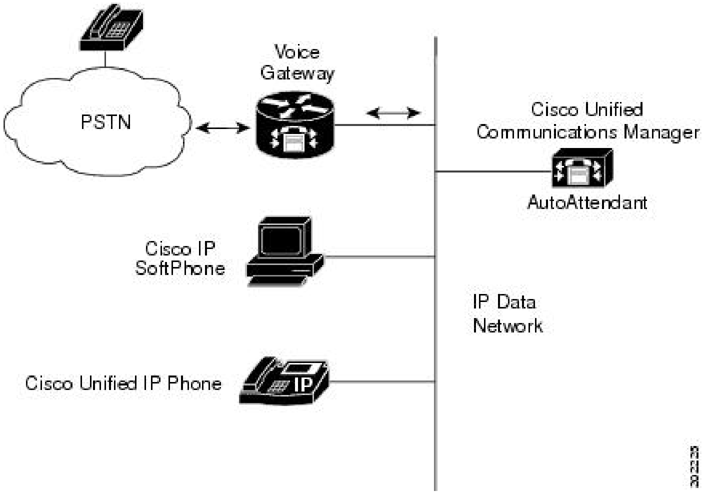
- Modify an instance of Cisco Unified Communications Manager Auto-Attendant.
- Configure the Cisco Unified Communications Manager Auto-Attendant prompts.
    - Recording the welcome prompt
    - Configuring the welcome prompt
    - Uploading a spoken name

CUCM Auto-Attendant Feature

Cisco Unified Communications Manager Auto-Attendant (see the following figure) works with Cisco 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.

This section provides an introduction to Cisco Unified Communications Manager Auto-Attendant.

Figure 24: Using Cisco Unified Communications Manager Auto-Attendant



CUCM Auto-Attendant Overview

Cisco Unified Communications Manager 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.
  - 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 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.
- When the caller has specified 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.

Components of CUCM Auto-Attendant

The Cisco Customer Response Solutions (CRS) Platform provides the components that are required to run Cisco Unified Communications Manager Auto-Attendant. The platform provides a multimedia (voice/data/web) IP-enabled customer care application environment.

Note Cisco CRS gets marketed under the names Cisco Unified Contact Center Express and Cisco Unified IP IVR, which are products on the Cisco CRS platform.

Cisco Unified Communications Manager Auto-Attendant uses three main components of the Cisco CRS Platform:

- Gateway - Connects the unified communications network to the Public Switched Telephone Network (PSTN) and to other private telephone systems such as Public Branch Exchange (PBX). You must purchase gateways separately.
- Cisco Unified Communications Manager Server - Provides the features that are required to implement IP phones, manage gateways, provides failover and redundancy service for the telephony system, and directs voice over IP traffic to the Cisco CRS system. You must purchase Cisco Unified Communications Manager separately.
- Cisco CRS Server - Contains the Cisco CRS Engine that runs Cisco Unified Communications Manager Auto-Attendant. The Cisco Unified Communications Manager Auto-Attendant package includes the Cisco CRS Server and Engine.

See the installation and configuration guides for more information about the Cisco CRS Platform.

System Requirements for Cisco Unified Communications Manager Auto-Attendant

Cisco Unified Communications Manager Auto-Attendant requires the following software components to operate:

- Cisco Unified Communications Manager
- Cisco CRS platform

Cisco Unified Communications Manager Auto-Attendant runs on the Cisco Media Convergence Server (Cisco MCS) platform or on a Cisco-certified server.

See the following Cisco documentation:

- *Installing Cisco Unified Communications Manager*
- Cisco CRS documentation installation and configuration guides

Install the CUCM Auto-Attendant

No installation is required. Auto-Attendant comes standard with the five-seat bundle. See the Cisco Customer Response Solutions Administration Guide, Release 5.0(1) and the Cisco Customer Response Solutions Installation Guide for more information.

Configure CUCM Auto-Attendant and the Cisco CRS Engine

To configure the Cisco Unified Communications Manager Auto-Attendant, review the Configure Auto-Attendant, on page 373.

Managing CUCM Auto-Attendant

Use Cisco CRS Administration to manage Cisco Unified Communications Manager Auto-Attendant. Use the online help to learn how to use the interface and perform these tasks. The following table describes the management tasks.

Table 40: Managing Cisco Unified Communications Manager Auto-Attendant

Task	Purpose	Commands (from the Cisco CRS Administration main window)
Start and stop the Cisco CRS Engine	Make sure that the engine is running for your automated attendant to work. You can stop and restart the engine to help resolve or troubleshoot problems.	Choose **System** > **Control Center** and click the Cisco CRS Engine in the menu on the left. In the list that appears, find “CRS Engine”. In the Status column, if a triangular button points to the right, you know that the engine is running. If a square shows in this column, you know that the engine is not running. To restart the engine, click the radio button next to “CRS Engine” and click Restart. If the engine is running and you want to stop it, click the radio button next to “CRS Engine” and click Stop.
Change the Cisco CRS Engine configuration	Modify the engine configuration to resolve problems.	Choose **System** > **System Parameters**.
Set up trace files	Set up trace files to collect troubleshooting information.	Choose **System** > **Tracing**; then, click **Trace File Configuration**. See the online help for detailed information.
View trace files	View trace files to see the results of your tracing.	Choose**System** > **Control Center**; then, click server name. Click the **Server Traces** link. Choose the trace file that you created.
Monitor performance in real time	You can monitor the performance of the system while it is running if you install the real-time reporting monitor.	Choose **Tools** > **Real-Time Reporting**. See the online help for information on using Real Time Reporting.

CHAPTER 15

Client Matter Codes and Forced Authorization Codes

This chapter provides information about Forced Authorization Codes (FAC) and Client Matter Codes (CMC) which allow you to manage call access and accounting. CMC assists with call accounting and billing for billable clients, while Forced Authorization Codes regulate the types of calls that certain users can place.

Client matter codes force the user to enter a code to specify 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. The Forced Authorization Codes feature forces the user to enter a valid authorization code before the call completes.

The CMC and FAC features require that you make changes to route patterns and update your dial plan documents to reflect that you enabled or disabled FAC and/or CMC for each route pattern.

Configure Client Matter Codes and Forced Authorization Codes

Forced Authorization Codes (FAC) and Client Matter Codes (CMC) allow you to manage call access and accounting. CMC assists with call accounting and billing for billable clients, while Forced Authorization Codes regulate the types of calls that certain users can place.

Client matter codes force the user to enter a code to specify 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. The Forced Authorization Codes feature forces the user to enter a valid authorization code before the call completes.

Perform the following steps to configure client matter codes and forced authorization codes.

Procedure

Step 1 Review feature limitations.

Step 2 Design and document the system; for example, document a list of client matters that you want to track.

Step 3 Insert the codes by using Cisco Unified Communications Manager Administration or by using Bulk Administration Tool (BAT).

Tip Consider using BAT for small or large batches of codes; the comma separated values (CSV) file in BAT can serve as a blueprint for the codes, corresponding names, corresponding levels, and so on.

Step 4 To enable FAC or CMC, add or update route patterns in Cisco Unified Communications Manager Administration.

Step 5 Update your dial plan documents or keep a printout of the BAT CSV file with your dial plan documents.

Step 6 Provide all necessary information, for example, codes, to users and explain how the features works.

Related Topics

Client Matter Codes and Forced Authorization Codes, on page 379

Interactions and Restrictions, on page 382

Client Matter Codes, on page 380

Forced Authorization Codes, on page 381

Configure Client Matter Codes, on page 384

Configure Forced Authorization Codes, on page 386

Enable Client Matter Codes, on page 385

Enable Forced Authorization Codes, on page 387

Provide Information to Users, on page 388

Client Matter Codes

To use the Client Matter Codes feature, users must enter a client matter code to reach certain dialed numbers. You enable or disable CMC through route patterns, and you can configure multiple client matter codes. When a user dials a number that is routed through a CMC-enabled route pattern, a tone prompts the user for the client matter code. When the user enters a valid CMC, the call occurs; if the user enters an invalid code, reorder occurs. The CMC writes to the CDR, so you can collect the information by using CDR Analysis and Reporting (CAR), which generates reports for client accounting and billing.

The Client Matter Codes feature benefits law offices, accounting firms, consulting firms, and other businesses or organizations where tracking the length of the call for each client is required. Before you implement CMC, obtain a a list of all clients, groups, individuals, parties, and so on that you plan to track through CMC. Determine whether you can assign the codes consecutively, arbitrarily, or whether your organization requires a special code structure; for example, using existing client account numbers for CMC. For each client (or group, individual, and so on) that you want to track, you must add a client matter code in the Client Matter Code Configuration window of Cisco Unified Communications Manager Administration. Then, in Cisco Unified Communications Manager Administration, you must enable CMC for new or existing route patterns. After you configure CMC, make sure that you update your dial plan documents to indicate the CMC-enabled route patterns.

Tip If you want users to enter a CMC for most calls, consider enabling CMC for most or all route patterns in the dial plan. In this situation, users must obtain CMCs and a code, such as 555, for calls that do not relate to clients. All calls automatically prompt the users for a CMC, and the users do not have to invoke CMC or dial special digits. For example, a user dials a phone number, and the system prompts the user for the client code; if the call relates to a client matter, the user enters the appropriate CMC; if the call does not relate to a client, the user enters 555.

Tip If only a select number of users must enter a CMC, consider creating a new route pattern specifically for CMC; for example, use 8.@, which causes the system to prompt users for the client code when the phone number that is entered starts with the number 8. Implementing CMC in this manner provides a means to invoke CMC and allows the existing dial plan to remain intact. For example, for client-related calls, a user may dial 8-214-555-1234 to invoke CMC; for general calls that are not related to clients, the users just dial 214-555-1234 as usual.

Forced Authorization Codes

When you enable FAC through route patterns in Cisco Unified Communications Manager Administration, users must enter an authorization code to reach the intended recipient of the call. When a user dials a number that is routed through a FAC-enabled route pattern, the system plays a tone that prompts for the authorization code.

In Cisco Unified Communications Manager Administration, you can configure various levels of authorization. If the user authorization code does not meet or exceed the level of authorization that is specified to route the dialed number, the user receives a reorder tone. If the authorization is accepted, the call occurs. The name of the authorization writes to call detail records (CDRs), so you can organize the information by using CDR Analysis and Reporting (CAR), which generates reports for accounting and billing.

You can use FAC for colleges, universities, or any business or organization when limiting access to specific classes of calls proves beneficial. Likewise, when you assign unique authorization codes, you can determine which users placed calls. For each user, you specify an authorization code, then enable FAC for relevant route patterns by selecting the appropriate check box and specifying the minimum authorization level for calls through that route pattern. After you update the route patterns in Cisco Unified Communications Manager Administration, update your dial plan documents to define the FAC-enabled route patterns and configured authorization level.

To implement FAC, you must devise a list of authorization levels and corresponding descriptions to define the levels. You must specify authorization levels in the range of 0 to 255. Cisco allows authorization levels to be arbitrary, so you define what the numbers mean for your organization. Before you define the levels, review the following considerations, which represent examples or levels that you can configure for your system:

- Configure an authorization level of 10 for interstate long-distance calls in North America.
- Because intrastate calls often cost more than interstate calls, configure an authorization level of 20 for intrastate long-distance calls in North America.
- Configure an authorization level of 30 for international calls.

Tip Incrementing authorization levels by 10 establishes a structure that provides scalability when you need to add more authorization codes.

Interactions and Restrictions

You can implement client matter codes (CMC) and forced authorization codes (FAC) 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. If you implement CMC and FAC together as described in the previous example, the user dials a number, enters the user-specific authorization code when prompted to do so, and then enters the client matter code at the next prompt. CMC and FAC tones sound the same to the user, so the feature tells the user to enter the authorization code after the first tone and enter the CMC after the second tone.

Cisco Unified Communications Manager provides redundancy, which handles the normal processes that are in place for Cisco Unified Communications Manager.

The CMC and FAC features work with all Cisco Unified IP Phones running SCCP and SIP, Cisco Mobility, and gateways.

Before you implement CMC and FAC, review the following restrictions:

- Because the number of CMCs directly impacts the time that is required for Cisco Unified Communications Manager to start up, you should limit the number of CMCs to 60,000. If you configure more CMCs than that, expect significant delays. For example, a system with 400,000 CMCs requires 1 hour to start up; a system with 1 million CMCs requires 4 hours to start up.

- After dialing the phone number, hearing-impaired users should wait 1 or 2 seconds before entering the authorization or client matter code.

- Calls that are forwarded to an FAC- or CMC-enabled route pattern fail because no user is present to enter the code. This limitation applies to call forwarding that is configured in Cisco Unified Communications Manager Administration or the Cisco Unified Communications Self Care Portal. You can configure call forwarding, but all calls that are forwarded to an FAC- or CMC-enabled route pattern results in reorder. When a user presses the CFwdALL softkey and enters a number that has FAC or CMC enabled on the route pattern, the user receives reorder, and call forwarding fails.

  You cannot prevent the configuration of call forwarding to an FAC- or CMC-enabled route pattern; forwarded calls that use these route patterns drop because no code is entered. 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 does not localize FAC or CMC. 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, FAC and CMC are localized.

- The CMC and FAC features do not support overlap sending because the 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 becomes disabled. If you check the Allow Overlap Sending check box, the Require Forced Authorization Code and the Require Client Matter Code check boxes become disabled.
- The CMC and FAC feature on Cisco Mobility does not support an alternative number as its DVO callback number. The DVO callback number has to be the number registered in the MI (Mobility Identity) page.
- The FAC and CMC tones play only on Cisco Unified IP Phones that are running SCCP or SIP, TAPI/JTAPI ports, and MGCP FXS ports.
- Calls that originate from a SIP trunk, H.323, or MGCP gateway fail if they encounter a route pattern that requires FAC or CMC and the caller is not configured as Cisco Unified Mobility.
- H.323 analog gateways do not support FAC or CMC because these gateways cannot play tones.
- Restrictions apply to CTI devices that support FAC and CMC. For more information, see the Use FAC/CMC with CTI JTAPI and TAPI Applications, on page 383.
- Cisco Web Dialer does not support FAC or CMC.
- Cisco IP softphone cannot play tones; however, after a Cisco IP softphone user dials a directory number, the user can use CMC and FAC by waiting 1 or 2 seconds before entering the code.
- If you do not append the FAC or CMC with #, the system waits for the T302 timer to extend the call.
- When you press the Redial softkey on the phone, you must enter the authorization code or CMC when the number that you dialed is routed through an FAC- or CMC-enabled route pattern. Cisco does not save the code that you entered for the previous call.
- You cannot configure authorization code or CMC for speed-dial buttons. You must enter the code when the system prompts you to do so.
- FAC and CMC do not work with failover calls.

Use the Cisco Bulk Administration Tool

You can use Bulk Administration Tool (BAT) to insert, update, and delete CMC and FAC. For more information on how to perform these tasks, see the Cisco Unified Communications Manager Bulk Administration Guide that is compatible with this release of Cisco Unified Communications Manager.

Use CDR Analysis and Reporting

CDR Analysis and Reporting (CAR) allows you to run reports that provide call details for authorization code names, authorization levels, and CMCs. For information on how to generate reports in CAR, see the Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide.

Use FAC/CMC with CTI JTAPI and TAPI Applications

In most cases, Cisco Unified Communications Manager 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 FAC- or CMC-enabled route pattern, the user must enter a code after receiving the tone. When a user redirects or blind transfers a call through a FAC- or CMC-enabled route pattern, the user receives no tone, so the application must send the codes to Cisco Unified Communications Manager. If Cisco Unified Communications Manager receives the appropriate codes, the call connects to the intended party. If Cisco Unified Communications Manager does not receive the appropriate codes, Cisco Unified Communications Manager sends an error to the application that indicates which code is missing.

Cisco Unified Communications Manager does not support call forwarding through FAC- or CMC-enabled route patterns. For more information, see the Interactions and Restrictions, on page 382.

System Requirements

The minimum requirements for CMC and FAC specify that every server in the cluster must have Cisco Unified Communications Manager Release 5.0 or a later version.

Cisco Unified IP Phones that are running SCCP and SIP support CMC and FAC. The following Cisco Unified IP Phones (SCCP) support CMC and FAC:

- Cisco Unified IP Phones 6900 Series
- Cisco Unified IP Phones 7900 Series

Installation of CMC and FAC

The CMC and FAC features install automatically when you install Cisco Unified Communications Manager. To make these features work in your Cisco Unified Communications Manager network, you must perform the tasks that are described in the Configure Client Matter Codes, on page 384.

Configure Client Matter Codes

This section provides information to configure and enable client matter codes. After you obtain the list of CMCs that you plan to use, you add those codes to the database and enable the CMC feature for route patterns.

Tip Before you configure client matter codes, review the configuration summary task for client matter and forced authorization codes.

Related Topics

Configure Client Matter Codes and Forced Authorization Codes, on page 379

CMC Configuration

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Client Matter Codes** menu path to configure client matter codes.

Client matter codes (CMC) allow you to manage call access and accounting. CMC assists with call accounting and billing for billable clients by forcing the user to enter a code to specify 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.

Tips About Configuring Client Matter Codes

You enter CMCs in Cisco Unified Communications Manager Administration or through the Cisco Bulk Administration Tool (BAT). If you use BAT, the BAT comma separated values (CSV) file provides a record of CMCs and client names. After you configure CMC, make sure that you update your dial plan documents or keep a printout of the BAT CSV file with your dial plan documents.

After you add all CMCs, see the Enable Client Matter Codes, on page 385.

Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the Enable Client Matter Codes, on page 385 section in the Cisco Unified Communications Manager Administration Guide and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration Settings Table

Use the following table as a guide when you configure client matter codes. For more information on client matter codes and forced authorization codes, see the Client Matter Codes and Forced Authorization Codes, on page 379.

This table describes the client matter codes configuration settings. Use this table in conjunction with the Configure Client Matter Codes, on page 384.

Table 41: Configuration Settings for Adding a CMC

Setting	Description
Client Matter Code	Enter a unique code of no more than 16 digits that the user will enter when placing a call. The CMC displays in the CDRs for calls that use this code.
Description	This optional field associates a client code with a client. The description can include up to 50 characters in any language, but it cannot include double-quotes (“), percentage sign (%), ampersand (&), back-slash (\), angle brackets (<>), or either type of brackets ([ ] { }).

Enable Client Matter Codes

Perform the following steps to enable CMCs on route patterns:

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Call Routing** > **Route/Hunt** > **Route Pattern**.

Step 2 Perform one of the following tasks:

a) To update an existing route pattern, enter search criteria in the Find and List Route Pattern window, as described in the Cisco Unified Communications Manager Administration Guide.

b) To add a new route pattern, see the Cisco Unified Communications Manager Administration Guide.

Step 3 In the Route Pattern Configuration window, check the Require Client Matter Code check box.

Step 4 Perform one of the following tasks:

a) If you updated the route pattern, click Save.

b) If you added a new route pattern, click Save.

Step 5 Update an existing route pattern, or add a new route pattern for all route patterns that require a client matter code.

Step 6 After you complete the route pattern configuration, see the Provide Information to Users, on page 388.

Configure Forced Authorization Codes

This section provides information to configure and enable forced authorization codes.

Tip Before you configure forced authorization codes, review the configuration summary task for client matter and forced authorization codes..

After you design your FAC implementation, you enter authorization codes either in Cisco Unified Communications Manager Administration or through the Cisco Bulk Administration Tool (BAT). Consider using BAT for large batches of authorization codes; the comma separated values (CSV) file in BAT serves as a blueprint for authorization codes, corresponding names, and corresponding levels.

Note For future reference, make sure that you update your dial plan documents or keep a printout of the CSV file with your dial plan documents.

Related Topics

Configure Client Matter Codes and Forced Authorization Codes, on page 379

FAC Configuration

In Cisco Unified Communications Manager Administration, use the **Routing** > **Forced Authorization Codes** menu path to configure forced authorization codes.

Forced Authorization Codes (FAC) allow you to manage call access and accounting by regulating the types of calls that certain users can place. The Forced Authorization Codes feature forces the user to enter a valid authorization code before the call completes.

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the *Cisco Unified Communications Manager Administration Guide* and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Tip After you add all authorization codes, see the topic to enable forced authorization codes.

Related Topics

Enable Forced Authorization Codes, on page 387
FAC Configuration Settings, on page 387

FAC Configuration Settings

The following table describes the FAC configuration settings.

Table 42: Configuration Settings for FAC

Setting	Description
Authorization Code Name	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; this name displays in the CDRs for calls that use this code.
Authorization Code	Enter a unique authorization code that is no more than 16 digits. The user enters this code when the user places a call through a FAC-enabled route pattern.
Authorization Level	Enter a three-digit authorization level that exists in the range of 0 to 255; the default equals 0. The level that you assign to the authorization code determines whether the user can route calls through FAC-enabled route patterns. To successfully route a call, the user authorization level must equal or be greater than the authorization level that is specified for the route pattern for the call.

Related Topics

Client Matter Codes and Forced Authorization Codes, on page 379
Configure Forced Authorization Codes, on page 386

Enable Forced Authorization Codes

Perform the following steps to enable FACs for route patterns:

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Call Routing** > **Route/Hunt** > **Route Pattern**.

Step 2 Perform one of the following tasks:

a) To update an existing route pattern, enter search criteria in the Find and List Route Pattern window, as described in the Cisco Unified Communications Manager Administration Guide.

b) To add a new route pattern, see the Cisco Unified Communications Manager Administration Guide.

Step 3 In the Route Pattern Configuration window, check the Require Forced Authorization Code check box.

Step 4 Click **Save.**

Tip Even if you do not check the Require Forced Authorization Code check box, you can specify the authorization level because the database stores the number that you specify.

Step 5 Repeat for all route patterns that require an authorization code.

Step 6 After you complete the route pattern configuration, see the Provide Information to Users, on page 388.

Provide Information to Users

After you configure the feature(s), communicate the following information to your users:

- Inform users about restrictions that are described in Interactions and Restrictions, on page 382.
- Provide users with all necessary information to use the features; for example, authorization code, authorization level, client matter code, and so on. Inform users that dialing a number produces a tone that prompts for the codes.
- For FAC, the system attributes calls that are placed with the user authorization code to the user or the user department. Advise users to memorize the authorization code or to keep a record of it in a secure location.
- Advise users of the types of calls that users can place; before a user notifies a phone administrator about a problem, users should hang up and retry the dialed number and code.
- Inform users that they can start entering the code before the tone completes.
- To immediately route the call after the user enters the code, the users can press # on the phone; otherwise, the call occurs after the interdigit timer (T302) expires; that is, after 15 seconds by default.
- The phone plays a reorder tone when the user enters an invalid code. If users misdial the code, the user must hang up and try the call again. If the reorder tone persists, users should notify the phone or system administrator that a problem may exist with the code.

CHAPTER 16

Custom Phone Rings

This chapter provides information about how you can customize the phone ring types that are available at your site by creating your own PCM files and editing the Ringlist.xml file.

Custom Phone Rings Description

Cisco Unified IP Phones ship with two default ring types that are implemented in hardware: Chirp1 and Chirp2. Cisco Unified Communications Manager also provides a default set of additional phone ring sounds that are implemented in software as pulse code modulation (PCM) files. The PCM files, along with an XML file (named Ringlist.xml) that describes the ring list options that are available at your site, exist in the TFTP directory on each Cisco Unified Communications Manager server.

You can get a copy of the Ringlist.xml file from the system using the following admin cli "file" commands:

- admin:file
    - file list*
    - file view*
    - file search*
    - file get*
    - file dump*
    - file tail*
    - file delete*

Customize and Modify Configuration Files

You can modify configuration files (for example, edit the xml files) and add customized files (for example, custom ring tones, call back tones, phone backgrounds) to the TFTP directory. You can modify files and/or add customized files to the TFTP directory in Cisco Unified Communications Operating System Administration, from the TFTP Server File Upload page. See the Cisco Unified Communications Operating System Administration Guide for information on how to upload files to the TFTP folder on a Cisco Unified Communications Manager server.

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.

PCM File Requirements for Custom Ring Types

The PCM files for the rings must meet the following requirements for proper playback on Cisco Unified IP Phones:

- Raw PCM (no header)
- 8000 samples per second
- 8 bits per sample
- mu-law compression
- Maximum ring size - 16080 samples
- Minimum ring size - 240 samples
- Number of samples in the ring evenly divisible by 240
- Ring starts and ends at the zero crossing.
- To create PCM files for custom phone rings, you can use any standard audio editing packages that support these file format requirements.

Configure a Custom Phone Ring

The following procedure applies to creating custom phone rings for only the Cisco Unified IP Phones 7940, 7960, and 7970.

Procedure

Step 1 Create a PCM file for each custom ring (one ring per file). Ensure that the PCM files comply with the format guidelines that are listed in the PCM File Requirements for Custom Ring Types, on page 391.

Step 2 Use an ASCII editor to edit the Ringlist.xml file. See the Ringlist.xml File Format Requirements, on page 390 for information on how to format this file, along with a sample Ringlist.xml file.

Step 3 Save your modifications and close the Ringlist.xml file.

Step 4 Upload the Ringlist.xml file by using the Cisco Unified Communications Operating System. See the Cisco Unified Communications Operating System Administration Guide.

Step 5 To cache the new Ringlist.xml file, stop and start the TFTP service by using Cisco Unified Serviceability or disable and reenable the “Enable Caching of Constant and Bin Files at Startup” TFTP service parameter (located in the Advanced Service Parameters).

CHAPTER 17

Device Mobility

This chapter provides information about device mobility, which allows Cisco Unified Communications Manager to determine whether the phone is at its home location or at a roaming location. Cisco Unified Communications Manager uses the device IP subnets to determine the exact location of the phone. By enabling device mobility within a cluster, mobile users can roam from one site to another and acquire the site-specific settings. Cisco Unified Communications Manager then uses these dynamically allocated settings for call routing, codec section, media resource selection, and so forth.

With Cisco Unified Communications Manager, a site or a physical location gets identified by using various settings, such as locations, regions, calling search spaces, and media resources. Cisco Unified IP Phones that reside at a particular site get statically configured with these settings, and Cisco Unified Communications Manager uses these settings for proper call establishment, call routing, media resource selection, and so forth. However, when phones get moved from the home location to a remote location, these phones retain the home settings that are statically configured on the phones. Cisco Unified Communications Manager uses these home settings for the phones that are located at the remote site, which may cause problems with call routing, codec selection, media resource selection, and other call processing functions.

Configure Device Mobility

With Cisco Unified Communications Manager, a site or a physical location gets identified by using various settings, such as locations, regions, calling search spaces, and media resources. Cisco Unified IP Phones that reside at a particular site get statically configured with these settings, and Cisco Unified Communications Manager uses these settings for proper call establishment, call routing, media resource selection, and so forth. However, when phones get moved from the home location to a remote location, these phones retain the home settings that are statically configured on the phones. Cisco Unified Communications Manager uses these home settings for the phones that are located at the remote site, which may cause problems with call routing, codec selection, media resource selection, and other call processing functions.

You can configure device mobility, which allows Cisco Unified Communications Manager to determine whether the phone is at its home location or at a roaming location. Cisco Unified Communications Manager uses the device IP subnets to determine the exact location of the phone. By enabling device mobility, mobile users can roam from one site to another and acquire the site-specific settings. Cisco Unified Communications Manager then uses these dynamically allocated settings for call routing, codec section, media resource selection, and so forth.

For more information on device mobility, see the Device Mobility Feature, on page 394 and the Device Mobility, on page 393.

Perform the following steps to configure device mobility.

Procedure

Step 1 Review the related device mobility documentation.

Tip For information on dial plan design considerations, see the Cisco Unified Communications Solution Reference Network Design (SRND), which provides information on building class of service if you use device mobility.

Step 2 Enable the device mobility mode in the Service Parameter Configuration or Phone Configuration window. (**System** > **Service Parameters** (choose Cisco CallManager service) or **Device** > **Phone**)

Step 3 Configure physical locations. (**System** > **Physical Location**)

Step 4 Configure device mobility groups. (**System** > **Device Mobility** > **Device Mobility Groups**)

Step 5 Configure subnets and assign one or more device pools to a subnet in the Device Mobility Info Configuration window. (**System** > **Device Mobility** > **Device Mobility Info**)

Step 6 In the Device Pool Configuration window, update your device pools for device mobility settings, if you have not already done so. (**System** > **Device Pool**)

Step 7 If you have not already done so, update your dial plans for device mobility; for example, update calling search spaces, AAR group settings, and so on. (**Call Routing** > **...**)

Related Topics

Device Mobility, on page 393
View Roaming Device Pool Parameters, on page 411
Configure a Physical location, on page 404
Configure a Device Mobility Group, on page 406
Physical Location Configuration, on page 404
Device Mobility Group Configuration, on page 407
Configure Device Mobility Information, on page 409
Device Mobility Information Configuration, on page 409
Configure Device Pools for Device Mobility, on page 411

Device Mobility Feature

With Cisco Unified Communications Manager, a site or a physical location gets identified by using various settings, such as locations, regions, calling search spaces, and media resources. Cisco Unified IP Phones that reside at a particular site get statically configured with these settings, and Cisco Unified Communications

Manager uses these settings for proper call establishment, call routing, media resource selection, and so forth. However, when phones get moved from the home location to a remote location, these phones retain the home settings that are statically configured on the phones. Cisco Unified Communications Manager uses these home settings for the phones that are located at the remote site, which may cause problems with call routing, codec selection, media resource selection, and other call processing functions.

You can configure device mobility, which allows Cisco Unified Communications Manager to determine whether the phone is at its home location or at a roaming location. Cisco Unified Communications Manager uses the device IP subnets to determine the exact location of the phone. By enabling device mobility within a cluster, mobile users can roam from one site to another and acquire the site-specific settings. Cisco Unified Communications Manager then uses these dynamically allocated settings for call routing, codec section, media resource selection, and so forth.

The dynamically reconfigured location settings ensure that voice quality and allocation of resources are appropriate for the new phone location:

- When a mobile user moves to another location, call admission control (CAC) can ensure video and audio quality with the appropriate bandwidth allocations.
- When a mobile user makes a PSTN call, the phone can access the local gateway instead of the home gateway.
- When a mobile user calls the home location, Cisco Unified Communications Manager can assign the appropriate codec for the region.

Device Mobility Description

When a phone device has mobility mode enabled, Cisco Unified Communications Manager uses the IP address of the registering device to find the proper location settings. The system compares the physical location that is configured in the device pool for the IP subnet and for the device to determine when a phone is away from its home location.

For example, phone A in Richardson with an IP address 10.81.17.9 registers with Cisco Unified Communications Manager. This IP address maps to subnet 10.81.16.0/16. Cisco Unified Communications Manager checks the device pool settings for the device and the subnet in the database. The physical location setting for the device pool in the phone record matches the physical location setting for the device pool in the subnet. The system considers the phone to be in its home location and uses the configuration settings in the phone record.

If phone A moves to Boulder, the phone queries the local DHCP server and gets an IP address of 130.5.5.25, which maps to subnet 130.5.5.0/8. Cisco Unified Communications Manager compares the physical location for the device pool in the phone record to the device pool location setting that is configured for the subnet. The system determines that the device is roaming because the physical locations do not match. Cisco Unified Communications Manager overwrites the phone record configuration settings with configuration settings for the subnet, downloads the settings in a new configuration file, and resets the device. The phone reregisters with the settings from the roaming device pool.

Note The phone must have a dynamic IP address to use device mobility. If a phone with a static IP address roams, Cisco Unified Communications Manager uses the configuration settings from its home location.

For roaming devices, Cisco Unified Communications Manager overwrites the following device pool parameters with the device pool settings for the subnet:

- Date/Time Group
- Region
- Location
- Network Locale
- SRST Reference
- Connection Monitor Duration
- Physical Location
- Device Mobility Group
- Media Resource Group List

When networks span geographic locations outside the United States, you can configure device mobility groups to allow phone users to use their configured dial plan no matter where they roam. When a device is roaming but remains in the same device mobility group, Cisco Unified Communications Manager also overwrites the following device pool parameters:

- AAR Group
- AAR Calling Search Space
- Device Calling Search Space

When the phone returns to its home location, the system disassociates the roaming device pool, downloads the configuration settings for home location, and resets the device. The device registers with the home location configuration settings.

Tip Cisco Unified Communications Manager always uses the Communications Manager Group setting from the phone record. The device always registers to its home location Cisco Unified Communications Manager server even when roaming. When a phone is roaming, only network location settings such as bandwidth allocation, media resource allocation, region configuration, and AAR group get changed.

Device Mobility Operations Summary

This section describes how Cisco Unified Communications Manager manages phone registration and assignment of parameters for device mobility.

Following initialization, the device mobility feature operates according to the following process:

1. A phone device record gets created for an IP phone that is provisioned to be mobile, and the phone gets assigned to a device pool. The phone registers with Cisco Unified Communications Manager, and an IP address gets assigned as part of the registration process.
2. Cisco Unified Communications Manager compares the IP address of the device to the subnets that are configured for 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.

3. If the device pool in the phone record matches the device pool in the matching subnet, the system considers the phone to be in its home location, and the phone retains the parameters of its home device pool.
4. If the device pool in the phone record does not match the device pools in the matching subnet, the system considers the phone to be roaming. The following table describes possible scenarios for device mobility and the system responses.

Table 43: Device Mobility Scenarios

Scenario	System Response
The physical location setting in the phone device pool matches the physical location setting in a device pool that is associated with the matching subnet. **Note** Although the phone may have moved from one subnet to another, the physical location and associated services have not changed.	The system does not consider the phone to be roaming, and the system uses the settings in the home location device pool.
The matching subnet has a single device pool that is assigned to it; the subnet device pool differs from the home location device pool, and the physical locations differ.	The system considers the phone to be roaming. It reregisters with the parameters of the device pool for the matching subnet.
The physical locations differ, and the matching subnet has multiple device pools assigned to it.	The system considers the phone to be roaming. The new device pool gets assigned according to a round-robin rule. Each time that a roaming devices comes in to be registered for the subnet, the next device pool in the set of available device pools gets assigned.
Physical location gets defined for the home device pool but is not defined for the device pools that are associated with the matching subnet	The physical location has not changed, so the phone remains registered in the home device pool.
Physical location that is not defined for the home device pool gets defined for the device pools that are associated with the matching subnet	The system considers the phone to be roaming to the defined physical location, and it registers with the parameters of the device pool for the matching subnet.
A subnet gets updated or removed.	The rules for roaming and assigning device pools get applied by using the remaining subnets.

Device Mobility Groups Operations Summary

You can use device mobility groups to determine when a device moves to another location within a geographic entity, so a user can use its own dial plan. For example, you can configure a device mobility group for the

United States and another group for the United Kingdom. If a phone moves into a different mobility group (such as from the United States to the United Kingdom), Unified Communications Manager uses the Calling Search Space, AAR Group and AAR CSS from the phone record, and not from the roaming location.

If the device moves to another location with same mobility group (for example, Richardson, USA, to Boulder, USA), the CSS information gets taken from the roaming device pool settings. With this approach, if the user is dialing PSTN destinations, the user reaches the local gateway.

The following table describes the device pool parameters that the system uses for various scenarios.

Table 44: Device Mobility Group Scenarios

Scenario	Parameters Used
A roaming device moves to another location in the same device mobility group.	Roaming Device Pool: yes Location: Roaming device pool setting Region: Roaming device pool setting Media Resources Group List: Roaming device pool setting Device CSS: Roaming device pool setting (Device Mobility CSS) AAR Group: Roaming device pool setting AAR CSS: Roaming device pool setting
A roaming device moves to another location in a different device mobility group.	Roaming Device Pool: yes Location: Roaming device pool setting Region: Roaming device pool setting Media Resources Group List: Roaming device pool setting Device CSS: Home location settings AAR Group: Home location settings AAR CSS: Home location settings
A device roams, and a device mobility group does not get defined for the home or roaming device pool.	Because the device is roaming, it takes the roaming device pool settings, including the Device Mobility Calling Search Space, AAR Calling Search Space, and AAR Group.

Network Considerations

The device mobility structure accommodates different network configurations.

For efficient device mobility design, divide the network into device mobility groups (optional), physical locations, and subnets. The number and levels of groups in the hierarchy depend on the size and complexity of the organization.

- Device mobility groups represent the top-level geographic entities in your network. The device mobility group setting determines whether the device is moved within the same geographical entity, primarily to allow users to keep their own dial plans. The device mobility group defines a logical group of sites with similar dialing patterns (for example, US_dmg and EUR_dmg). For example, if you want a roaming device to access the local gateway for PSTN calls, be sure that the device mobility group for the home location device pool and roaming location device pool are the same.

Device mobility groups could represent countries, regions, states or provinces, cities, or other entities. An enterprise with a worldwide network might choose device mobility groups that represent individual countries, whereas an enterprise with a national or regional network might define device mobility groups that represent states, provinces, or cities. The system does not require defining device mobility groups to use the device mobility feature.

- Physical location, the next level in the hierarchy, identifies a geographic location for device pool parameters that are location-based, such as date/time, region, and so on. Cisco Unified Communications Manager uses the geographic location to determine which network resources to assign to a phone. If a user moves away from the home location, the system ensures that the phone user uses local media resources and the correct bandwidth for the call.

  For example, a Music on Hold (MOH) server may serve a specific office or campus within the enterprise. When a device roams to another office or campus and reregisters with Cisco Unified Communications Manager, having the device served by the MOH server at the roaming location represents best practice.

  By defining the physical location according to availability of services such as MOH, you can assure efficient and cost-effective reassignment of services as devices move from one physical location to another. Depending upon the network structure and allocation of services, you can define physical locations based upon city, enterprise campus, or building.

  Ideally, your network configuration places each network in one physical location, so a network can be mapped to a single physical location.

- A subnet may include all the devices at a geographical location, within the same building, or on the same LAN. You can configure one or more device pools, including device mobility group and physical location, for a subnet.

- Location identifies the CAC for a centralized call-processing system. You configure a location for a phone and a device pool. See the *Cisco Unified Communications Manager System Guide* for more information.

Tip For information on dial plan design considerations, see the *Cisco Unified Communications Solution Reference Network Design (SRND)*, which provides information on building class of service if you use device mobility.

Interactions and Restrictions

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 displays on the phone. For information on how calling party normalization works with device mobility, see the Calling Party Normalization Interactions and Restrictions, on page 203 in the Calling Party Normalization, on page 193 chapter.

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 device mobility.
- If the device is assigned an IP address by using NAT/PAT, the IP address that is provided during registration may not match the actual IP address of the device.

IPv6 and Device Mobility

Device mobility supports IPv4 addresses only, so you cannot use phones with an IP Addressing Mode of IPv6 Only with device mobility. For more information on IPv6, see the Internet Protocol Version 6 (IPv6), on page 739.

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 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 get 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 get used as the CFA CSS.
- If the device is roaming within a different device mobility group, the Device CSS and Line CSS get used as the CFA CSS.

For more information about configuration options for "Call Forward All", see the *Cisco Unified Communications Manager Administration Guide* and the *Cisco Unified Communications Manager System Guide*.

System Requirements

Device Mobility requires the following software components:

- Cisco CallManager service running on at least one server in the cluster
- Cisco CallManager service running on the server
- Cisco Database Layer Monitor service running on the same server as the Cisco CallManager service
- Cisco TFTP service running on at least one server in the cluster
- Cisco TFTP service running on the server
- Cisco Unified Communications Manager Locale Installer (if you want to use non-English phone locales or country-specific tones)

Any phone that is running either SCCP or SIP and that can be configured in Cisco Unified Communications Manager Administration supports device mobility, including

- Cisco Unified IP Phone 6900 series (except 6901 and 6911)
- Cisco Unified IP Phone 7900 series
- Cisco Unified IP Phone 8900 series

- Cisco Unified IP Phone 9900 series
- Computer Telephony Integration (CTI) Ports
- Cisco IP Communicator

For more information about IP Phones and the device mobility feature, see the user guide for your phone model.

Install Device Mobility

Device mobility automatically installs when you install Cisco Unified Communications Manager. After you install Cisco Unified Communications Manager, you must configure device mobility settings in Cisco Unified Communications Manager Administration to enable the feature.

Note Existing device pools automatically migrate to the new device pool and common profile structure as part of the upgrade to Cisco Unified Communications Manager Release 6.0 or later.

Configure Device Mobility

For successful configuration of the Device Mobility feature, review the network design considerations, review the steps in the configuration summary task, perform the configuration requirements, and activate the Cisco CallManager service, if it is not already activated.

This section provides information to configure and enable Device Mobility, including configuring device pools for device mobility, physical location parameters, Device Mobility groups, and other Device Mobility information parameters. Instructions to delete Device Mobility information is also provided.

Tip Before you configure device mobility, review the configuration summary task for Device Mobility.

Related Topics

Configure Device Mobility, on page 393

Configuration Tips for Device Mobility

Consider the following information when you configure device mobility in Cisco Unified Communications Manager Administration:

- When the Device Mobility Mode is set to Default in the Phone Configuration window, the Device Mobility Mode service parameter determines whether the device is enabled for the device mobility feature.
- Cisco Unified Communications Manager uses the longest match rule to match IP addresses and subnets, meaning the best match uses the largest number of bits in the IP subnet mask. 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.

- If no device mobility information entries match the device IP address, the device uses the home location device pool settings.
- You assign the device pool to the phone device in the Phone Configuration window; you assign device pools to subnets in the Device Mobility Info Configuration window.
- You can assign one or more device pools to a subnet address. Cisco Unified Communications Manager assigns device pools for the same subnet to roaming devices in round-robin fashion; for example, roaming device 1 gets assigned the first device pool in the list, and roaming device 2 gets assigned the second device pool in the list. This process allows you to load share when you expect a large number of phones to roam into an area, such as a meeting in the head office that employees from all branch locations will attend.
- Although physical location does not represent a required setting in the Device Pool Configuration window, you must define a physical location for a device pool to use the device mobility feature. Be sure to configure physical location for the home location device pool and for the roaming device pool.
- After the device mobility structure is in place, you can turn device mobility on for IP phones that support device mobility.

Enable Device Mobility

This section describes the procedure to enable the device mobility feature in the Service Parameter or Phone Configuration window.

Consider the following information when enabling the device mobility feature:

- When device mobility mode is enabled or disabled, the setting applies to all phones for the server that support device mobility.
- At installation, the default setting for the Device Mobility Mode service parameter specifies Off, which means that device mobility is disabled.
- When device mobility mode is enabled or disabled in the Phone Configuration window, the Device Mobility Mode phone settings take precedence over the service parameter setting.
- When the phone setting for Device Mobility Mode equals Default, Cisco Unified Communications Manager uses the service parameter setting for the device.

Procedure

Step 1 To enable the Device Mobility service parameter, perform the following tasks:

a) Choose **System** > **Service Parameters** in Cisco Unified Communications Manager Administration.
b) From the Server drop-down list box, select the server that is running the Cisco CallManager service.
c) From the Service drop-down list box, select the Cisco CallManager service. The Service Parameters Configuration window displays.
d) To enable the Device Mobility Mode service parameter, choose **On.**

Step 2 To configure the Device Mobility Mode setting for a specific phone, perform the following tasks:

a) Choose **Device** > **Phone** in Cisco Unified Communications Manager Administration.
b) Click **Find** to display the device pools list, or use the search results from an active query.
c) Choose a device from the phone list that displays in the Find and List Phones window. The Phone Configuration window displays.

d) In the Device Mobility Mode drop-down list box, choose On to enable device mobility, choose **Off** to disable device mobility, or choose **Default**, which ensures that the phone uses the configuration from the Device Mobility Mode service parameter.

Find a Physical Location

Because you may have several physical locations in your network, Cisco Unified Communications Manager lets you locate specific physical locations on the basis of specific criteria. Use the following procedure to locate physical locations.

Note During your work in a browser session, Cisco Unified Communications Manager Administration retains your physical location search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your physical location search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **System** > **Physical Location**.

The Find and List Physical Locations window displays. Records from an active (prior) query may also display in the window.

Step 2 To filter or search records:

a) From the first drop-down list box, select a search parameter.
b) From the second drop-down list box, select a search pattern.
c) Specify the appropriate search text, if applicable.

Note To add additional search criteria, click the **+** button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the **–** button to remove the last added criterion or click the **Clear Filter** button to remove all added search criteria.

Step 3 To find all records in the database, ensure the dialog box is empty, click **Find.**

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

Note You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking **Delete Selected**. You can delete all configurable records for this selection by clicking Select All and then clicking Delete Selected.

Step 4 From the list of records that display, click the link for the record that you want to view.

Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Configure a Physical location

To add a physical location for a device pool, use the following procedure.

Procedure

Step 1 Choose **System** > **Physical Location**.

The Find and List Physical Locations window displays.

Step 2 Perform one of the following tasks:

a) To copy an existing physical location, locate the appropriate physical location as described in the Find a Physical Location, on page 403, and click the **Copy** button next to the physical location that you want to copy.

b) To add a new physical location, click the **Add New** button.

c) To update an existing physical location, locate the appropriate physical location as described in Find a Physical Location, on page 403.

Step 3 Enter the appropriate settings as described in Device Mobility Group Configuration, on page 407.

Step 4 To save the physical location information in the database, click **Save.**

Physical Location Configuration

A physical location, which is used with the device mobility feature, identifies a geographic location for device pool parameters that are location-based, such as date/time, region, and so on. Cisco Unified Communications Manager uses the geographic location to determine which network resources to assign to a phone. If a user moves away from the home location, the system ensures that the phone user uses local media resources and the correct bandwidth for the call.

For example, a Music on Hold (MOH) server may serve a specific office or campus within the enterprise. When a device roams to another office or campus and reregisters with Cisco Unified Communications Manager, having the device served by the MOH server at the roaming location represents best practice.

By defining the physical location according to availability of services such as MOH, you can assure efficient and cost-effective reassignment of services as devices move from one physical location to another. Depending upon the network structure and allocation of services, you can define physical locations based upon city, enterprise campus, or building.

Ideally, your network configuration places each network in one physical location, so a network can be mapped to a single physical location. Depending upon the network structure and allocation of services, you may define physical locations based upon a city, enterprise campus, or building.

The following table describes the physical location configuration settings. For related procedures, see the Device Mobility, on page 393.

Table 45: Physical Location Configuration Settings

Field	Description
Physical Location Information	
Name	Enter a name to identify the physical location. The name can contain up to 50 alphanumeric characters with any combination of spaces, periods (.), hyphens (-), underscore characters (_).
Description	Enter text describing the physical location. The description can include up to 50 characters in any language, but it cannot include double-quotes (“), percentage sign (%), ampersand (&), or angle brackets (<>).

Delete a Physical Location

If a physical location is currently used in a device pool, you cannot delete it. To delete the physical location, you can first find the associated device pools from the dependency record and disassociate them before deleting the physical location.

To delete a physical location, use the following procedure.

Procedure

Step 1 To locate the physical location that you want to delete, follow the procedure on Find a Physical Location, on page 403.

Step 2 Check the check box next to the physical locations that you want to delete. To select all the physical locations in the window, check the check box in the matching records title bar.

Step 3 Click **Delete Selected**.

Step 4 To confirm your selection, click **OK.**

Find Device Mobility Groups

Because you may have several device mobility groups in your network, Cisco Unified Communications Manager lets you locate specific device mobility groups on the basis of specific criteria. Use the following procedure to locate device mobility groups.

Note During your work in a browser session, Cisco Unified Communications Manager Administration retains your device mobility group search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your device mobility group search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **System** > **Device Mobility** > **Device Mobility Group**.

The Find and List Device Mobility Groups window displays. Records from an active (prior) query may also display in the window.

Step 2 To filter or search records

a) From the first drop-down list box, select a search parameter.
b) From the second drop-down list box, select a search pattern.
c) Specify the appropriate search text, if applicable.

Note To add additional search criteria, click the **+** button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the **–** button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

Step 3 To find all records in the database, ensure the dialog box is empty, click **Find.**

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

Note You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking **Delete Selected**. You can delete all configurable records for this selection by clicking **Select All** and then clicking **Delete Selected**.

Step 4 From the list of records that display, click the link for the record that you want to view.

Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Configure a Device Mobility Group

To configure a device mobility group, which supports the device mobility feature, use the following procedure.

Procedure

Step 1 Choose **System** > **Device Mobility** > **Device Mobility Group**.

The Find and List Device Mobility Groups window displays.

Step 2 Perform one of the following tasks:

a) To copy an existing device mobility group, locate the appropriate device mobility group as described in the Find Device Mobility Groups, on page 405, click the **Copy** button next to the device mobility group that you want to copy.
b) To add a new device mobility group, click the **Add New** button.
c) To update an existing device mobility group, locate the appropriate device mobility group as described in the Find Device Mobility Groups, on page 405.

Step 3 Enter the appropriate fields as described in Device Mobility Group Configuration, on page 407.

Step 4 Click **Save** to save the device mobility group information to the database.

Device Mobility Group Configuration

Device mobility groups support the device mobility feature. Device mobility groups represent the highest level geographic entities in your network. Depending upon the network size and scope, your device mobility groups could represent countries, regions, states or provinces, cities, or other entities. For example, an enterprise with a worldwide network might choose device mobility groups that represent individual countries, whereas an enterprise with a national or regional network might define device mobility groups that represent states, provinces, or cities.

Tip The device mobility group defines a logical group of sites with similar dialing patterns (for example, US_dmg and EUR_dmg).

The following table describes the device mobility group configuration settings. For related procedures, see the Device Mobility, on page 393.

Table 46: Device Mobility Group Configuration Settings

Field	Description
Device Mobility Group Information	
Name	Enter a name to identify the device mobility group.
Description	Enter the description of the profile. The description can include up to 50 characters in any language, but it cannot include double-quotes (“), percentage sign (%), ampersand (&), or angle brackets (<>).

Delete a Device Mobility Group

If a device mobility group is currently used in a device pool, you cannot delete it. To delete the device mobility group, you must find the associated device pools from the dependency record, disassociate them, and then delete the device mobility group.

Procedure

Step 1 To locate the device mobility group that you want to delete, follow the procedure in Find Device Mobility Groups, on page 405.

Step 2 Check the check box next to the device mobility groups that you want to delete. To select all the device mobility groups in the window, check the check box in the matching records title bar.

Step 3 Click **Delete Selected**.

Step 4 To confirm your selection, click **OK**.

Find Device Mobility Information

Because you may have several device mobility info records in your network, Cisco Unified Communications Manager lets you locate specific device mobility information on the basis of specific criteria. Use the following procedure to locate device mobility information.

Note During your work in a browser session, Cisco Unified Communications Manager Administration retains your device mobility info search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your device mobility info search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **System** > **Device Mobility** > **Device Mobility Info**.

The Find and List Device Mobility Infos window displays. Records from an active (prior) query may also display in the window.

Step 2 To filter or search records

a) From the first drop-down list box, select a search parameter.
b) From the second drop-down list box, select a search pattern.
c) Specify the appropriate search text, if applicable.

Note To add additional seTo find all records in the database, ensure the dialog box is emptyarch criteria, click the **+** button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the **–** button to remove the last added criterion or click the **Clear Filter** button to remove all added search criteria.

Step 3 To find all records in the database, ensure the dialog box is empty, click **Find.**

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

Note You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking **Delete Selected**. You can delete all configurable records for this selection by clicking **Select All** and then clicking **Delete Selected**.

Step 4 From the list of records that display, click the link for the record that you want to view.

Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Configure Device Mobility Information

To add device mobility information, use the following procedure.

Procedure

Step 1 Choose **System** > **Device Mobility** > **Device Mobility Info**.

The Find and List Device Mobility Infos window displays.

Step 2 Perform one of the following tasks:

a) To copy an existing device mobility info, locate the appropriate device mobility info as described in the Find Device Mobility Information, on page 408, click the **Copy** button next to the device mobility info that you want to copy.
b) To add a new device mobility info, click the **Add New** button.
c) To update an existing device mobility info, locate the appropriate device mobility info as described in the Find Device Mobility Information, on page 408.

Step 3 Enter the appropriate fields as described in Device Mobility Group Configuration, on page 407.

Step 4 To save the device mobility info information to the database, click **Save.**

Device Mobility Information Configuration

The Device Mobility Info Configuration window specifies the subnets and device pools that are used for device mobility. When a phone registers with Cisco Unified Communications Manager, the system compares the IP address of the device to the subnets that are configured for 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.

If the device pool in the phone record matches the device pool in the matching subnet, the system considers the phone to be in its home location, and the phone retains the parameters of its home device pool.

If the device pool in the phone record does not match the device pools in the matching subnet, the system considers the phone to be roaming. Device Mobility Operations Summary, on page 396 describes possible scenarios for device mobility and the system responses.

The following table describes the device mobility info configuration settings. For related procedures, see the Device Mobility, on page 393.

Table 47: Device Mobility Info Configuration Settings

Field	**Description**
Device Mobility Info Information	
Name	Enter a name to identify the device mobility info record.
Subnet	Enter the device mobility subnet in dotted decimal format; for example, xxx.xxx.xxx.xxx.

Field	Description
Subnet Mask (bits size)*	Enter the device mobility subnet mask. Based on the bit mask, this value represents the number of IP addresses that are included in this subnet; for example, 24, which represents a standard class C subnet bit mask. The value does not need to match the subnet mask on the phone.
Device Pools for This Device Mobility Info	
Available Device Pools	Choose a device pool in the Available Device Pools list box by clicking the down arrow button between the two list boxes. To add multiple device pools that are listed consecutively, click the first device pool in the range; then, hold down the Shift key while clicking the last device pool in the range. Click the down arrow button between the two list boxes to add the device pools. To add multiple device pools that are not listed consecutively, hold down the Control (Ctrl) key while clicking device pools. Click the down arrow button between the two list boxes to add the chosen device pools.
Selected Device Pools	Select any device pools that you would like to remove from the device mobility record and double-click or use the up arrow to move the device pool back to the Available Device Pools field.

Delete a Device Mobility Information

If you delete a device mobility info that is currently used by a device, Cisco Unified Communications Manager reapplies the appropriate device mobility rules according to the descriptions in the Device Mobility, on page 393 chapter.

To delete a device mobility info record, use the following procedure.

Procedure

Step 1 To locate the device mobility info that you want to delete, follow the procedure in the Find Device Mobility Information, on page 408.

Step 2 Check the check box next to the device mobility record that you want to delete. To select all the records in the window, check the check box in the matching records title bar.

Step 3 Click **Delete Selected**.

Step 4 To confirm your selection, click **OK**.

Configure Device Pools for Device Mobility

The roaming sensitive settings in the Device Pool Configuration window override the device-level settings when the device roams within or outside a of device mobility group. The settings, which include Date/time Group, Region, Media Resource Group List, Location, Network Locale, SRST Reference, Physical Location, Device Mobility Group, and so on, provide call admission control and voice codec selection. Additionally, these settings update the media resource group list (MRGL), so appropriate remote media resources get used for music on hold, conferencing, transcoding, and so on. The roaming sensitive settings also update the Survivable Remote Site Telephony (SRST) gateway. Mobile users register to a different SRST gateway while roaming. This registration may affect the dialing behavior when the roaming phones are in SRST mode.

The device mobility related parameters in the Device Pool Configuration window override the device-level settings only when the device is roaming within a device mobility group. The device mobility related settings affect the dial plan because the calling search space dictates the patterns that can be dialed or the devices that can be reached.

See the Cisco Unified Communications Manager Administration Guide to configure device pool parameters.

View Roaming Device Pool Parameters

When the phone has device mobility mode enabled, you can view the roaming device pool settings by clicking View Current Device Mobility Settings next to the Device Mobility Mode field in the Phone Configuration window. If the device is not roaming, the home location settings display.

CHAPTER 18

Do Not Disturb

This chapter provides information about the Do Not Disturb (DND) feature which provides the following options:

- 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.

Users can configure DND directly from their Cisco Unified IP Phone or from the Cisco Unified Communications Self Care Portal.

Configure Do Not Disturb

The Do Not Disturb (DND) feature provides the following options:

- 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.

When DND is enabled, all new incoming calls with normal priority will honor the DND settings for the device. High-priority calls, such as Cisco Emergency Responder (CER) calls or calls with Multi-Level Precedence & Preemption (MLPP), will ring on the device. Also, when you enable DND, the Auto Answer feature gets disabled.

Procedure

Step 1 Configure DND service parameters.

Step 2 Configure DND softkeys.

Step 3 Configure DND feature button.

Step 4 Configure device-based DND parameters.

Step 5 Configure phone profile settings.

Related Topics

Set the Do Not Disturb Service Parameters, on page 419
Configure DND Softkeys, on page 420
Configure Device Parameters for DND, on page 420
Add DND to Common Phone Profiles, on page 422
Do Not Disturb Feature, on page 414

Do Not Disturb Feature

When DND is enabled, all new incoming calls with normal priority will honor the DND settings for the device. High-priority calls, such as Cisco Emergency Responder (CER) calls or calls with Multi-Level Precedence & Preemption (MLPP), will ring on the device. Also, when you enable DND, the Auto Answer feature gets disabled.

The user can enable and disable DND by any of the following methods:

- Softkey
- Feature button
- Cisco Unified Communications Self Care Portal

You can also enable and disable DND on a per-phone basis in Cisco Unified Communications Manager Administration.

When you enable DND, the Cisco Unified IP Phone displays the message Do Not Disturb is active. when DND is active. Some Cisco Unified IP Phones display DND status icons. For more information about Cisco Unified IP Phones and the DND feature, see the user guides for that IP phone.

Call Alert Settings

DND incoming call alert settings determine how the incoming call alert gets presented to the user when DND Ringer Off or DND Call Reject is enabled. The following list gives the available 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.

You can configure DND Incoming Call Alert on a per-device basis and also configure it on the Common Phone Profile window for group settings. If you do not set up the configuration at the device level, the Common Phone Profile settings get used.

Do Not Disturb Architecture

This section provides an overview of DND architecture for both SIP and SCCP devices.

DND Status Notification for SIP Devices

Cisco Unified Communications Manager supports Do Not Disturb that a SIP device initiates or that a Cisco Unified Communications Manager device initiates. A DND status change gets signaled from a SIP device to Cisco Unified Communications Manager by using the SIP PUBLISH method (RFC3909). A DND status change gets signaled from a Cisco Unified Communications Manager to a SIP device by using a dndupdate Remote-cc REFER request. Cisco Unified Communications Manager can also publish the Do Not Disturb status for a device, along with the busy and idle status for the device.

DND Status Notification for SCCP Devices

Cisco Skinny Client Control Protocol (SCCP) supports Do Not Disturb requests that an SCCP device initiates or that a Cisco Unified Communications Manager device initiates. A DND status change gets signaled from an SCCP device to Cisco Unified Communications Manager by using SCCP messaging.

System Requirements for Do Not Disturb

This section provides software and hardware requirement for Do Not Disturb.

Software Requirements

To operate, the Do Not Disturb feature requires the following software components:

- Cisco Unified Communications Manager Release 6.0(1) or later

Hardware Requirements

The following Cisco Unified IP Phones support the Do Not Disturb feature:

- Cisco Unified IP Phone 6900 series (except 6901 and 6911)
- Cisco Unified IP Phone 7900 series
- Cisco Unified IP Phone 8900 series
- Cisco Unified IP Phone 9900 series

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 window.

For more information about Cisco Unified IP Phones and the DND feature, see the user documentation for your phone model.

Determine Device Support for Do Not Disturb

Use the Cisco Unified Reporting application to generate a complete list of devices that support Do Not Disturb. To do so, follow these steps:

For additional information about the Cisco Unified Reporting application, see the *Cisco Unified Reporting Administration Guide*.

Procedure

Step 1 Start Cisco Unified Reporting by using any of the methods that follow.

The system uses the Cisco Tomcat service to authenticate users before allowing access to the web application. You can access the application

- by choosing Cisco Unified Reporting in the Navigation menu in Cisco Unified Communications Manager Administration and clicking **Go.**
- by choosing File > Cisco Unified Reporting at the Cisco Unified Real Time Monitoring Tool (RTMT) menu.
- by entering `https://<server name or IP address>:8443/cucreports/` and then entering your authorized username and password.

Step 2 Click **System Reports** in the navigation bar.

Step 3 In the list of reports that displays in the left column, click the Unified CM Phone Feature List option.

Step 4 Click the Generate a new report link to generate a new report, or click the Unified CM Phone Feature List link if a report already exists.

Step 5 To generate a report of all devices that support DND, choose these settings from the respective drop-down list boxes and click the **Submit** button:

Product: All

Feature: Do Not Disturb

The List Features pane displays a list of all devices that support the DND. You can click on the Up and Down arrows next to the column headers (Product or Protocol) to sort the list.

Do Not Disturb Interactions and Restrictions

This section provides information about Do Not Disturb interactions and restrictions.

Interactions

This section describes how the Do Not Disturb feature interacts with Cisco Unified Communications Manager applications and call processing features.

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 voicemail messages, which allows the user to know when DND is active. 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 (both options). If Phone A has DND turned on and parked a call, the park reversion to Phone A will occur normally and will ring Phone A.

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 will not ring and will honor the DND settings.
- If Phone A activates DND Call Reject, the park reversion call will not be presented to Phone A.

Pickup

For a locally placed Pickup request, Pickup overrides DND (both options). If Phone A has DND turned on and has initiated any type of Pickup, the Pickup call would be presented normally, and it will ring Phone A.

For a remotely placed Pickup request, DND overrides Pickup.

- If Phone A (with DND Ringer Off activated) shares a line with Phone A-prime, when Phone A-prime initiates Pickup, the Pickup call to Phone A will not ring and will honor DND settings.
- If Phone A is in DND Call Reject mode, the Pickup call will not be presented to Phone A.

Hold Reversion and Intercom

Hold reversion and intercom override DND (both options), and the call gets presented normally.

MLPP and CER

MLPP (phones that are running SCCP) and CER calls override DND (both options). MLPP and CER calls get presented normally, and the phone will ring.

Call Back

For the originating side, callback overrides DND. When the activating device is on DND mode (both options), the callback notification (both audio and visual) will still be presented to the user.

For the terminating side, DND overrides callback:

- When the terminating side is on DND Ringer Off, the Callback Available screen will be sent after the terminating side goes off hook and on hook.
- When the terminating side is on DND Call Reject and is available (goes off hook and on hook), a new screen will be 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 will be 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 will get still presented to the user when a call gets made to that Hunt List. 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

Install and Activate Do Not Disturb

Do Not Disturb, a system feature, comes standard with Cisco Unified Communications Manager software. It does not require special installation.

Configure Do Not Disturb

This section describes the procedures for configuring the Do Not Disturb feature.

Tip Before you configure the Do Not Disturb feature, review the configuration summary task for DND.

Related Topics

Configure Do Not Disturb, on page 413

Set the Do Not Disturb Service Parameters

Cisco Unified Communications Manager provides one systemwide service parameter for Do Not Disturb: BLF Status Depicts DND. This parameter determines whether DND status is considered in the Busy Lamp Field (BLF) status calculation, and you can set the parameter to True or False.

- When you specify True for BLF Status Depicts DND and DND is activated on the device, the BLF status indicator for the device or line appearance reflects the DND state.
- When you specify False for BLF Status Depicts DND and DND is activated on the device, the BLF status indicator for the device or line appearance reflects the actual device state.

When BLF Status Depicts DND is enabled or disabled for the cluster, the cluster setting applies to all phones on the server that support DND.

Note To set this service parameter, navigate to System > Service Parameters and choose the Cisco CallManager service for the server that you want to configure. Specify the desired state for BLF Status Depicts DND in the Clusterwide Parameters (System - Presence) pane.

Configure DND Softkeys

Default softkey templates do not make a DND softkey available. To add a DND softkey, navigate to **Device** > **Device Settings** > **Softkey Template**, add Do Not Disturb to a softkey template in the Softkey Template Configuration window, and associate the template to the device.

A DND softkey is available in the following states:

- Connected
- Connected Conference
- Connected Transfer
- Off Hook
- Off Hook with Feature
- On Hold
- Remote In Use
- On Hook
- Ring In
- Ring Out
- Digits After First

Configure a DND Button

To configure a DND button, navigate to **Device** > **Device Settings** > **Phone Button Template** and add Do Not Disturb in the Phone Button Template Configuration window.

Configure Device Parameters for DND

To configure DND on a particular Cisco Unified IP Phone, navigate to **Device** > **Phone** and choose the phone that you want to configure. In the Do Not Disturb pane on the Phone Configuration window, configure the parameters that are shown in the following table.

Table 48: DND Device Parameters

Field	Description
Do Not Disturb	Check this check box to enable Do Not Disturb on the phone.

Field	Description
DND Option	When you enable DND on the phone, this parameter allows you to specify how the DND features handle 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.

Add DND to Common Phone Profiles

To add DND to a common phone profile, navigate to **Device** > **Device Settings** > **Common Phone Profile** and choose the phone profile that you want to modify. In the Common Phone Profile Configuration window, configure the DND parameters that are shown in the following table.

Table 49: Common Phone Profile DND Parameters

Field	Description
DND Option	When you enable DND on the phone, this parameter allows you to specify how the DND features handle 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. **Note** 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.

How to Use Do Not Disturb

This section provides instructions for using Do Not Disturb, as well as usage examples for different Do Not Disturb call scenarios.

Use the Do Not Disturb Feature

You can activate Do Not Disturb using any of the following methods:

- Softkey
- Feature button
- Cisco Unified Communications Self Care Portal

After you activate DND, the phone status line displays Do not disturb is active, the DND line button icon becomes an empty circle, and the light turns amber.

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.

Do Not Disturb Usage Examples

This section provides several examples of how calls get presented to phones with the Do Not Disturb feature enabled for both the DND Ringer Off option and the DND Call Reject option.

DND Ringer Off Option

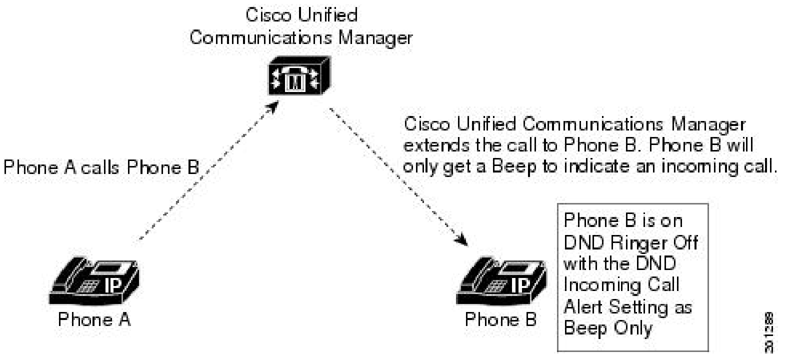
The following examples use the DND Ringer Off option.

Normal Priority Call with DND Ringer Off Enabled on a Nonshared Line

The following figure shows the steps that are associated with DND when you place a normal-priority call to a phone with DND Ringer Off enabled on a nonshared line:

1. Phone B activates DND. Phone B displays Do Not Disturb is active.
2. Phone A dials phone B.
3. Phone B beeps, and phone A receives ringback tone.

Figure 25: Normal Priority Call with DND Ringer Off Enabled on a Nonshared Line

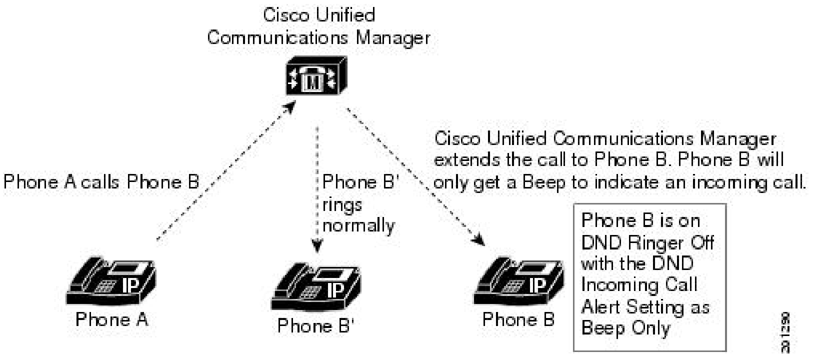

Cisco Unified
Communications Manager
Phone A calls Phone B
Cisco Unified Communications Manager extends the call to Phone B. Phone B will only get a Beep to indicate an incoming call.
Phone B is on DND Ringer Off with the DND Incoming Call Alert Setting as Beep Only
Phone A
Phone B
201289

Normal Priority Call with DND Ringer Off Enabled on a Shared Line

The following figure shows the steps that are associated with DND when you place a normal-priority call to a phone with DND Ringer Off enabled on a shared line:

1. Phone B activates DND. Phone B displays Do Not Disturb is active.
2. Phone A dials a shared line on phone B.
3. Phone B beeps, and phone B', which shares the line, rings normally.
4. Phone A receives ringback tone.

Figure 26: Normal Priority Call with DND Ringer Off Enabled on a Shared Line


Cisco Unified
Communications Manager
Phone A calls Phone B
Phone B' rings normally
Cisco Unified Communications Manager extends the call to Phone B. Phone B will only get a Beep to indicate an incoming call.
Phone B is on DND Ringer Off with the DND Incoming Call Alert Setting as Beep Only
Phone A
Phone B'
Phone B
201290

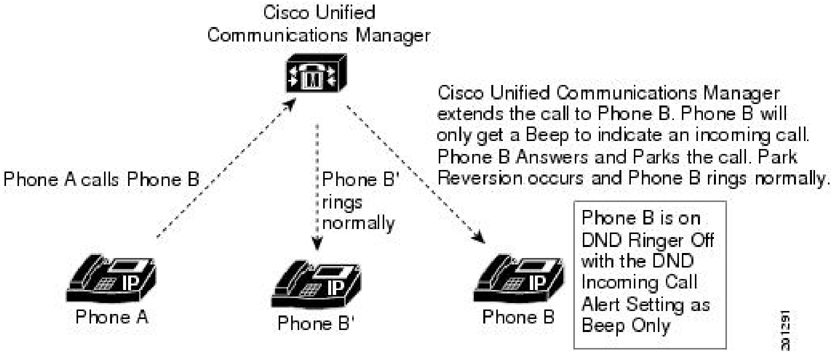
High Priority Call with DND Ringer Off Enabled on a Shared Line

The following figure shows the steps that are associated with DND when you place a high-priority call to a phone with DND Ringer Off enabled on a shared line:

1. Phone B activates DND. Phone B displays Do Not Disturb is active.
2. Phone A dials a shared line on phone B.
3. Phone B beeps, and phone B', which shares the line, rings normally.
4. Phone A receives ringback tone.
5. Phone B answers and parks the call.

6. Park reversion occurs, and phone B rings normally.

Figure 27: High Priority Call with DND Ringer Off Enabled on a Shared Line


Cisco Unified Communications Manager
Cisco Unified Communications Manager extends the call to Phone B. Phone B will only get a Beep to indicate an incoming call. Phone B Answers and Parks the call. Park Reversion occurs and Phone B rings normally.
Phone A calls Phone B
Phone B' rings normally
Phone B is on DND Ringer Off with the DND Incoming Call Alert Setting as Beep Only
Phone A
Phone B'
Phone B
201291

Normal Call with DND and Call Forward No Answer Enabled on a Nonshared Line

The following steps show the call flow for a call that you make to a phone with both DND and Call Forward No Answer active:

1. Phone B configures Call Forward No Answer to forward calls to Phone C.
2. Phone B activates DND.
3. Phone A calls Phone B.
4. Phone B beeps and does not answer the call.
5. The call gets forwarded to phone C, which rings normally.

DND Call Reject Option

The following examples use the DND Call Reject option.

Normal Priority Call with DND Call Reject Enabled on a Nonshared Line

The following steps show the call flow for a call with Call Reject enabled on a nonshared line:

1. Phone B activates DND Call Reject with a DND Incoming Call Alert setting of Beep Only.
2. Phone A call Phone B.
3. Cisco Unified Communications Manager rejects the call with the reason User Busy.
4. Phone B gets a beep tone only.

Normal Priority Call with DND Call Reject Enabled on a Shared Line

The following steps show the call flow for a call with Call Reject enabled on a shared line:

1. Phone B activates DND Call Reject with a DND Incoming Call Alert setting of Beep Only.
2. Phone A call Phone B.
3. Cisco Unified Communications Manager rejects the call with the reason User Busy.

4. Phone B gets a beep tone only.
5. Phone B-prime, which is not on DND, rings normally.

High-Priority Call with DND Call Reject Enabled on a Shared Line

The following steps show the call flow for a high-priority call with DND Call Reject enabled on a shared line:

1. Phone A activates DND Call Reject with a DND Incoming Call Alert setting of Beep Only.
2. Phone A calls Phone B.
3. Cisco Unified Communications Manager extends the call the Phone B.
4. Phone B answers the call.
5. Phone A parks the call.
6. Phone A-prime, which is not on DND, rings normally.
7. Park Reversion occurs, and Phone A rings normally.

Troubleshooting Do Not Disturb

The section provides troubleshooting information for Cisco Unified IP Phones (SCCP and SIP).

DND Troubleshooting

If DND does not operate as expected, determine whether the settings maintained by the SCCP station code are the same as what the user thinks they are, as shown in the following examples.

Verify DND status by toggling DND

If you toggle DND status using a softkey or a feature button, you can see the new status in the LmFeatureInd message that is sent to line control. (The new status implies the old status was the opposite.) You can then toggle back.

The LmFeatureInd SDL trace gives the following three fields:

- feature: A value of 4 indicates DND.
- featureState: A value of 0 indicates on; a value of 1 indicates off.
- dndOption: A value of 0 indicates unknown; a value of 1 indicates ringer-off, and a value of 2 indicates call-reject.

  Verify all DND settings by resetting the phone

If you reset the phone, all of the DND settings will be printed in the detailed SDI traces, for example:

```
StationD: (xxxxxxx) DND settings from TSP: status=a, option=b, ringSetting=d
```

where

- a equals 0 (DND off) or 1 (DND on)

- b equals 1 (DND ringer-off option, 1 indicates ringer-off)
- d equals 1 (disable ringer), 2 (flash only), or 5 (beep only)

Troubleshooting Phones Running SIP

Use the following information to troubleshoot phones that are running SIP:

- debugs: sip-dnd, sip-messages, dnd-settings
- show: config, dnd-settings
- Sniffer traces

Troubleshooting Phones Running SCCP

Use the following information to troubleshoot phones that are running SCCP:

- debug: jvm all info
- Sniffer traces

Troubleshooting DND Errors

The following table shows symptoms and actions for DND troubleshooting.

Table 50: DND Troubleshooting Symptoms and Actions

Symptom	Actions
DND feature key does not display	• Check the Cisco Unified Communications Manager version and ensure that it is 6.0 or above. • Verify the button template for this phone has the DND feature key. • Capture a sniffer trace and verify that the phone gets the correct button template. • Verify that the phone is running firmware 8.3(1) and above.

Symptom	Actions
DND softkey does not display	• Check the Cisco Unified Communications Manager version and ensure that it is 6.0 or above. • Verify the softkey template for this phone has DND. • Capture a sniffer trace and verify that the phone gets the correct softkey template. • Verify that the phone is running firmware 8.3(1) and above.
BLF speed dial does not show DND status	• Check the Cisco Unified Communications Manager version and ensure that it is 6.0 or above. • Verify that the BLF DND is set to enabled in Enterprise parameters. • Capture a sniffer trace and verify that the phone gets the correct NotificationMessage. • Verify that the phone is running firmware 8.3(1) and above.

CHAPTER 19

Enhanced Location Call Admission Control

The following sections provide information about the Enhanced Location Call Admission Control feature.

Configure Enhanced Location Call Admission Control

The Enhanced Location Call Admission Control (CAC) feature improves the Location CAC mechanism to support complex network, multi-tier, multi-hop topology. This feature supports Location CAC within a cluster and among multiple clusters and allows end to end bandwidth deduction. This enhancement to the CAC feature creates a much more flexible and dynamic system for the management of bandwidth.

The enhanced CAC feature provides a new service, called Location Bandwidth Manager (LBM). The LBM service can be configured to run on every node or selected nodes of a Cisco Unified Communications Manager (Unified CM) server.

Perform the following steps to configure the Enhanced Location Call Admission Control feature:

Procedure

Step 1 Activate the LBM service.

If a server is upgraded from pre-9.0 release, the LBM service is activated on all servers where the Cisco Callmanager service is enabled. For a new system install, the LBM service must be manually activated on the desired nodes.

Step 2 Create an LBM group.

Each Unified CM server must communicate with an LBM. If LBM is not running on the same node, configure an LBM group and assign the LBM group to the Unified CM server.

Step 3 Model the network using locations and links.

Step 4 Add the locations for the system.

By default, when a new location is created, a link from the newly added location to the Hub_None is added as well, with unlimited audio bandwidth, 384 kbps video bandwidth and 384 kbps immersive video bandwidth. This can be adjusted to match the model and if needed the link to the Hub_None location can be deleted.

Step 5 Assign intra-location bandwidth to the location, if the default of unlimited bandwidth is not desired.

Step 6 Add links from one location to other locations (inter-location). And assign bandwidth allocations and weight to the links.

If you are enabling intercluster Enhanced Location CAC complete the following steps:

Step 7 Configure the LBM Hub Group page to allow the LBM servers acting as Hubs to find LBM servers in remote clusters and establish external communication with those clusters.

Any LBM servers that are assigned an LBM Hub Group establish communication with all other LBM servers assigned the same or an overlapping LBM Hub Group.

Step 8 Assign the SIP ICT that is used to route calls between clusters to the system location Shadow.

Enhanced Location Call Admission Control Feature

The following sections provide information on the Enhanced Location Call Admission Control feature.

Terminology for Enhanced Location Call Admission Control

This document uses the following terms to discuss Enhanced Location Call Admission Control (CAC):

- **Link:** Links interconnect locations and are used to define the bandwidth available between locations.
- **Weight:**The relative priority of a link in forming the effective path between any pairs of locations. Weights are used on links to provide a “cost” to the “effective path”. The effective path has the least cumulative weight of all other paths. Weights are pertinent only when there is more than 1 path between any 2 locations.
- **Locations:** A Location represents a LAN. It could contain endpoints or simply serve as a transit location between links for WAN network modeling
- **Bandwidth Allocation:** The amount of bandwidth allocated in the model for each type of traffic: audio, video, and immersive video (Telepresence).
- **Path:** A sequence of links and intermediate locations connecting a pair of end locations. Only one effective path between a pair of end locations is used
- **Locations Bandwidth Manager:** A service that assembles a network model from configured location and link data in one or more clusters, determines the effective paths between pairs of locations, determines whether to admit calls between a pair of locations based on the availability of bandwidth for each type of call, and deducts (reserves) bandwidth for the duration of each call that is admitted.
- **Locations Bandwidth Manager Hub:** An LBM service that has been designated to participate directly in inter-cluster replication of fixed and dynamic data. LBMs assigned an LBM hub group discover each other through their common connections and form a fully meshed replication network. Other LBM

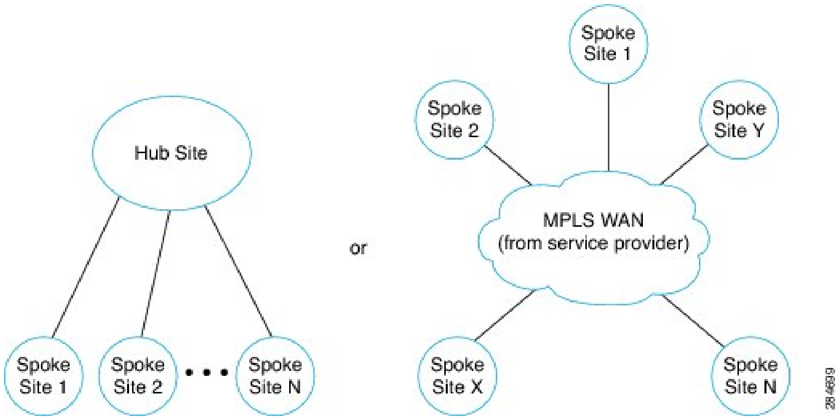
services in a cluster with an LBM hub participate indirectly in inter-cluster replication through the LBM hubs in their cluster.

- **Shadow location:** SIP Inter-cluster Trunks must be assigned to the Shadow location to enable proper inter-cluster operation of this feature. SIP trunks to devices with a specific location, such as SIP Gateways, may be assigned to ordinary locations. A Shadow location is a special location that has no links to other locations and no bandwidth allocations.

Limitations of Bandwidth Management Prior to Release 9.0

Previously Unified CM Location Call Admission Control (CAC) could only effectively support the simple Hub and Spoke location model, such as remote sites connected to a main site or all sites connected to an MPLS-based IP WAN.

Figure 28: Hub and Spoke Location Model



Many customer networks do not conform to the Hub and Spoke location model; therefore customers need to have a Location CAC mechanism that better models the path that media actually travel through the network.

There are many deployments where multiple Unified CM clusters manage devices in the same physical site, for example, multiple Unified CM clusters manage phones in the same branch. When phones call each other within the same site but are managed by different clusters, bandwidth may be deducted (reserved) unnecessarily, which may cause blocking of other calls. Adding video calls and immersive video calls to the network exacerbates these issues because video calls consume more bandwidth than audio calls.

When Session Manager Edition (SME) attempts to manage bandwidth between clusters it can only assign location bandwidth to trunks connecting the SME and the leaf clusters, not reflecting the fact that media is may not be traversing the SME.

Enhancement to Bandwidth Management Solution

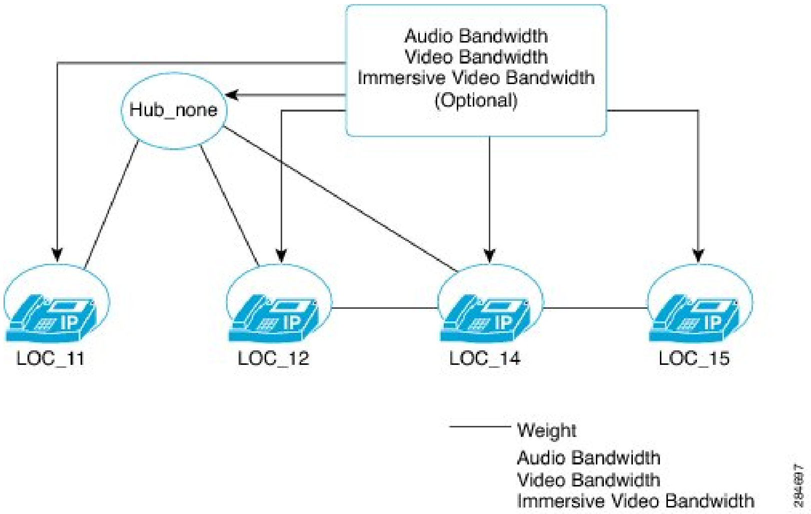
The bandwidth management solution has been enhanced to support complex network models, including multi-tier, multi-hop topology. In these models audio and video calls can traverse multiple network links and locations and deduct bandwidth across each link. Enhanced network model is structured as follow:

- When two locations are directly connected, a link is modeled between them.
- Weights are assigned to the links to model the actual media path between two locations.
- Audio, video, and immersive video bandwidth capacity are assigned to each link and location.

- Bandwidth deductions are made from each link and from each location along the media path.

The following graphic represents a simple Location CAC topology model.

Figure 29: Simple Location CAC Model



Enhanced Location Call Admission Control Architecture

The following sections provide information about Enhanced Location Call Admission Control architecture.

Model-Based Call Admission Control

Enhanced Location Call Admission Control (CAC) is a model-based CAC mechanism. The administrator creates a model of the network and how the network infrastructure handles the media.

Note The more accurate and detailed the model of the network is, the more effective the management of the bandwidth and avoidance of congestion is within the network. However, the model cannot account for transient network failure conditions.

Through the Cisco Unified Communications Manager interface the administrator configures the Enhanced Location CAC mechanism based on the network model.

After the administrator creates the model and enters it into Cisco Unified Communications Manager database, Location Bandwidth Manager (LBM) calculates the effective paths between all originating and terminating locations, and deducts bandwidth from each link and location along that path.

When a call is admitted between two locations, LBM deducts (reserves) bandwidth from each link and location along that path for the duration of the call. The bandwidth deduction is symmetric (bidirectional). For example, for a G.711 audio call, 80 kb bandwidth is deducted from the audio allocation assigned to each link and location in the call path. When a call is terminated, LBM restores the bandwidth deduction.

The administrator may assign bandwidth allocations to locations as well as to links, if it is desired to limit admission of intra-location as well as inter-location calls.

Note The intra-location bandwidth allocations are unlimited by default.

Location Bandwidth Manager

A Location Bandwidth Manager (LBM) can reside and run on every Cisco Unified Communications Manager node, or on a few selected Cisco Unified Communications Manager nodes within the cluster. LBM is a feature service and can be started and stopped from the serviceability configuration page.

Main functions of Location Bandwidth Manager are:

- Model Formation and path determination
- Replication of the model to other LBMs within the cluster, and between clusters
- Servicing bandwidth requests from Unified CM
- Replication of bandwidth deductions to other LBMs within the cluster, and between clusters
- Provide configured and dynamic information on request to Serviceability
- Update Location RTMT counters

When LBM service is started, it reads configured location information from the local database. This includes configured locations; audio, video, and immersive video capacities in those locations; links from a given location to other locations, the weight associated with those link; and the audio, video, and immersive video capacities on those links. It creates a local model with these values. Other LBMs in the cluster have access to the same data from the database and thus create the same local model at their startup. The LBM is now synchronized with the rest of the cluster and is ready to provide service.

Each Cisco Callmanager service communicates with LBM services within the cluster, as designated by an LBM group. By default, each Cisco Callmanager service communicates with the local LBM within the cluster.

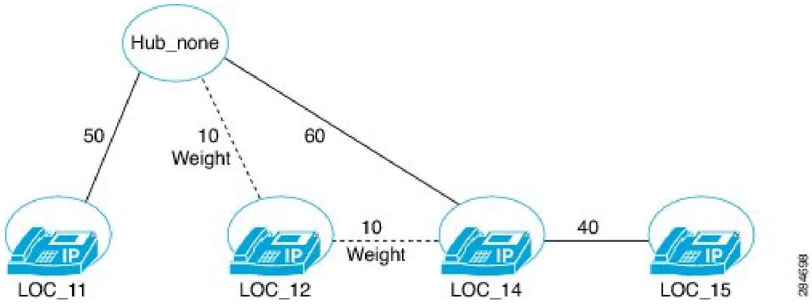
Each LBM service communicates with all other LBMs within the cluster and may communicate through LBM Hubs with LBM services in other clusters. LBM services within the cluster are fully meshed.

The LBM service computes the effective path from the source location to the destination location by adding the weight of each link for each possible path between source and destination. The path with the least cumulative weight is designated as the effective path. If there is more than one path that has the same weight LBM chooses which path to use. All calls that have the same source and destination locations use the same path.

The following figure provides an example, demonstrating the calculation of the effective path from Hub_none to Loc_14:

- A path from Hub_none through Loc_12 to Loc_14 is the effective path with a total weight of 20.
- A path from Hub_none to Loc_14 has weight of 60 which is greater than 20 and therefore not the effective path.

Figure 30: Location CAC Effective Reservation Path Determination



The following are some important considerations:

- LBM group configuration allows the administrator to select the LBM service that Cisco Unified Communications Manager can communicate with.
- It is not necessary to run the LBM service on every Cisco Unified Communications Manager node.
- The administrator can configure the LBM group based on consideration to minimize the network delay for bandwidth deduction.
- The LBM group can provide redundancy of LBM service to maintain the availability of CAC mechanism during network outage.
- When Cisco Unified Communications Manager is trying to locate the LBM service to communicate with:
  - It honors the LBM group association if one exists
  - If there is no LBM group assigned or an empty LBM group is assigned, Cisco Unified Communications Manager uses a local LBM if it is activated
  - If there is no LBM available, then Cisco Unified Communications Manager uses a service parameter to determine how to treat the call

When selectively activating LBM services and configuring the LBM groups consider the following:

- Activate at least one LBM on each distinct call processing site. Consider activating LBM on standalone servers.
- For split data center deployment, activate at least one LBM for each data center.
- Consider activating LBM on the stand-by servers where there are active and stand-by servers to reduce the impact on the active servers.
- Connect to a local LBM service when available.
- For clusters with multiple sites, select LBM services in the data center or in the closest regional site.

Inter-Cluster Location Call Admission Control

With the model-based Location CAC between clusters (intercluster), each Cisco Unified Communications Manager cluster has a local model that it controls. Through an intersystem replication mechanism, each system in the enterprise network propagates its local model to other systems and creates a global model of the entire enterprise network by putting in each model from the remote systems, and storing it in the internal memory.

LBM services in each system in the enterprise network that participate in the intercluster location CAC, has the global model stored in its local memory.

When a call is made across the clusters, originating and terminating systems pass their locations and call identifiers to each other through the signaling protocol (e.g. SIP signaling protocol). Terminating and originating clusters reserve location CAC bandwidth end to end locally, using its global location CAC model, and then replicate the bandwidth reservation to other systems in the enterprise network.

Note The amount of intersystem bandwidth replication messages can be significant. Select LBM Hubs carefully to make replication more efficient within the enterprise network.

Race conditions may occur as each local system reserves bandwidth from the global model and then replicates the deduction. When race conditions occur, calls may be admitted in excess of those for which bandwidth is deducted.

Note When modeling the network, use conservative bandwidth capacity assumptions to allow for the fact that calls may be admitted in excess of those for which bandwidth is deducted.

Intercluster Location Call Admission Call Configuration Considerations

The following are some considerations when configuring intercluster location CAC between a local cluster and a remote cluster:

- The local administrator must configure the remote locations adjacent to local locations and the links between local and remote locations.
- When the local cluster receives a model replication from a remote cluster, it joins the models by identifying locations and links that appear in both models and forms a global network model.
- It is critical to name locations consistently in all clusters, to ensure the global network model assembles correctly. Follow the principle of same location, same name; different location, different name.

  Note If there is a conflict in bandwidth capacity or weight assignment on the common links or locations, the local cluster uses the minimum of the assigned values.

Intercluster Location Call Admission Control Replication

An Enhanced Location CAC LBM replication network is used to replicate the model topology, and bandwidth deduction across multiple clusters, and within the cluster. All LBM services are fully connected within the cluster and all LBM Hubs are fully connected between clusters. LBM services that are not LBM Hubs participate in intercluster replication only through the LBM Hubs in their cluster.

The LBM Hub Group provides the mechanism for an LBM Hub to find out how to communicate with other LBM Hubs in remote clusters. By this mechanism, the LBM Hub builds a fully meshed replication network with all other LBM Hubs.

Location Bandwidth Manager Hubs

The following describes Location Bandwidth Manager (LBM) Hubs:

- An LBM service becomes a Hub when an LBM Hub Group is assigned to it.
- If a cluster has multiple LBM Hubs, the LBM Hub with the lowest IP Address functions as the sender of messages to other remote clusters.
- The LBM Hub organizes its links to remote LBM Hubs by the ClusterId assigned to it.
- The LBM Hub that functions as the sender for messages, and picks the first LBM Hub of each cluster to send messages to.
- The LBM Hub that receives messages from the remote clusters, forwards the received messages to other LBM services within the cluster.

Location Bandwidth Service Parameters

Service parameters for Enhanced Location Call Admission Control

There are three new service parameters for Enhanced Location CAC:

- **Unified CM to LBM Periodic Reservation Refresh Timer:** This parameter specifies the time duration in minutes that Cisco Unified Communications Manager refreshes the active bandwidth reservations to the Cisco Location Bandwidth Manager.
- **Call Treatment When No LBM Available:** This parameter specifies whether Cisco Unified Communications Manager allows or rejects calls when there is no Cisco Location Bandwidth Manager available for location-based call admission control.
- **Locations Media Resource Audio Bit Rate Policy:** This parameter determines the bit rate value to deduct from the audio bandwidth pools within and between the locations of the parties for an audio-only call when a Media Resource such as a transcoder is inserted into the media path and for more complex scenarios.

Shadow System Location

Shadow Location

Shadow is a new system location created for intercluster Enhanced Location CAC. In order to pass location information across clusters, the SIP ICT needs to be assigned to the system location Shadow.

The system location Shadow:

- Is a valid location only for a SIP ICT. Devices other than SIP trunks assigned incorrectly to the Shadow location are treated as if assigned to the Hub_None location.
- Cannot have a link connecting to other user defined locations, so bandwidth cannot be deducted between the Shadow location and other user defined locations.
- Has no intra-location bandwidth capacities, so bandwidth cannot be deducted within the Shadow location.

Note SIP trunks, including ICTs, may be assigned to fixed locations, if their destination does not participate in intercluster Enhanced Location CAC.

Devices That Support Enhanced Location Call Admission Control

Device support

Unified CM and LBM manage bandwidth for all types of end devices, including IP phones, gateways, and H.323 and SIP trunk destinations. However, inter-cluster Enhanced Locations CAC requires SIP ICTs assigned to the system location Shadow. All other types of devices are supported only when assigned to ordinary (fixed) Locations.

Unified CM and LBM do not manage bandwidth for media resources; calls are modeled and bandwidth reserved between the locations of end devices only. For cases in which media resources change the bandwidth requirement for a call, the customer has the option to change a global parameter setting that determines whether the minimum or maximum bandwidth is reserved.

Enhanced Call Admission Control Limitations

Limitations

The model created by the system is not perfectly synchronized at all times; excess calls may be admitted due to race conditions. Use conservative bandwidth allocations in the model to allow for this possibility.

During network failure conditions, the bandwidth reservation path calculated by Unified CM may not accurately reflect network conditions. There is no satisfactory way to allow for this scenario in the model.

If video capabilities are enabled, then bandwidth for audio will be allocated from video.

Location Bandwidth Manager Security

Location Bandwidth Manager Security Mode

LBM is able to secure its intercluster communications between LBM hubs and in order to support backward compatibility and upgrades LBM has an option to configure how intercluster LBM hubs communicate with each other. To meet these requirements, the enterprise service parameter, LBM Security Mode, is available with the following values:

- Secure
- Insecure
- Mixed

The default setting is Insecure. You enable LBM secure communication by changing this Enterprise service parameter to either Secure or Mixed. And when this service parameter is changed, the LBM hubs in that cluster need to be restarted so that connections with the new security setting can be attempted.

The Mixed configuration is insecure, but very flexible and allows Unified CM Release 9.1 and later clusters to communicate with Unified CM Release 9.0 clusters, the latter operating in the strict insecure mode. This is an intermediate step while converting all the clusters from insecure to secure mode or secure to insecure mode. A description of this would be: starting with the clusters in insecure mode, make sure all the certificates are present on all nodes using, for instance, the Bulk Certificate export/import. Change the parameter to Mixed without losing communication (except when the LBM hubs are restarted). After all the clusters are moved into Mixed and all LBM hubs are confirmed to have secure connections to all other hubs, switch to Secure mode. Similar steps involving intermediate mixed state can be followed to move to insecure from secure.

The Enterprise service parameter is used by LBM to determine whether an LBM hub accepts and attempts secure only, insecure only, or both, connections from or to a remote LBM hub.

LBMs has one port for secure connections (9005), one for insecure connections (9004). The insecure port 9004 has been defined since Unified CM 9.0 release. Secure port 9005 is added for Unified CM Release 9.1.

The communication between LBMs within the cluster remains through the insecure connections.

An LBM hub accepts connections from remote LBM hubs:

- If the Enterprise service parameter is set to Mixed, an LBM hub in this cluster accepts both secure and insecure connections from remote LBM hubs.
- If the Enterprise service parameter is set to Insecure, an LBM hub only accepts insecure connections from remote LBM hubs.
- If the Enterprise service parameter is set to Secure, an LBM hub only accepts secure connections from remote LBM hubs.

An LBM hub attempts to open a connection to remote LBM hubs:

- If the Enterprise service parameter is set to Mixed, an LBM hub in this cluster attempts both secure and insecure connections to remote LBM hubs, which is also based on validation and availability of local and remote security certificates.
- If the Enterprise service parameter is set to Insecure, an LBM hub only attempts an insecure connection to remote LBM hubs.
- If the Enterprise service parameter is set to Secure, an LBM hub only attempts a secure connection to remote LBM hubs. Secure connections are based on validation and availability of local and remote security certificates.

In Unified CM Release 9.0 LBM two connections between each LBM were available, one connection for outgoing and one for incoming insecure communication. For Unified CM Release 9.1, LBM two additional connections are available for LBM hubs connecting between clusters for secure communication. Therefore there are up to 4 connections for the Mixed Mode service parameter for LBM hubs connecting between clusters.

LBM selects a secure connection to send information, if a secure connection is available in its connection pool. If a secure connection is not available, but an insecure connection is available, LBM sends information on the insecure connection. Under race conditions when the connections are being established, it is possible that initially there are only insecure connections available. However, LBM automatically switches to secure connections when those become available. This logic applies to connections coming and going during the application lifetime. This illustrates one reason why mixed connections are inherently insecure.

Note To use the Secure LBM feature where the LBM Security Mode is set to Mixed or Secure, Tomcat certificates for every node must be deployed on each respective node. For more information about deploying certificates, see *Cisco Unified Communications Operating System Administration Guide*.

CHAPTER 20

Extend and Connect

This chapter provides information about the Extend and Connect feature. This chapter contains the following information:

Extend and Connect

Overview of Extend and Connect

Changes in personal device preferences and an increasing number of mobile and remote workers necessitates a flexible solution that extends Unified Communications (UC) features with a Bring Your Own Device (BYOD) philosophy. Extend and Connect provides this solution.

Extend and Connect is a feature that allows administrators to rapidly deploy UC Computer Telephony Integration (CTI) applications which interoperate with any endpoint. With Extend and Connect, users can leverage the benefits of UC applications from any location using any device. This feature also allows interoperability between newer UC solutions and legacy systems, so customers can migrate to newer UC solutions over time as existing hardware is deprecated.

Features and Benefits

Features

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 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

Benefits

The Extend and Connect feature provides the following benefits to its users:

- Standardized call control across the Enterprise
- Centralized applications
- Simplified integration points and network topology
- Centralized licensing
- Centralized call-detail records for accounting and billing
- Accelerated application deployment
- Existing investments in legacy PBXs and devices are preserved
- Migration to Cisco IP devices over time is enabled

Use Cases

Cisco Jabber for Customers with a Third-Party PBX

Customers want to deploy Cisco Jabber as the desktop standard for IM and Presence Service capability, but they have not yet decided to adopt Cisco IP devices. They plan to migrate to Cisco IP devices over time, or they need to maintain a hybrid device environment.

Cisco Jabber for Mobile Workers

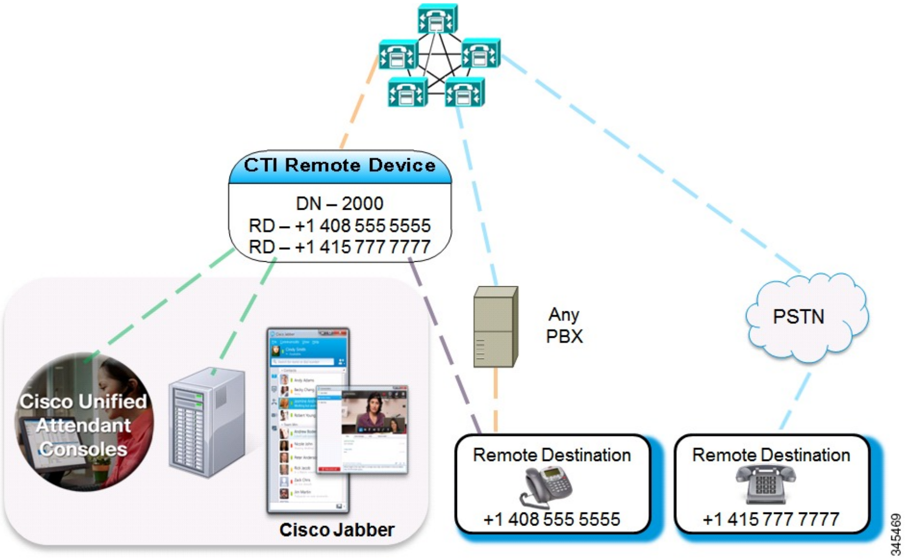
- Users want to use Cisco Jabber to make and receive calls using a home or hotel phone, because their PC hardware or available network connection does not support VoIP.
- Users want to use Cisco Jabber because they want the convenience of Jabber click-to-call features to work with the device they are sitting next to at that moment.

- Users already have a Cisco Unified IP Phone, Jabber Softphone, or both, but they also want to use Jabber with a home or hotel phone.

System Architecture

Figure 31: Extend and Connect System Architecture

The following graphic represents the system architecture for the Extend and Connect feature.



- A CTI Remote Device is registered to Unified Communications Manager. For example, directory number (DN) 2000 is the internal and external extension, of the user, represented as +1 408 200 2000 or 2000.
- Remote Destinations represent the off-cluster devices of a user.
- Off-cluster devices are registered to the PBX or PSTN.
- CTI applications receive call events and can perform call operations.
- Trunks connect Unified Communications Manager with the PSTN or PBX. Supported types include PRI , BRI , SIP, and FXO.

Note When you use remote destinations across MGCP gateways, the display name, the display number, and the call information that is passed across the gateway cannot be updated after the call is answered. This is a limitation of the MGCP protocol.

Call Flow

This section describes the flow of events for Extend and Connect from a system perspective.

1. Unified Communications Manager and Cisco Unified Communications Manager Session Management Edition (Unified Communications Manager SME) control the Enterprise PSTN trunking and dial-plan.

2. Administrators add users to Unified Communications Manager and assign them a new CTI Remote Device type.
3. Each CTI Remote Device is configured with the user work number directory number (DN) (for example, 2000) and a remote destination which represents any off-cluster device (for example, a PBX phone with the number +1 408 555 5555).
4. Administrators can configure remote destinations using the Cisco Unified Communications Manager Administration interface, Administrative XML (AXL) interface, or the Bulk Administration Tool (BAT), and end users can configure remote destinations using the Jabber client.
5. Users sign in to Jabber and select **Use my other device**.
6. Users may add a new remote destination (for example, home office, +1 415 777 7777) or can select from previously configured remote destinations.
7. The Jabber client marks the selected remote destination as **Active**.
8. Incoming calls to the work DN (+1 408 200 2000) are automatically routed to the active destination (+1 415 777 7777).
9. Outbound call requests follow a Dial Via Office reverse call flow, as follows:
   a. The user clicks to call.
   b. A server call is placed to the active remote destination.
   c. The user answers the server (DVO) call.
   d. The call is immediately redirected to the desired number.
10. During calls, midcall features are available through the Jabber client, such as Hold and Resume, Consult, Conference, and Transfer.
11. When users shut down or sign out of the Jabber client, the remote destination is marked **Inactive**.
12. When remote destinations are inactive, calls to the DN are routed to voicemail by default. Administrators can select the option to always forward calls to all remote destinations based on their schedule when using third-party voicemail.

Figure 32: Incoming Call from PBX

The following illustration shows a sample incoming call from the PBX.

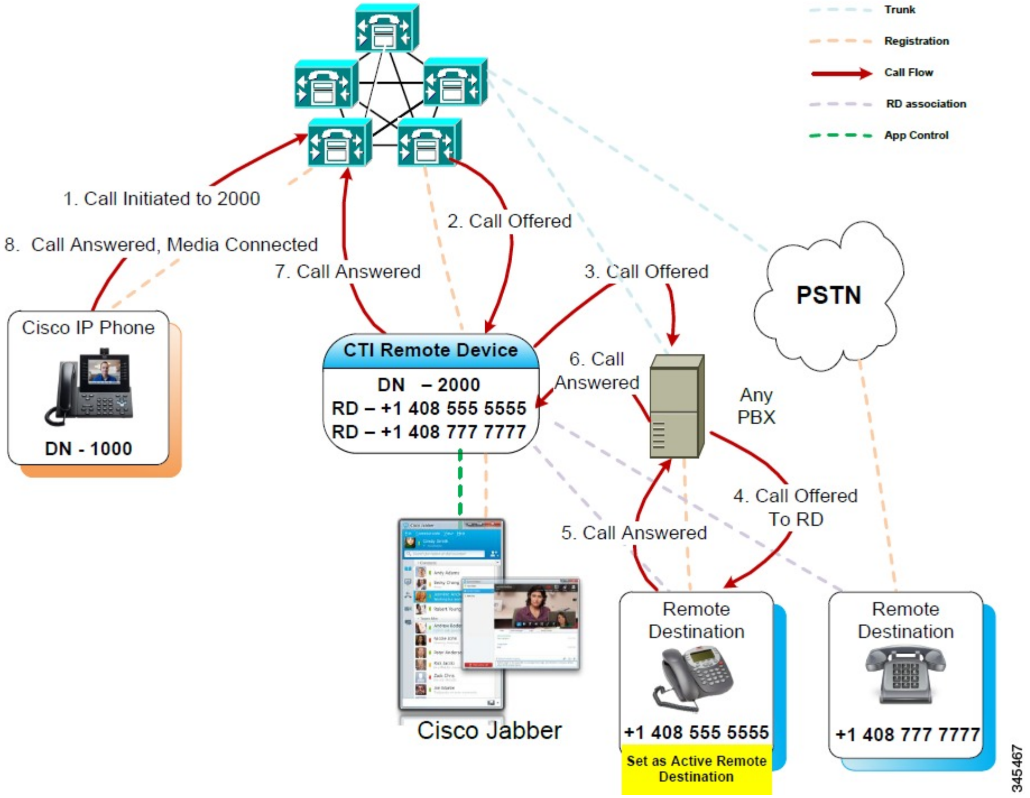
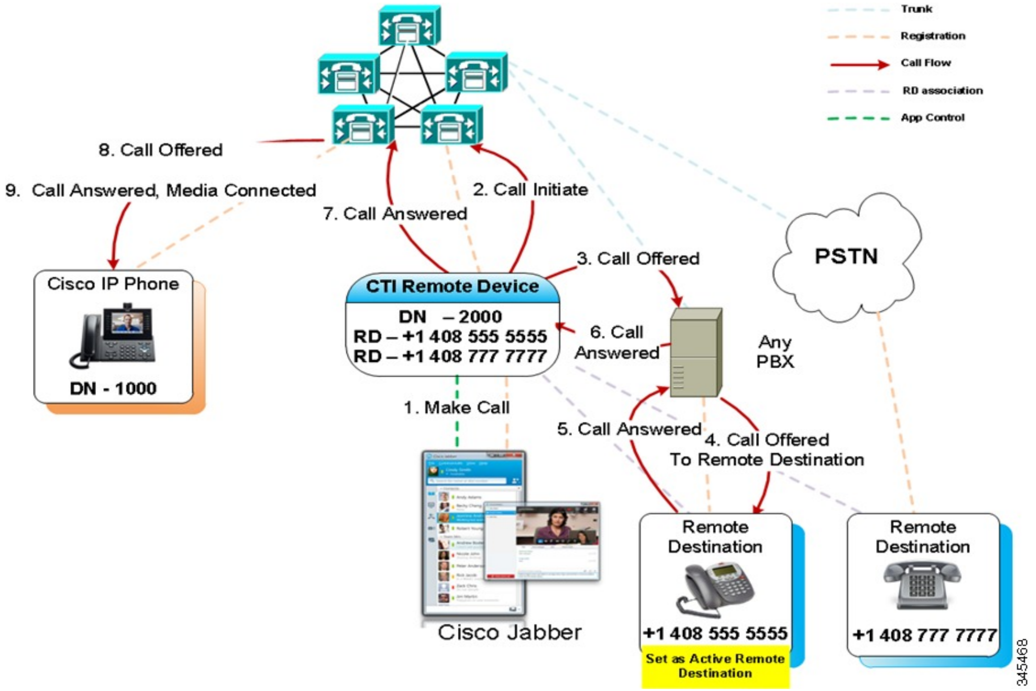


Figure 33: Outgoing Call to PBX

The following illustration shows a sample outgoing call to the PBX.



System Requirements

Software Components

To operate correctly, Extend and Connect requires the following software components:

- Cisco Unified Communications Manager, Release 9.1(1)
- Cisco Jabber, Release 9.1(1)
    - The initial release supports the third-party PBX use case.
    - The maintenance release adds support for the mobile worker use case.

For more information and use cases, see the *Cisco Jabber Install and Upgrade Guides*.

Licensing Requirements

Extend and Connect operates under the following licenses:

- CUWL Standard
- CUWL Professional
- UCL-Enhanced

Interactions and Restrictions

This section describes the interactions and restrictions for Extend and Connect.

Interactions

Directory URI Dialing

A Directory URI is the SIP address of a user that takes the form **user@host**, where *user* specifies a phone number or user name and *host* specifies the IP address, domain, or hostname where the user is available. You can assign multiple URIs to a single DN. End user Directory URIs are automatically associated to the primary extension for the user.

You can configure a Directory URI as the DN, remote destination, or both for the CTI remote device.

Unified Mobility

The Unified Mobility feature allows users to answer incoming calls to their enterprise extension on either their Cisco Unified IP phone or a remote destination, such as a mobile phone, home phone, or hotel phone. Users can move active calls between their Cisco Unified IP phone and their mobile phone without losing the connection. This feature requires configuration of Remote Destination Profile device type.

The Extend and Connect feature allows users to answer incoming calls on any of their Cisco Unified IP phones or remote destination phones under the control of Cisco Jabber. However, connected (active) calls cannot be moved between the Cisco Unified IP phone and the remote destination phone. Therefore, Extend and Connect provides application control over the remote phone, but does not support mobility features such as being able to move the call to a Cisco Unified IP phone. This feature requires configuration of CTI Remote Device type.

Users who want the capabilities of both Unified Mobility and Extend and Connect may 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 or later.

Remote destinations used with Cisco Extend and Connect feature should not be configured on Cisco Dual-mode for iPhone, Cisco Dual-mode for Android, and Carrier-integrated Mobile device types. Prefixes should not be used to differentiate the same remote destination address. For example, 91- 4085555555 and +1- 4085555555 are treated as the same number.

For more information, see the Unified Mobility chapter.

Hunt List

A hunt list consists of a group of extensions that can answer calls. The Extend and Connect feature allows users to receive hunt calls on remote destination phones under the following conditions:

- User has Cisco Unified IP Phone
- Cisco Unified P Phone is available to answer hunt calls (logged-in/HLog)
- Cisco Jabber is running in Extend and Connect mode

Note Users can indicate their availability to answer hunt list calls by pressing the HLog softkey or programmable line key on their Cisco IP Phone. The HLog key is not currently available using Cisco Jabber.

For more information, see the Hunt List chapter.

Restrictions

The following restrictions apply to Extend and Connect:

- 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.

- Remote destination numbers must represent off-cluster devices.
- Remote destinations can be off-cluster URIs.
- Directory numbers cannot be configured as remote destination numbers.
- Remote destinations that are configured using Cisco Jabber are verified to be routable by the configured dial plan before they are saved.

- 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.
- 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).

- Each remote destination number must be unique within the cluster.

  Note The same remote destination number cannot be used by two or more users.

Availability Information

The availability status "on a call" is displayed for a user in the following situations:

- Outgoing Calls
  - The user initiates a call from Cisco Jabber in Extend and Connect mode.
  - The user initiates a call from a device that is configured as a remote destination which is routed using Unified Communications Manager or Unified Communications Manager with Unified Communications Manager SME.
- Incoming Calls
  - The user answers a call on a device configured as a remote destination routed using Unified Communications Manager or Unified Communications Manager with Unified Communications Manager SME.

The availability status "on a call" is not displayed for a user in the following situations:

- When the user initiates a call from a device that is configured as a remote destination, but the call is not routed using Unified Communications Manager or Unified Communications Manager with Unified Communications Manager SME.
- When the user answers a call on a device that is configured as a remote destination, but the call is not routed using Unified Communications Manager or Unified Communications Manager with Unified Communications Manager SME.

CallerID Information

The follow information explains the CallerID behavior for Extend and Connect:

- The incoming CallerID information (name and number) is displayed in 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 CM.
- Remote destination numbers are never displayed to the called party.

Performance and Scalability

This section details performance and scalability information that relates to Extend and Connect resources.

Busy Hour Call Attempts

Add 1 to the Busy Hour Call Attempts (BHCA) for each outbound call. BHCA is the number of attempted calls at the busiest hour of the day.

- A Dial via Office call to the active remote destination is one call.
- A redirect from the active remote destination to the desired called party is one call.

Trunk Usage

Incoming calls may consume one or more outbound trunks.

- An internal call that is routed to the active remote destination uses one external trunk.
- A received external call that is routed to the active remote destination uses two external trunks: one trunk for the incoming leg and one trunk for the outgoing leg.

Outgoing calls follow a Dial via Office flow that may consume one or more outbound trunks per call.

- A call to a cluster directory number uses one external trunk for a Dial via Office call to an active remote destination.
- A call to an external party uses one external trunk for a Dial via Office call to an active remote destination, as well as one external trunk for a redirect to an external called party.

CTI Device Weight

The weight of each CTI remote device is the same as a standard Cisco Unified IP Phone (SIP) device.

- A 10,000 user OVA virtual machine template can support a maximum of 10,000 Cisco Unified IP Phones when each phone is a CTI remote device.
- Each CTI remote device can be configured with five lines using five concurrent CTI applications.

Note Use the Cisco Unified Communications Sizing Tool when sizing production clusters.

Extend and Connect Setup

This section describes the procedures that you must complete to provision Cisco Unified Communications Manager users with Extend and Connect capabilities.

For information about provisioning Cisco Jabber users with Extend and Connect, see the *Cisco Jabber Environment Configuration Guide*.

Set Up User Account

For a new or existing user in Unified CM, you must enable user mobility to provision 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 Select **User Management** > **End User**.

The **Find and List Users** window appears.

Step 2 Perform one of the following:

- To configure a new user, select **Add New**.
- To select an existing user, specify the appropriate filters in the **Find User Where** field, select **Find** to retrieve a list of users, and then select the user from the list.

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

The **End User Configuration** window appears.

Step 3 Locate the Mobility Information section.

Step 4 Select **Enable Mobility**.

Step 5 Select **Save**.

What to do next

Add user permissions.

Add User Permissions

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

Procedure

Step 1 Select **User Management** > **End User**.

The **Find and List Users** window appears.

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.

The **End User Configuration** window appears.

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

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

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

Step 6 Select **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
- Standard CCMUSER Administration

Step 8 Select **Add Selected**.

The window closes and the access control groups are added to the user account.

Step 9 Select **Save**.

What to do next

Create CTI remote devices.

Create CTI Remote Devices

A CTI remote device is a new 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 Open the Cisco Unified Communications Manager Administration interface.

Step 2 Select **Device** > **Phone**.

The **Find and List Phone Window** appears.

Step 3 Select **Add New**.

Step 4 Select **CTI Remote Device** from the Phone Type drop-down list and then select **Next**.

The **Phone Configuration** window appears.

Step 5 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 6 Edit the default value in the Device Name field, if appropriate.

Step 7 Enter a meaningful description in the Description field.

Tip 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 8 Ensure 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 9 Specify all other configuration settings on the **Phone Configuration** window as appropriate.

For more information, see “CTI Remote Device Setup” in the *Cisco Unified Communications Manager Administration Guide*.

Step 10 Select **Save**.

The fields to associate directory numbers and add remote destinations become available on the **Phone Configuration** window.

What to do next

Add a directory number to the device.

Add Directory Number to 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).

You must add directory numbers to devices in Unified CM. This procedure provides instructions for adding directory numbers using the **Device** > **Phone** menu option after you create your device. Under this menu option, only the configuration settings that apply to the phone model or CTI route point display. See the *Cisco Unified Communications Manager Administration Guide* for more information about different options to configure directory numbers.

Procedure

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

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

The **Directory Number Configuration** window appears.

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

Step 4 Specify all other required configuration settings as appropriate.

Step 5 Select **Save**.

What to do next

Add Remote Destination.

Add Remote Destination

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.

This procedure to add a remote destination is optional.

Note Administrators can determine which remote destination the Jabber client has set as Active 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 Environment 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 CM Administration interface.

Note Unified Communications Manager automatically applies application dial rules to all remote destination numbers for CTI remote devices. For more information about application dial rules, see “Application Dial Rule Setup” in the *Cisco Unified Communications Manager Administration Guide*.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, select **Device** > **Phone**

The **Find and List Phones** window appears.

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

Step 3 Select the CTI remote device from the list.

The **Phone Configuration** window appears.

Step 4 Locate the Associated Remote Destinations section.

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

The **Remote Destination Information** window appears.

Step 6 Enter the destination number in the Destination Number field and specify all other values as appropriate.

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

For more information about configuring remote destinations, see “Remote Destination Setup” in the *Cisco Unified Communications Manager Administration Guide*.

Step 7 Select **Save**.

What to do next

Complete the following steps to verify the remote destination and apply the configuration to the CTI remote device:

1. Repeat the steps to open the **Phone Configuration** window for the CTI remote device.
2. Locate the Associated Remote Destinations section.
3. Verify that the remote destination is available.
4. Select **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 to Device

Before you begin

You must create or modify an end user account and enable it for mobility. You must also create a CTI Remote Device.

Procedure

Step 1 Navigate to the end user account.

Step 2 Locate the Device Information section.

Step 3 Select **Device Association**.

Step 4 Find and select the CTI remote device.

Step 5 Verify that the selected device appears as a controlled device for the user.

Persistent Connection

The Extend and Connect feature allows a user to benefit from UC applications from any location and any device on a call by call basis. The Persistent Connection feature extends that functionality by allowing the connection to remain persistent between calls.

Persistent connections are created by CTI applications such as Contact Center Express/Enterprise to accelerate call delivery and media setup. Additionally, whisper announcements can be played on persistent connection calls to announce callers (for example, Customer Sales – English) or indicate when media is connected (for example, zip tone).

Persistent Connection Creation

- A persistent connection must be created using a CTI application such as Contact Center Express/Enterprise
- Requirements
  - At least one Remote Destination (RD) must be configured
  - The RD must be Active
- A request to create a second Persistent Connection after the first one is successfully established will fail
- A request to create a second Persistent Connection when the first one is being setup will fail
- A Persistent Connection will have a unique Global Call ID and Call ID, different from a typical call
- A Longest Active Call timer will drop the Persistent Connection when the timer expires
- Call features (such as Consult and Transfer) cannot be performed on a persistent connection, but are supported for a typical call when media is connected.
- After a Persistent Connection is answered, it will remain in the state as Connected for the duration of the call
- When the active remote destination is reset, a Persistent Connection call will drop if there are no other active calls. If there are active calls, it will drop after the current active call is dropped
- The Real-time Monitoring Tool will report the Persistent Connection call as an active call
- A maximum of 8000 Persistent Connections can be created per cluster, or 2000 per node

Persistent Connection Use Cases

Verify Remote Destination in Add

- Route Pattern configured is 9.XXXX
- Application initiates AddRemoteDestination (OtherExtn, 91000, Active=TRUE)
- CTI verifies 91000 and confirms that it is reachable
- AddRemoteDestination is successful

Verify Remote Destination in Update

- Route Pattern configured is 9.XXXX
- Remote Destination configured as 92000
- Application initiates UpdateRemoteDestination (OtherExtn, 92000, 91000, Active=True)
- CTI verifies 91000 and confirms that it is reachable
- UpdateRemoteDestination is successful

Verify Remote Destination with a Wrong Route Pattern

- Route Pattern configured is 8.XXXX
- Application initiates AddRemoteDestination (OtherExtn, 91000, Active=True)
- CTI verifies 91000 and confirms that it is not reachable
- AddRemoteDestination is rejected (RD_NOT_REACHABLE)
- UpdateRemoteDestination reports a similar error

Verify Remote Destination with Conflicting Route Patterns

- Route Pattern configured is 9.XXXX
- Application initiates AddRemoteDestination (OtherExtn, 91000, Active=True)
- CTI verifies 91000 and confirms that it is reachable
- AddRemoteDestination is successful
- A similar UpdateRemoteDestination will be successful also

Verify Remote Destination with Typo Error by User

- Route Pattern configured is 9.XXXX
- Remote Destination the user intended to configure is 91000
- Application initiates AddRemoteDestination (OtherExtn, 91100, Active=True)
- CTI verifies 91100 and confirms that it is reachable

- AddRemoteDestination is successful
- A similar UpdateRemoteDestination be successful also
- A call initiated or offered from Remote Device will not be offered to 91000 because the Remote Destination is 91100

Persistent Connection Creation

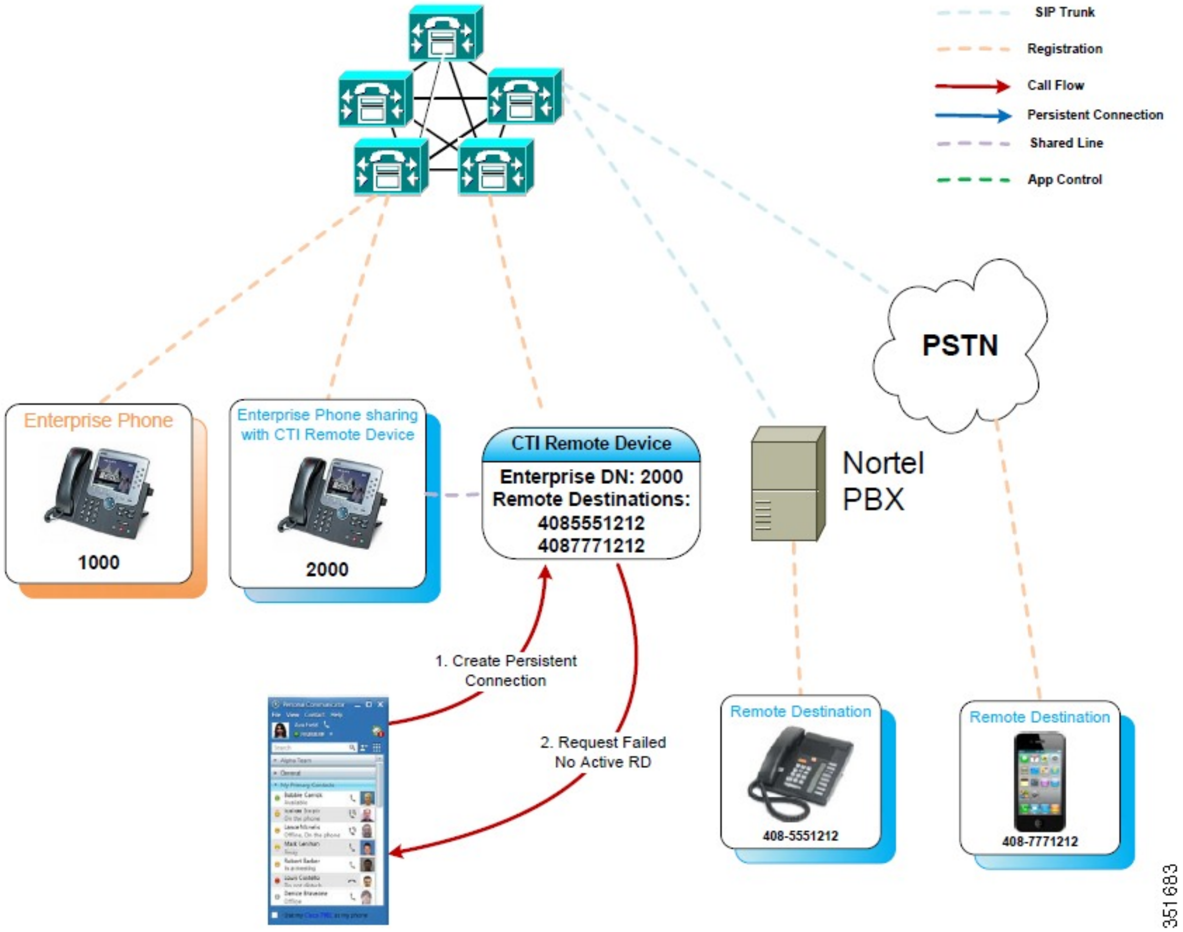
- A persistent connection must be created using a CTI application such as Contact Center Express/Enterprise
- Requirements
  - At least one Remote Destination (RD) must be configured
  - The RD must be Active
  - User may specify Calling Party Destination Number and Calling Party Name
- Any application can create a Persistent Connection, regardless of which application created the Active RD
- Use the Parking Lot to create the persistent connection
- If no Calling Party DN or Calling Party Name are specified, the default will be a Voice Connect with DN
- Only supports Remote Devices and Jabber in Extend Mode
- There is no admin configuration to allow Persistent Connection
- Remote Connection succeeds as soon the call is offered to a Remote Device
- A Persistent Connection Call answered by Voice Mail, Annunciator device inserted to avoid voice mail answers
- A Persistent Connection Call will not be offered to shared lines (such as DVO)
- A Persistent Connection will appear as RIU on shared lines after Remote Destination answers (such as DVO)
- Privacy on Hold will be false (such as DVO) so User can resume call from a desk phone
- A request to create a second Persistent Connection after the first one is successfully established will fail
- A request to create a second Persistent Connection when the first one is being setup will fail
- You can create a Persistent Connection on any line in the Remote Device
- A Persistent Connection will have a unique Global Call ID and Call ID, different from a typical call
- A Longest Active Call timer will drop the Persistent Connection when the timer expires
- Call features (such as Consult and Transfer) cannot be performed on a persistent connection, but are supported for a typical call when media is connected.
- A Persistent Connection cannot be included in other feature invocations such as Direct Transfer and Join
- After a Persistent Connection is answered, it will remain in the state as Connected for the duration of the call

- When the active remote destination is reset, a Persistent Connection call will drop if there are no other active calls. If there are active calls, it will drop after the current active call is dropped
- The Real-time Monitoring Tool will report the Persistent Connection call as an active call
- CDR for the Persistent Connection call should be updated for the entire lifetime of the call (not only when the Half call is cleared)
- A maximum of 8000 Persistent Connections can be created per cluster, or 2000 per node

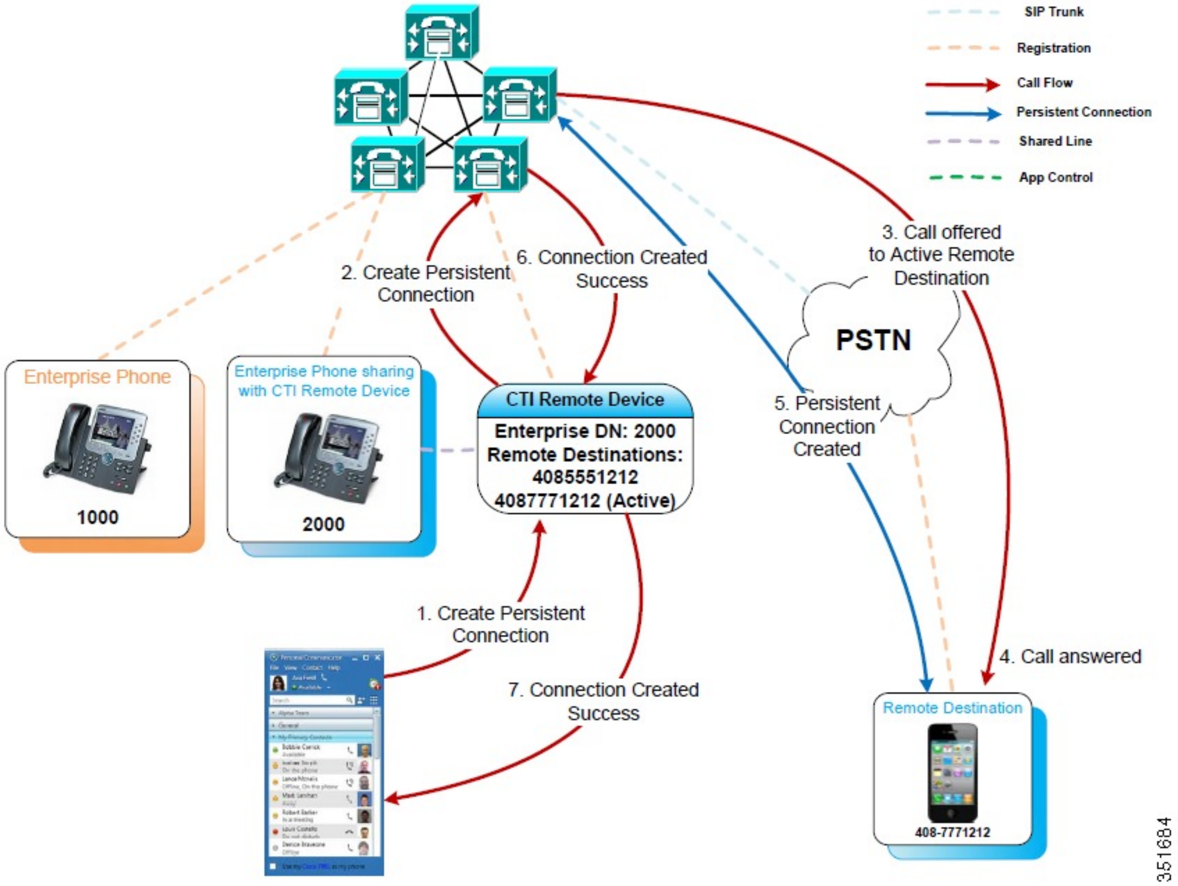
Persistent Connection Call Events

- When a Persistent Connection Call is offered
  - New Call Event (Attribute = Persistent Connection, Caller ID, Caller ID Name)
  - Call State (Offering)
  - Call State (Accepted)
- When the call is answered
  - Call State (Connected)

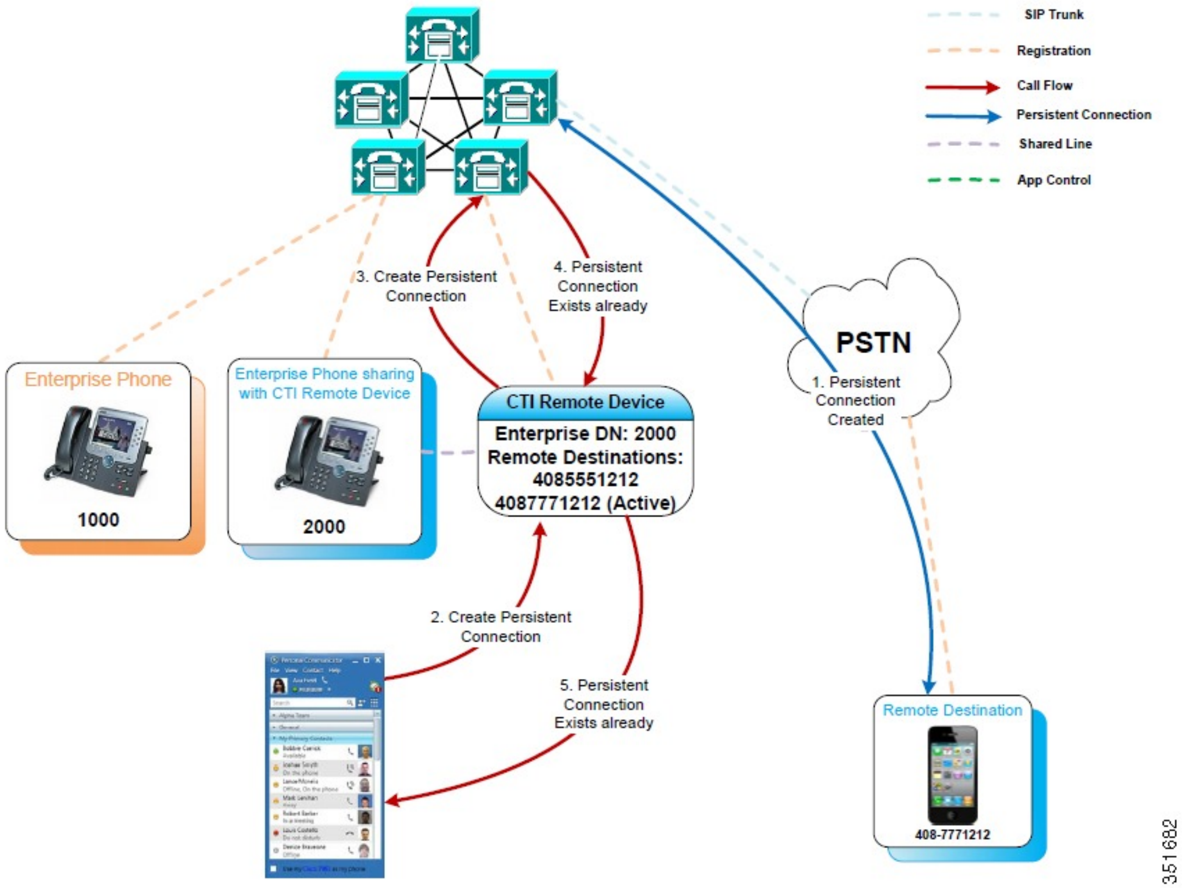
No Active Remote Destination Device



Active Remote Destination Device


SIP Trunk
Registration
Call Flow
Persistent Connection
Shared Line
App Control
2. Create Persistent Connection
6. Connection Created Success
3. Call offered to Active Remote Destination
PSTN
Enterprise Phone
1000
Enterprise Phone sharing with CTI Remote Device
2000
CTI Remote Device
Enterprise DN: 2000
Remote Destinations:
4085551212
4087771212 (Active)
5. Persistent Connection Created
1. Create Persistent Connection
7. Connection Created Success
4. Call answered
Remote Destination
408-7771212
351684

Persistent Connection Already Exists



Whisper Announcement

Whisper announcements Whisper announcements are played by CTI applications such as Contact Center Express/Enterprise. These announcements help agents answer the customer call with the appropriate greeting (for example, Customer Support – Spanish) or indicate when customer call media is connected (for example, zip tone).

Typical Use Cases

- Contact Center plays the zip tone before connecting customer to agent.
- Contact Center plays the Whisper Announcement before connecting customer to agent.

Requirements

- A CTI application, such as Contact Center Express/Enterprise, must be used to play the announcement.
- Announcement is configured on Cisco Unified CM Administration (**Media Resources** > **Announcement**).
- A persistent connection call is established and connected.
- No other active call is connected. A customer call may be ringing.

- Any call state change will stop the announcement.

CHAPTER 21

Extension Mobility

This chapter provides information about Cisco Extension Mobility which allows users to temporarily access their Cisco Unified IP Phone configuration such as line appearances, services, and speed dials from other Cisco Unified IP Phones. Extension Mobility supports Cisco Unified IP Phones that run SCCP and SIP.

Extension mobility functionality extends to most Cisco Unified IP Phones. You can configure each Cisco Unified IP Phone to support Cisco Extension Mobility by using the Default Device Profile window in Cisco Unified Communications Manager Administration. This allows users who do not have a user device profile for a particular Cisco Unified IP Phone to use Cisco Extension Mobility with that phone.

Note Check the Cisco Unified IP Phone documentation to verify that Cisco Extension Mobility is supported.

Configure Cisco Extension Mobility

Cisco Extension Mobility allows users to temporarily access their Cisco Unified IP Phone configuration such as line appearances, services, and speed dials from other Cisco Unified IP Phones.

Extension mobility functionality extends to most Cisco Unified IP Phones. You can configure each Cisco Unified IP Phone to support Cisco Extension Mobility by using the Default Device Profile window in Cisco Unified Communications Manager Administration. This allows users who do not have a user device profile for a particular Cisco Unified IP Phone to use Cisco Extension Mobility with that phone.

Note Check the Cisco Unified IP Phone documentation to verify that Cisco Extension Mobility is supported.

Perform the procedures in the order shown in the following steps to configure Cisco Extension Mobility. For more information on Cisco Extension Mobility, see the Cisco Extension Mobility Feature, on page 465 and the **Extension Mobility**.

Procedure

Step 1 Using Cisco Unified Serviceability, choose **Tools** > **Service Activation** to activate the Cisco Extension Mobility service.

Note To disable the extension mobility service on any node, you must first deactivate the service for that node in Service Activation.

Note When a change in activation or deactivation of the Cisco Extension Mobility service occurs, on any node, the database tables get updated with information that is required to build the service URLs. The database tables also get updated when the extension mobility service parameters get modified. The EMApp service handles the change notification.

Step 2 Create the Cisco Extension Mobility Service. Summary steps include

- Choose **Device** > **Device Settings** > **Phone Services**.
- Enter the service name (such as, Extension Mobility Service or EM).
- Enter the following URL: **`http://10.89.80.19:8080/emapp/EMAppServlet?device=#DEVICENAME#`**

Note If you should enter the URL incorrectly and subscribe the wrong service to the phones, you can correct the URL, save it, and press Update Subscriptions or correct the URL and resubscribe each phone to which the wrong service was subscribed.

- Select values for Service Category and Service Type.
  - For Service Category select “XML Service”.
  - For Service Type, select “Standard IP Phone Service.”
- Enter a value for Service Vendor (Java MIDlet services only).
- Click **Save.**

Note For Java MIDlet services, the service name and service vendor must exactly match the values that are defined in the Java Application Descriptor (JAD) file.

Step 3 Configure administration parameters.

Step 4 Create a default device profile for each phone type that you want to support Cisco Extension Mobility.

Step 5 Create the user device profile for a user. Summary steps include

- Choose **Device** > **Device Settings** > **Device Profile** and click **Add New**.
- Enter the Device Type.
- Enter the Device Profile Name, choose the phone button template, and click **Save.**
- Enter the directory numbers (DNs) and required information and click Save. Repeat for all DNs.

- To enable intercom lines for this device profile, configure intercom directory numbers (DNs) for this device profile. You configure an intercom DN in the Intercom Directory Number Configuration window, which you can also access by choosing **Call RoutingIntercomIntercom Directory Number**. You must designate a Default Activated Device in the Intercom Directory Number Settings pane for an intercom DN to be active.
- To subscribe the device profile to Cisco Extension Mobility, on the Device Profile Configuration Window, from the related links drop-down list (in the upper right corner of the window), choose “Subscribe/Unsubscribe Services” and click **Go**.

Note Subscribe the directory number and the device profile the same Extension Mobility service.

Step 6 Associate a user device profile to a user. Summary steps include

- Choose **User Management** > **End User** and click **Add New**; enter user information.
- In Extension Mobility Available Profiles, choose the user device profile that you created in **Configure Cisco Extension Mobility** and click the down arrow; this places the service that you chose in the Controlled Profiles box.
- Click **Save.**

Step 7 Configure and subscribe Cisco Unified IP Phone and user device profile to Cisco Extension Mobility. Summary steps include

- Subscribe the phone and the user device profile to Cisco Extension Mobility.
- Choose **Device** > **Phone** and click **Add New**

  .
- On the Phone Configuration window, in Extension Information, check Enable Extension Mobility.
- In the Log Out Profile drop-down list box, choose Use Current Device Settings or a specific configured profile and click **Save.**
- To subscribe Cisco Extension Mobility to the Cisco Unified IP Phone, go to the Related Links drop-down list box in the upper, right corner of the window and choose Subscribe/Unsubscribe Services; then, click **Go.**

Step 8 To allow a Cisco Extension Mobility end user to change the user PIN on the phone, configure the Change Credential Cisco Unified IP Phone service and associate the user, the user device profile, or the Cisco Unified IP Phone with the Change Credential phone service.

Cisco Extension Mobility Feature

This section provides information to configure and troubleshoot Cisco Extension Mobility, and includes information about the following:

- Cisco Extension Mobility and Extension Mobility equivalency
- Device profiles

- Login and logout behavior and call flow

Device Profiles

A device profile defines the attributes of a particular device. A device profile includes information such as the phone template, user locale, subscribed services, and speed dials.

The device profile does not get associated with a physical phone. It includes all the properties of a device except those that are explicitly tied to a device, such as MAC address or directory URL.

When a device profile has been loaded onto a device, the device adopts the attributes of that device profile.

User Device Profile

As system administrator, you configure a user device profile for each individual user. Using the Cisco Unified Communications Self Care Portal window, a user can access this profile and make changes, such as adding a service. You can add, modify or delete a user device profile in Cisco Unified Communications Manager Administration.

When a user logs in to a phone that is configured for Cisco Extension Mobility and the user has a user device profile that is configured for that phone, the user device profile replaces the existing configuration of the device.

When a user logs out, the logout profile replaces the user device profile.

Default Device Profile

You can configure a default device profile for each Cisco Unified IP Phone that you want to support Cisco Extension Mobility. The phone takes on the default device profile whenever a user logs in to a phone for which that user does not have a user device profile.

A default device profile includes device type (phone), user locale, phone button template, softkey template, and multilevel precedence and preemption (MLPP) information.

You create a default device profile by using the Default Device Profile Configuration window (**Device** > **Device Settings** > **Default Device Profile**). A phone can have zero or one default device profile. The maximum number of default device profiles cannot exceed the number of phones that support Cisco Extension Mobility.

Overview of Cisco Extension Mobility

Cisco Extension Mobility (an XML-based authentication feature) comprises the Cisco Extension Mobility application service and the Cisco Extension Mobility service. You need to activate the Cisco Extension Mobility service from Cisco Unified Serviceability to enable EM.

The Cisco Extension Mobility service runs as an application on the Cisco Tomcat Web Service.

You can activate and deactivate services from **Cisco Unified Serviceability** > **Service Activation**. See the *Cisco Unified Serviceability Administration Guide* for more information.

Note Cisco Extension Mobility works only between phones that are configured in Cisco Unified Communications Manager Administration.

Note Cisco Extension Mobility Cross Cluster works on phones that are located in different Cisco Unified Communications Manager clusters. For details about the Cisco Extension Mobility Cross Cluster feature, see the Extension Mobility Cross Cluster, on page 497 chapter.

You can use Cisco Unified Communications Manager Administration to start the Cisco Extension Mobility services (in Cisco Unified Serviceability administration), define how the features will work in your system (using the Service Parameters window [**System** > **Service Parameters**]), and define the phones that will support the feature (using the Default Device Profile window [**Device** > **Device Settings** > **Default Device Profile**]).

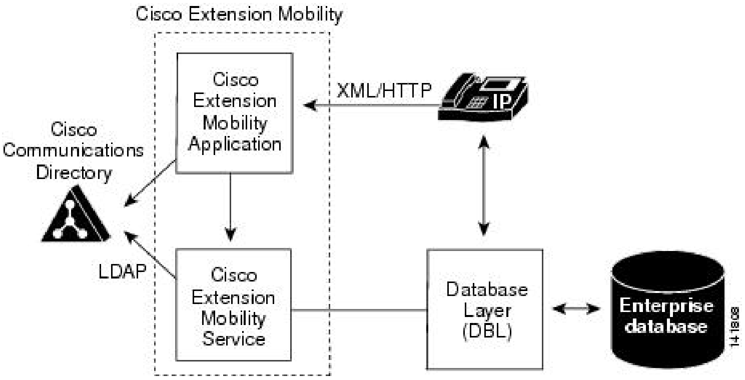
As a system administrator, you can configure a user device profile for each individual user. Using the Cisco Unified Communications Self Care Portal, a user can access this profile and make changes, such as adding a service like Cisco Extension Mobility.

Users access Cisco Extension Mobility by pressing the Services or Applications button on a Cisco Unified IP Phone and then entering login information in the form of a Cisco Unified Communications Manager UserID and a Personal Identification Number (PIN). If a user has more than one user device profile, a prompt displays on the phone and asks the user to choose a device profile for use with Cisco Extension Mobility.

If the user phone is subscribed to the Change Credential IP Phone service, the user can use the Change Credential IP Phone service to change the user PIN.

When a user logs in, the Cisco Extension Mobility application receives the XML-over-HTTP request for user authentication and verifies the information against the Cisco Unified Communications Manager Directory. (See the following figure.)

Figure 34: Cisco Extension Mobility


Cisco Extension Mobility
Cisco Extension Mobility Application
XML/HTTP
IP
Cisco Communications Directory
LDAP
Cisco Extension Mobility Service
Database Layer (DBL)
Enterprise database
141808

On authentication, if the login profile matches the login device (that is, the user has a user device profile that is configured for a Cisco Unified IP Phone 7975 and logs into a Cisco Unified IP Phone 7975), Cisco Extension Mobility behaves as follows:

- The phone automatically reconfigures with the individual user device profile information.

  If the user has one user device profile, the system uses this profile. If the user has more than one user device profile, the user can choose the user device profile that will be used from a list.

- The user can access all the services that the user configured on the device profile.

If that same user logs into a Cisco Unified IP Phone where the user does not have a configured user device profile, the login profile will not match the login device on authentication. In this scenario, the system loads the default device profile for that phone model onto the phone, and Cisco Extension Mobility works as described here:

- The system copies all device-independent configuration (that is, user hold audio source, user locale, userid, speed dials, and directory number configuration except for the setting “line setting for this device”) from the user device profile to the login device.
- The system uses the default device profile for that phone for phone template and softkey template configuration and, if the phone can support addon modules, for the addon module.
- If the login device supports feature safe on the phone button template and if the phone template that is configured in the login profile matches the number of buttons, the system uses the phone template from the login profile. Otherwise, the system uses the default device profile for the phone to configure the phone template.
- If the phone supports Cisco Unified IP Phone Services and they are configured, the system copies the services from the user device profile.

  If the user device profile does not have Cisco Unified IP Phone Services configured, the system uses the Cisco Unified IP Phone Services that are configured in the default device profile for the login device that is accessed during login. If parameters exist for the subscriber service, the system copies the parameters from the default device profile, and the parameters may not reflect the correct information.

For example, the following scenarios occur when a user who has a user device profile that is configured for Cisco Unified IP Phone 7975 logs in to a Cisco Unified IP Phone 7906, and the default device profile is loaded on the phone.

- The user can access the user hold audio source, user locale, userid, speed dials and directory number configuration. The user cannot access phone line setting; the system configured the phone line setting from the default device profile that is configured for the Cisco Unified IP Phone 7906.
- The user can access the phone template and the softkey template of the Cisco Unified IP Phone 7906.
- The user cannot access an addon module because Cisco Unified IP Phone 7906 does not support it.
- The user can access Cisco Unified IP Phone Services if they are configured for the Cisco Unified IP Phone 7906, but the parameters from the subscriber services will reflect the default device profile, not the parameters that the user chose on the Cisco Unified Communications Self Care Portal.

Users log out of Cisco Extension Mobility by pressing the **Services** button and choosing logout. If users do not log out themselves, the system will automatically log them out if you configured the Service Parameters to do so, or the next user of the phone can log out the previous user. After logout, Cisco Unified Communications Manager sends the logout profile to the phone and restarts the phone.

Secure Extension Mobility

The Extension Mobility HTTPS Support feature ensures that when communications are exchanged between a Cisco Unified IP Phone service and other applications, that the communications use the HTTPS protocol to ensure that the communications are secure. Users must log into the Cisco Unified CM applications by providing their authentication information. Their credentials are encrypted after the communication protocol changes to HTTPS.

When a visiting Extension Mobility (EM) application fails to locate a user's identification in the local database, the following event occurs:

1. Cisco Extension Mobility Cross Cluster (EMCC) sends a request to the local EM service to determine the home cluster of that user (the cluster which owns the user's identification, and which can handle the EM login).
2. The visiting EM service sends a user identification message over HTTPS to all the remote clusters added in the local database.
3. The visiting EM service then parses the response received from the home cluster to get the list of device profiles associated with that user.

   All further communication between the visiting EM service and home EM service takes place over HTTPS.

   Similarly, visiting logout requests are also sent from the home EM service to the visiting EM service over HTTPS.

The Extension Mobility HTTPS Support feature is supported on the following IP phones (SIP):

- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 9971

Note Configure Cisco Extension Mobility on Cisco Unified IP Phones before configuring EMCC.

Login and Logout Behavior

This section describes how login and logout works from the user perspective. Use this information to respond to questions or problems that users may encounter.

- Cisco recommends that you direct your users to log in to their phones at the beginning of the work day. This practice ensures that the user device profile gets loaded on the phone.
- If users make changes to their profiles on the Cisco Unified Communications Self Care Portal window, the changes will apply the next time that they log in.
- The system does not apply the change if the user is already logged in.
- If the User Locale that is associated with the login user or profile does not match the locale or device, after a successful login, the phone will perform a restart followed by a reset. This occurs because the phone configuration file gets rebuilt. Addon module mismatches between profile and device may generate the same behavior.
- Cisco Extension Mobility supports a maximum of 250 login or logout operations per minute (or 15,000 operations per hour). Remember that these operations are sequential, not concurrent. (Some devices may support more login or logout operations per hour.)
- You can establish a time limit, so Cisco Extension Mobility automatically logs out users, after a certain time. At the Enforce Maximum Login Time, choose True to specify a maximum time for logins and then set the maximum login time.

  See the Set the Service Parameters, on page 480.

- You can set the service parameter to allow for multiple logins. If you set multiple login not allowed, Cisco Extension Mobility supports only one login at a time for a user. Subsequent logins on other devices will fail until the user logs out on the first device.
- If Auto Logout is not enabled and if users forget to log out of a phone, as system administrator, you can log them out. Another user also can log them out when the second user tries to log in to that phone.
- If users are logged out of a Cisco Unified IP Phone that has the Cisco Extension Mobility feature configured for it, depending on the logout profile, they may not be able to check voice-messaging systems from that phone until they log in. If they receive a busy signal after pressing the Messages button or any key on the touchtone key pad, they must log in before using the phone.
- Users can log in to a phone that is off hook; however, their Cisco Unified IP Phone will not assume their settings until they go on hook. When they go on hook after logging in, their phone will display a "Resetting..." message, and their phone settings will be available from that phone.
- The Cisco Extension Mobility profile of a user does not maintain ring type, contrast settings, and volume settings; users configure these settings directly on the Cisco Unified IP Phone.
- When a Cisco Extension Mobility user logs out of a device, all Call Back services that are active on the Cisco Extension Mobility user automatically cancel.

Login Call Flow

This section describes the flow of events for the Cisco Extension Mobility login from a system perspective. Understanding the call flow will help you troubleshoot problems that you may have with the feature.

1. A user presses the Services or Applications button on the Cisco Unified IP Phone and requests to log in. This action invokes a URL for the Cisco Extension Mobility application.
2. The application determines the URL of the service.
3. The Cisco Extension Mobility application sends a formatted XML/HTTP query to the Cisco Extension Mobility service to determine the state of the phone.
4. The application prompts the user for UserID and PIN. The user enters the UserID and PIN and presses the Submit softkey.
5. The phone performs an HTTP request, and the application tries to authenticate the UserID and PIN.
6. If the UserID and PIN cannot be authenticated, the phone displays "Authentication Error."

   If the UserID and PIN are authenticated, the application queries the Cisco Unified Communications Manager Database to get the list of device profiles that are associated with the user.
7. The directory responds with the list of the user device profile(s). If the list has more than one entry, the phone displays the device profiles from which the user can choose.
8. When the user chooses an entry from this list (or if the list has only one entry), the application generates the XML for the service.
9. The application posts, via HTTP, the generated XML login request to the service URL. (The application determined the service URL in Step 2.)
10. The service responds in a defined XML format to the request with a restart to load the user device profile (that indicates success) or with a failure message.

11. The application returns the correct notification to the device. The phone restarts with the user device profile.

12. In the Phone Configuration window (**Device** > **Phone**) of Cisco Unified Communications Manager Administration, the Current End User Profile and the Current Device Profile, along with links to the applicable End User Profile and Device Profile configuration windows display.

Note In the Phone Configuration window, the line number of the device does not change when a user logs in to the phone. It continues to display the line number that is assigned to the phone when no user is logged in.

Logout Call Flow

This section describes the flow of events for the Cisco Extension Mobility logout from a system perspective. Understanding the call flow will help you troubleshoot any problems that you may have with the Cisco Extension Mobility feature.

1. A user presses the Services or Applications button on the Cisco Unified IP Phone and requests to log out. This action invokes a URL for the Cisco Extension Mobility application.

2. The application determines the URL of the service.

Note Cisco Extension Mobility looks up the URL in the Cisco Unified Communications Manager Directory on the first instance only; the system then stores the URL as a static variable.

3. The application generates the XML to query the Cisco Extension Mobility service for the current state of the device.

4. The service responds to the application with the current state of device; for example, <userID> is logged in.

5. The application prompts the user to confirm that the user wants to log out.

6. When the user presses the Yes softkey to confirm that the user wants to log out, the application generates XML for the logout operation.

7. The application posts, via HTTP, the generated XML login request to the service URL. (The application determined the service URL in Step 2.)

8. In the case of a successful operation, the phone will restart and load the appropriate device profile. If a failure occurs, a message gets sent to the phone.

9. The application parses the received XML and creates an XML response message.

10. The XML gets returned as a suitable notification to the device, and the phone restarts to load the original user profile or logout profile.

11. In the Phone Configuration window (**Device** > **Phone**) of Cisco Unified Communications Manager Administration, you (the administrator) will no longer see a Current End User Profile and Current Device Profile.

Note In the Phone Configuration window, the line number of the device does not change when a user logs out from the phone. It continues to display the line number that is assigned to the phone when no user is logged in.

Extension Mobility Equivalency

Cisco Extension Mobility (EM) equivalency eliminates the phone-model dependency of phone button templates. The following factors determine the model equivalency among the various phones:

- Various features that the phone models support
- Number of buttons that the phone models support

EM equivalency allows the user to use any phone button template that is configured on the system.

Cisco Unified Communications Manager enhances the existing Extension Mobility (EM) equivalency mechanism to work across both SCCP and SIP protocols on the following models:

- Cisco 7906
- Cisco 7941
- Cisco 7941G-GE
- Cisco 7942
- Cisco 7945
- Cisco 7961
- Cisco 7961G-GE
- Cisco 7962
- Cisco 7965
- Cisco 7970
- Cisco 7971
- Cisco 7975
- Cisco IP Communicator

The enhancement works for all phone models that are size safe and requires no administration tasks to activate.

Note The list of supported phone models varies per version and device pack. Log in to Cisco Unified Reporting to obtain the complete list of phone models that support these features in your installation. Within Cisco Unified Reporting, choose the Unified CM Phone Feature List system report. When generating this system report, specify All in the Product drop-down list box. In the Feature drop-down list box, specify Size Safe on Phone Template.

Size Safe Feature

If a phone model supports Size Safe on Phone Button Template, any phone button template can associate with that phone model. The actual phone button layout that displays on the phone shows the same order as the defined phone button template. If the phone model has more buttons than the phone button template, all defined buttons display. If the phone model has fewer buttons than the defined phone button template, only the buttons that are available on the phone display.

For example, a Cisco Unified IP Phone 7961 phone button template defines the following buttons:

- Line1
- Line2
- SD1
- SD2
- Line3
- Line4

When this phone button template gets assigned to a Cisco Unified IP Phone 7942, the actual phone button layout shows the following:

- Line1
- Line2

The rest of the template does not display because the buttons are not available.

When this phone button template gets assigned to a Cisco Unified IP Phone 7975, that actual phone button layout shows the following:

- Line1
- Line2
- SD1
- SD2
- Line3
- Line4
- Undefined
- Undefined

Thus, if a phone model supports the Size Safe on Phone Button Template feature, regardless of the login profile model, the user always sees the same order of the phone button template layout as that which gets defined with the login profile.

EM Equivalency During Login

Size safe phones use the template from the login profile and the template is applied as described in the preceding section.

Non-size safe phones must use the template that is associated with the default device profile for the model and protocol that matches the phone that the user logs into.

Note The device that the user logs into must support Size Safe on Phone Template for EM Equivalency. The capability of the EM Profile does not effect EM Equivalency during login.

System Requirements for Cisco Extension Mobility

Software Components

This version of Cisco Extension Mobility requires the following software components to operate:

- Cisco Unified Communications Manager 8.0 or later

Note Cisco Extension Mobility installs automatically on the same server with Cisco Unified Communications Manager. You do not require an additional server. Cisco Extension Mobility can run on any server in a Cisco Unified Communications Manager cluster.

- Netscape 7.1, Internet Explorer 6, or Internet Explorer 7 for Cisco Unified Communications Manager Administration
- Ensure the TFTP server is reachable. You can optionally install TFTP and Cisco Unified Communications Manager on the same server.

Extension mobility functionality extends to most Cisco Unified IP Phones. Check the Cisco Unified IP Phone documentation to verify that Cisco Extension Mobility is supported.

Backward Compatibility for Call Forward All Calling Search Space

An enhancement to Call Forward All calling search space (CSS) allows customers who are using Cisco Extension Mobility to 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 (**System** > **Service Parameters**), this parameter displays in the Clusterwide Parameters (Feature - Forward) section with two options.

- With Configured CSS (default)
- With Activating Device/Line CSS

For more information about configuration options for Call Forward All, see topics related to directory number configuration in the *Cisco Unified Communications Manager Administration Guide* and in the *Cisco Unified Communications Manager System Guide*.

Interactions and Restrictions

This section provides information about how Cisco Extension Mobility interacts with other Cisco Unified Communications Manager services and the restrictions that apply to Cisco Extension Mobility.

Interactions

This section describes how Cisco Extension Mobility reacts when running on more than one server, as well as the interaction with Cisco Unified Communications Manager application features such as the Bulk Administration Tool, CUCM Assistant, Call Display, Intercom, and IPv6.

CUCM Services Running on the Same Server

Cisco Extension Mobility can run on the same Cisco Unified Communications Manager server with Cisco Unified Communications Manager Assistant and CDR Analysis and Reporting (CAR).

Bulk Administration Tool

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 Cisco Unified Communications Manager Bulk Administration Guide for more information **.**

CUCM Assistant

A manager who uses Cisco Extension Mobility can simultaneously use Cisco Unified Communications Manager Assistant. The manager logs into 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). For more information about Cisco Unified Communications Manager Assistant, see the Cisco Unified Communications Manager Assistant with Proxy Line Support, on page 305 chapter.

Call Display Restrictions

When you enable Call Display Restrictions with Cisco Extension Mobility, 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 (**Device** > **Phone**).

To use Call Display restrictions with Cisco Extension Mobility, enable the Ignore Presentation Indicators (internal calls only) in both the Device Profile Configuration window (see the Create the Device Profile for a User, on page 489) and the Phone Configuration window (see the Subscribe Cisco Unified IP Phones to Cisco Extension Mobility, on page 492).

For more information about the Call Display Restrictions features, see the Call Display Restrictions, on page 103 chapter.

Intercom

Cisco Extension Mobility supports the Intercom feature. To do so, Cisco Extension Mobility uses a default device that is configured for an intercom line. An intercom line gets presented only on the default device.

You can assign an intercom line to a device profile. When a user logs on to a device that is not the default device, the intercom line does not get presented.

The following additional considerations apply to intercom for Cisco Extension Mobility:

- For an existing intercom line that is assigned to a device, migration from a Release 6.0(1) of Cisco Unified Communications Manager to Release 6.1(1) or later automatically designates the intercom default device for that intercom line.
- When Cisco Unified Communications Manager assigns an intercom line to a device and the default device value is empty, the current device gets selected as the default device.
- When assignment of an intercom DN takes place programatically through AXL, ensure the intercom DN is updated separately by using Cisco Unified Communications Manager Administration to set the default device.
- When deletion of a device that is set as the intercom default device for an intercom line occurs, the deletion completes, and the intercom default device will no longer be 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, make sure that you configure the phone with an IP Addressing Mode of IPv4 Only or IPv4 and IPv6. For more information on IPv6, see the Internet Protocol Version 6 (IPv6), on page 739.

Restrictions

The following restrictions apply to Cisco Extension Mobility:

- Cisco Extension Mobility works only between phones that are configured in Cisco Unified Communications Manager Administration.
- 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.
- Cisco Extension Mobility supports a limited number of special characters that can be entered on the phone for the login user ID. These characters include . (period), @, ~, *, &, %, #, +, $, \, the Euro sign, and the pound sterling sign.
- If the User Locale that is associated with the login user or profile is not the same as the locale or device, after a successful login, the phone will perform a restart followed by a reset. This occurs because the phone configuration file gets rebuilt. Addon module mismatches between profile and device may cause the same behavior.
- Cisco Extension Mobility requires a physical Cisco Unified IP Phone for login. Users of office phones that are configured with Cisco Extension Mobility cannot log in to their phones remotely.
- When a Cisco Extension Mobility user logs out of a device, all Call Back services that are active for the Cisco Extension Mobility user automatically cancel.

- When a migration from Cisco Unified CallManager Release 4.x to Cisco Unified Communications Manager Release 6.0 (or later) is done, the phones do not display the last login user IDs until users log in for the first time after the migration. When the service parameter “Remember the Last User Logged In” gets set to True, Cisco Extension Mobility displays the previous login user ID whenever the user logs in to the phone. This occurs based on a file on the hard disk. For the migration from Release 4.x to Release 6.0 (or later), this file does not get migrated to the database; therefore, the user ID of the previous login user does not display.
- If Cisco Extension Mobility gets stopped or restarted, the system does not auto log out users who are already logged in after the expiration of logout interval. For those phones, auto-logout happens only once in a day. You can manually log out these users from either the phones or from Cisco Unified Communications Manager Administration.
- Standard Extension Mobility (EM) Authentication Proxy Rights specifies both a standard role and a standard user group that are intended for use by applications that interact with Cisco Extension Mobility. Authentication by proxy does not support end-user authentication by proxy. Although you can add an end user to the Standard EM Authentication Proxy Rights user group, that end user does not get authorized to authenticate by proxy.
- Cisco Extension Mobility maintains a cache of all logged on user information for 2 minutes. If a request comes to extension mobility regarding a user who is represented in the cache, the user gets validated with information from the cache. This means that, if a user changes the password, logs out, and then logs back in within 2 minutes, both the old and new passwords get recognized.

Install Cisco Extension Mobility

When you install Cisco Unified Communications Manager, make sure that you also install the Cisco Unified Communications Manager Locale Installer on every server. Installing the Locale Installer ensures that you have the latest translated text that is available for user windows and phone displays. For more information, see the Cisco Unified Communications Operating System Administration Guide.

Now, perform the procedures in the Cisco Extension Mobility Configuration, on page 477.

Cisco Extension Mobility Configuration

This section contains information to configure Cisco Extension Mobility and includes guidelines, examples, and procedures.

Tip Before you configure Cisco Extension Mobility, review the Cisco Extension Mobility configuration task summary.

Related Topics

Configure Cisco Extension Mobility, on page 463

Configuration Guidelines

To avoid problems with deploying Cisco Extension Mobility, be sure to follow these configuration guidelines:

- Configure a Default Device Profile for each Cisco Unified IP Phone type that you want to support Cisco Extension Mobility.
- If you want to enable all phones for Cisco Extension Mobility, do not allow the users to control these phones.
    - In this scenario, when users go to their Cisco Unified Communications Self Care Portal window to change their services, they must choose the Device Profiles option from the Select a device to configure drop-down list box. They cannot control an individual phone nor modify the settings for an individual phone.
    - As administrator, you can change the services for a phone by using Cisco Unified Communications Manager Administration. After making the changes, if you update on the main window (not the popup menu), you must reset the phone for the changes to take effect. This action ensures that the new snapshot gets stored as the logout profile.
- If a particular user controls a device, for example, the user office phone, do not allow anyone else to log in to that device.

Caution The Cisco Extension Mobility feature does not operate properly if you allow users to access the assigned phone of another user.

- For information on Cisco Extension Mobility redundancy, see the Cisco Unified Communications Solution Reference Network Design (SRND).

Configuration Example 1

In a typical Cisco Extension Mobility scenario,

- All employees represent users of Cisco Extension Mobility.
- All users have a user device profile.
- Users do not control individual phones, and they cannot modify settings for an individual phone.
- Before a user can use a phone, the user needs to log in.
- Users can access common devices, such as lobby phones, conference room phones, and cubicle phones that are meant to be shared.
- When users go to their Cisco Unified Communications Self Care Portal window to change services or speed dials, they can choose only their device profiles from the “Select a device to configure” drop-down menu. This method ensures that changes that users make to their services will follow them to any Cisco Unified IP Phone after they log in.

Configuration Example 2

In another typical Cisco Extension Mobility scenario,

- Each user has an assigned phone.
- Each user has a device profile that follows the user to every device to which the user logs in.

- Each user can access common devices, such as lobby phones, conference room phones, and cubicle phones that are configured to be shared.
- In this scenario, no one can use the assigned phone of anyone else.

Add the Cisco Extension Mobility Service

Add the Cisco Extension Mobility service as a new Cisco Unified IP Phone Service. Configure a name, description, and the URL for the Cisco Extension Mobility service.

Tip When you subscribe devices to the Cisco Extension Mobility service, an error results if you click Update Subscriptions more than once. When you update many phones, it can take some time for the changes to propagate to all devices. You must click Update Subscriptions only once and wait for this propagation to complete.

To add the Cisco Extension Mobility service, perform the following steps:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Device** > **Device Settings** > **Phone Services**.

Step 2 Click **Add New**.

Step 3 At the Service Name field, enter a name for the service.

The user receives this name on the phone when the user presses the Services button. Use a meaningful name; for example, 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 At the ASCII Service Name field, enter the name of the service to display if the phone cannot display Unicode.

Step 5 Enter the Service URL field as it displays in the following example:

http://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#

where IP Address of Extension Mobility server specifies the IP Address of the Cisco Unified Communications Manager where Cisco Extension Mobility Application is activated and running.

For example:

http://123.45.67.89:8080/emapp/EMAppServlet?device=#DEVICENAME#

Tip To provide redundancy for the Cisco Unified IP Phone Service, create a Cisco Unified IP Phone Service that uses the host name rather than the IP address. The phone functionality for softkeys and filtering, as well as the phone service, will fail over automatically in the case of a failover.

Step 6 At the Service Category field, select whether the service is based on XML or Java MIDlet.

Step 7 At the Service Type field, select whether the service will be provisioned to the Services, Directories, or Messages button.

Step 8 For Java MIDlet services only, at the Service Vendor field, enter the service vendor that exactly matches the vendor that is defined in the JAD file. You can leave this field blank for XML services.

Note Be aware that entering a value for Service Version is not required. If you enter a value for a Java MIDlet service, the value must exactly match the version that is defined in the JAD file.

Step 9 Click **Save.**

Set the Service Parameters

Set the service parameters to define how the Cisco Extension Mobility service will work.

Be sure that you activate the Cisco Extension Mobility service before you configure the service parameters. See the Cisco Unified Serviceability Administration Guide for information about using Cisco Unified Serviceability.

To set the Service Parameters for Cisco Extension Mobility, choose **System** > **Service Parameters** in Cisco Unified Communications Manager Administration; choose the server that is running the Cisco Extension Mobility service, and then Cisco Extension Mobility. To display all service parameters, click **Advanced**. After you configure the service parameters, click **-**

The following table describes the Cisco Extension Mobility service parameters.

Note Service parameters with “intra-cluster” in the name apply to the Cisco Extension Mobility feature. Service parameters with “inter-cluster” in the name apply only to the Cisco Extension Mobility Cross Cluster feature.

Table 51: Service Parameters for Cisco Extension Mobility Service

Setting	Description
Enforce Intra-cluster Maximum Login Time	Choose True to specify a maximum time for local logins. After this time, the system automatically logs out the device. Choosing False, which is the default setting, means that no maximum time for logins exists. To set an automatic logout, you must choose True for the Enforce Intra-cluster Maximum Login Time 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.

Setting	Description
Intra-cluster Maximum Login Time	This parameter specifies the maximum time that a user is allowed to be locally logged in to a device, such as 8:00 (8 hours) or :30 (30 minutes). The system ignores this parameter if the Enforce Intra-cluster Maximum Login Time parameter is set to False. Valid values specify 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.
Inter-cluster Maximum Login Time	This field applies only to Extension Mobility Cross Cluster (EMCC) configuration. This parameter specifies the maximum time that a user is allowed to be remotely logged in to a device, such as 8:00 (8 hours) or :30 (30 minutes). EMCC always enforces auto logout based on this value, regardless of the value of Enforce Intra-cluster Maximum Login Time service parameter. Valid values specify between 0:00 and 168:00 in the format HHH:MM where HHH represents the number of hours and MM represents the number of minutes. (0:00 means indefinite logon: you will remain logged on without a maximum login time.)
Maximum Concurrent Requests	**Tip** In the Service Parameter Configuration window, click Advanced to display this service parameter. 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, which specifies 5, addresses most scenarios adequately.
Intra-cluster Multiple Login Behavior	Choose one of the following options: **1.** Multiple Logins Allowed - A user can log in to more than one device at a time. **2.** Multiple Logins Not Allowed - The second and subsequent login attempts after a user successfully logs in once will fail. **3.** 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.

Setting	Description
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 lower case.
Remember the Last User Logged In	Choose the default value, False. In a typical hoteling scenario, where users can come into any office and use any phone on a temporary basis, you should set this parameter to False. A True setting specifies that the extension mobility application remembers the user ID of the last user that logged in to the phone. Use this setting in situations where individuals use their own phone on a regular basis, and no one else uses that phone. For example, Cisco Extension Mobility could be 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, and you would set the field to True. When the field is set to True, all future logins will cause the user ID of the last successful logged-in user to automatically get filled in and remembered by Cisco Extension Mobility.

Setting	Description
Clear Call Logs on Intra-cluster EM	Choose True to specify that the call logs are cleared during the Cisco Extension Mobility manual login/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 user privacy by preventing other users of the same phone from seeing the call logs of the previous user, set the Clear Call Log service parameter to True. This ensures that the call logs get cleared when a successful login/logout occurs. 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 get cleared only during manual Cisco Extension Mobility login/logout. If a Cisco Extension Mobility logout occurs due to an automatic logout or any occurrence other than a manual logout, the call logs do not get cleared.

Setting	Description
Validate IP Address	**Tip** In the Service Parameter Configuration window, click Advanced to display this service parameter. This parameter specifies whether validation of the IP address of the source that is requesting login or logout occurs. If the parameter specifies true, the IP address from which a Cisco Extension Mobility log in or log out request is made gets validated to ensure that it is a trusted IP address. Validation gets first performed against the cache for the device to be logged in or logged out. If the requesting source IP address is not found in cache, the IP address gets checked against the list of trusted IP addresses and host names specified in the Trusted List of IPs service parameter. If the requesting source IP address is not present in the Trusted List of IPs service parameter, it is checked against the list of devices registered to Cisco Unified CallManager. If the IP address of the requesting source is found in the cache or in the list of trusted IP addresses or is a registered device, the device is allowed to perform login or logout. If the IP address is not found, the log in or log out attempt is blocked. If the parameter specifies false, the Cisco Extension Mobility log in or log out request does not get validated. Validation of IP addresses may increase the time required to log in or log out a device, but it offers an additional layer of security in the effort to prevent unauthorized log in or log out attempts, especially when used in conjunction with log ins from separate trusted proxy servers for remote devices. **Note** When PSIRT (Validate IP Address) is set to true, autologout does not go through the PSIRT validation path. The EM logs show that the phone signs out without PSIRT information. This scenario explains why the user signed out automatically instead of manually signing out.

Setting	Description
Trusted List of IPs	**Tip** In the Service Parameter Configuration window, click Advanced to display this service parameter. This parameter displays as a text box (maximum length - 1024 characters). You can enter strings of trusted IP addresses or host names, separated by semi-colons, in the text box. IP address ranges and regular expressions do not get supported.
Allow Proxy	**Tip** In the Service Parameter Configuration window, click Advanced to display this service parameter. If the parameter specifies true, the Cisco Extension Mobility log in and log out operations using a web proxy are allowed. If the parameter specifies false, the Cisco Extension Mobility log in and log out requests coming from behind a proxy get rejected. The setting you select takes effect only if the Validate IP Address parameter specifies true.
EMCC Allow Proxy	**Tip** In the Service Parameter Configuration window, click Advanced to display this service parameter. This field applies only to Extension Mobility Cross Cluster configuration. This parameter determines whether the use of web proxy for Extension Mobility Cross Cluster (EMCC) login/logout is allowed. The service parameter, Validate IP Address, must be set to True for this parameter to take effect. Valid values specify True (allow EMCC login or logout using a web proxy that is identified in the service parameter Trusted List of IPs) or False (do not allow EMCC login or logout operation using a web proxy).
Extension Mobility Cache Size	**Tip** In the Service Parameter Configuration window, click Advanced to display this service parameter. In this field, configure 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 specifies 10000. The value you enter takes effect only if the Validate IP Address parameter specifies true.

Cisco Extension Mobility Service Parameters

The following table provides a comparison of the Cisco Extension Mobility service parameters and how each service parameter behaves when used to configure the Extension Mobility feature or the Extension Mobility Cross Cluster feature.

Table 52: Comparison of Cisco Extension Mobility Service Parameter Behavior

Service Parameter Name	Behavior in Extension Mobility Feature	Behavior in Extension Mobility Cross Cluster Feature
Enforce Intra-cluster Maximum Login Time	Supported (True or False)	Does not apply. EMCC always enforces auto logout based on the inter-cluster maximum login time.
Intra-cluster Maximum Login Time	Value gets used if maximum login time is enforced.	Does not apply.
Inter-cluster Maximum Login Time	Does not apply.	This service parameter shares the same range for Intra-cluster Maximum Login Time, except that it can be set to zero.
Maximum Concurrent Requests	Supported. This service parameter combines both EM and EMCC login requests.	Supported. This service parameter combines both EM and EMCC login requests. This service parameter applies only to the home cluster.
Intra-cluster Multiple Login Behavior	Supported. Values specify the following: • Multiple Logins Allowed • Multiple Logins Not Allowed • Auto Logout	Always allows multiple EMCC logins (Multiple Login Allowed).
Alphanumeric User ID	Supported	Supported. Value of visiting cluster gets used.
Remember the Last User Logged In	Supported	Supported
Clear Call Logs on Intra-Cluster EM	Supported. Values specify the following: • True = Clear the call history. • False = Do not clear call history after login and logout.	Always get cleared once the phone runs the full cycle reset after login.
Validate IP Address	Supported. Validates the IP address of the device during login and logout.	Supported. Validates the IP address in the visiting cluster (vEMApp) during login. Validates the IP address in the home cluster (hEMApp) during logout.

Service Parameter Name	Behavior in Extension Mobility Feature	Behavior in Extension Mobility Cross Cluster Feature
Trusted List of IPs	Supported	Supported. Works in conjunction with Validate IP Address parameter. The parameter of home cluster or visiting cluster gets applied, depending on login or logout.
Allow Proxy	Supported	Does not apply.
EMCC Allow Proxy	Does not apply.	Supported
Extension Mobility Cache Size	Supported. Values specify the following: • Multiple Logins Allowed • Multiple Logins Not Allowed • Auto Logout	Supported. Uses the Max Cache Size value in the home cluster.

Create a Default Device Profile

Configure a default device profile for each type of Cisco Unified IP Phone that you want to support Cisco Extension Mobility. The phone takes on the default device profile whenever a user logs in to a phone type for which the user has no user device profile.

For more information on how Default Device Profiles work, see the Overview of Cisco Extension Mobility, on page 466.

To add a default device profile for a phone type, perform the following procedure.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Device** > **Device Settings** > **Default Device Profile**.

The Default Device Profile Configuration window displays.

Step 2 From the Device Profile Type drop-down list box, choose the device (such as a Cisco 7970) to which a profile gets created.

Step 3 Click **Next.**

Step 4 If applicable, from the Device Protocol drop-down list box, choose a protocol.

Step 5 Click **Next.**

Step 6 From the User Hold Audio Source field, choose from the drop-down list box to specify the audio source that plays when a user initiates a hold action.

If you do not choose an audio source, Cisco Unified Communications Manager uses the audio source that is defined in the device pool or, if the device pool does not specify an audio source ID, the system default.

Tip You define audio sources in the Music On Hold Audio Source Configuration window. For access, choose **Media Resources** > **Music On Hold Audio Source**.

Step 7 At the User Locale drop-down list box, 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. Cisco Unified Communications Manager makes this field available only for phone types that support localization.

Note If no user locale is specified, Cisco Unified Communications Manager uses the user locale that is associated with the device pool.

Note 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 Cisco Unified Communications Operating System Administration Guide.

Step 8 At the Phone Button Template field, choose the appropriate phone button template. The phone button template determines the configuration of the phone buttons on Cisco Unified IP Phones.

Step 9 At the Softkey Template field, choose the appropriate softkey template. The softkey template determines the configuration of the softkeys on Cisco Unified IP Phones. Choose None if you want to use the softkey profile that is configured in Common Device Configuration.

Step 10 From the Privacy drop-down list box, choose **On** for each phone that wants Privacy. For more configuration information, see the Barge and Privacy, on page 1.

Step 11 From the Single Button Barge drop-down list, choose one of the following options:

a) **Off** -This device does not allow users to use the Single Button Barge/cBarge feature.
b) **Barge** -Choosing this option allows users to press the Single Button Barge shared-line button on the phone to barge in to a call by using Barge.
c) **cBarge** -Choosing this option allows users to press the Single Button cBarge shared-line button on the phone to barge in to a call by using cBarge.
d) **Default** -This device inherits the Single Button Barge/cBarge setting from the service parameter.

For more configuration information, see the Barge and Privacy, on page 1.

Step 12 From the Join Across Lines drop-down list, choose one of the following options:

a) **Off** -This device does not allow users to use the Join Across Lines feature.
b) **On** -This device allows users to join calls across multiple lines.
c) **Default** -This device inherits the Join Across Lines setting from the service parameter.

For more information, see Barge and Privacy, on page 1 in the Cisco Unified Communications Manager System Guide.

Step 13 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.

Note 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 Call Display Restrictions, on page 103 chapter.

Step 14 To configure Multilevel Precedence and Preemption (MLPP) information, perform the following tasks:

Note See the Multilevel Precedence and Preemption, on page 907 for more information.

a) At the MLPP Domain, use the drop-down list box to choose the MLPP domain that is associated with this device profile.

b) If available, the MLPP Indication setting specifies whether a device will use the capability when it places the MLPP precedence call.

From the drop-down list box, choose a setting from the following options to assign to devices that use this default device profile:

- **Default** -This device inherits its MLPP indication setting from its device pool.
- **Off** -This device does not send indication of an MLPP precedence call.
- **On** -This device does send indication of an MLPP precedence call.

Note Do not configure a default device profile with the following combination of settings: MLPP Indication is set to Off while MLPP Preemption is set to Forceful.

c) If available, the MLPP Preemption setting specifies whether a device that is capable of preempting calls in progress will use the capability when it places an MLPP precedence call.

From the drop-down list box, choose a setting from the following options to assign to devices that use this default device profile:

- **Default** -This device inherits its MLPP preemption setting from its device pool.
- **Disabled** -This device does not preempt calls in progress when it places an MLPP precedence call.
- **Forceful** -This device preempts calls in progress when it places an MLPP precedence call.

Note Do not configure a default device profile with the following combination of settings: MLPP Indication is set to Off while MLPP Preemption is set to Forceful.

Step 15 Click **Save**.

Create the Device Profile for a User

The User Device Profile contains attributes such as name, description, phone template, addon modules, directory numbers, subscribed services, and speed-dial information.

To add a default device profile for a new user of Cisco Extension Mobility, perform the following procedure.

Note If you configure BLF speed-dial buttons in the Device Profile Configuration window, a device that supports Cisco Extension Mobility can display the real-time status of the BLF speed-dial buttons after you log in to the device; that is, if the Presence Group that is applied to the device profile allows you to view the status of the presence entity. See the BLF Presence, on page 17 chapter for more details.

Before you begin

Before proceeding, you must ensure that a device profile name and phone button template(s) are configured.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Device** > **Device Settings** > **Device Profile**.

The Find and List Device Profiles window displays.

Step 2 Click **Add New**.

The Device Profile Configuration window displays.

From the Device Profile Type drop-down list box, choose the device type and click **Next.**

If applicable, from the Device Protocol field, choose a protocol.

Click **Next.**

Step 3 At the Device Profile Name field, enter a name of your choice for the device profile. You can make this text anything that describes this particular user device profile, such as “Extension Mobility.”

Step 4 At the User Locale drop-down list box, 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. Cisco Unified Communications Manager makes this field available only for phone models that support localization.

Note If no user locale is specified, Cisco Unified Communications Manager uses the user locale that is associated with the device pool.

Note 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 Cisco Unified Communications Operating System Administration Guide.

Step 5 At the Phone Button Template field, choose the appropriate phone button template. The phone button template determines the configuration of the phone buttons on Cisco Unified IP Phones.

Step 6 From the Softkey Template drop-down list box, choose a softkey template. If you want to use the softkey template that is configured in the Common Device Configuration, choose None.

Step 7 From the Privacy drop-down list box, choose **On** for each phone that wants Privacy. For more configuration information, see the Barge and Privacy, on page 1.

Step 8 To enable the Call Display Restrictions feature, check the Ignore Presentation Indicators (internal calls only) check box.

Note To enable the Call Display Restrictions feature, check the Ignore Presentation Indicators (internal calls only) check box on the Device Profile Configuration window and also on the Phone Configuration window (see the Subscribe Cisco Unified IP Phones to Cisco Extension Mobility, on page 492).

Step 9 If the phone type supports Cisco Unified IP Phone Expansion Modules, Cisco Unified Communications Manager displays expansion module field. At the Module 1 drop-down list box and at the Module 2 drop-down list box, choose the appropriate expansion module.

Skip this step for Cisco IP Phone models 8961, 9951, and 9971. The expansion module field does not display for these phone models. The lines from the Phone Button Template are applied to the physical device no matter which expansion modules these phones use.

Tip You may view a phone button list at any time by choosing the View button list link next to the phone button template fields. A separate window pops up and displays the phone buttons for that particular expansion module.

Step 10 To configure Multilevel Precedence and Preemption (MLPP) information, perform the following tasks:

See the Multilevel Precedence and Preemption, on page 907 for more information.

a) From the MLPP Domain drop-down list box, choose a hexadecimal value for the MLPP domain that is associated with this device profile.
b) If available, the MLPP Indication setting specifies whether a device will use the capability when it places the MLPP precedence call.

From the drop-down list box, choose a setting from the following options to assign to devices that use this default device profile:

- **Default** -This device inherits its MLPP indication setting from its device pool.
- **Off** -This device does not send indication of an MLPP precedence call.
- **On** -This device does send indication of an MLPP precedence call.

Note Do not configure a default device profile with the following combination of settings: MLPP Indication is set to Off while MLPP Preemption is set to Forceful.

c) If available, the MLPP Preemption setting specifies whether a device that is capable of preempting calls in progress will use the capability when it places an MLPP precedence call.

From the drop-down list box, choose a setting from the following options to assign to devices that use this default device profile:

- **Default** -This device inherits its MLPP preemption setting from its device pool.
- **Disabled** -This device does not preempt calls in progress when it places an MLPP precedence call.
- **Forceful** -This device preempts calls in progress when it places an MLPP precedence call.

Note Do not configure a default device profile with the following combination of settings: MLPP Indication is set to Off while MLPP Preemption is set to Forceful.

Step 11 From the Login User Id drop-down list box, choose a user ID.

Click **Save.**

The page refreshes.

Step 12 From the Association Information section, click the **Add a new DN** link.

Step 13 At the Directory Number field, enter the directory number and click **Save.**

See Multilevel Precedence and Preemption, on page 907 in the Cisco Unified Communications Manager Administration Guide for field descriptions.

Step 14 The following prompt displays: Changes to Line or Directory Number settings require restart.

Click **Reset** and follow the prompts.

Step 15 To subscribe the Extension Mobility service to this device profile, go to the Related Links drop-down list box in the upper, right corner of the window and choose Subscribe/Unsubscribe Services; then, click **Go.**

A separate Subscribed Cisco IP Phone Services for window displays.

Step 16 From the Select a Service drop-down list box, choose the Extension Mobility service.

Step 17 Click **Next.**

Step 18 Click **Subscribe.**

The new service displays under Subscribed Services.

Step 19 Click **Save.**

Step 20 To unsubscribe a service, click **Unsubscribe and Save**.

See the Multilevel Precedence and Preemption, on page 907 chapter in the Cisco Unified Communications Manager Administration Guide for more details of configuring a device profile.

Associate a User Device Profile to a User

You associate a User Device Profile to a user in the same way that you associate a physical device. For more details, see the Multilevel Precedence and Preemption, on page 907 section in the Cisco Unified Communications Manager Administration Guide.

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 Cisco Unified Communications Manager Bulk Administration Guide for more information **.**

To associate a user device profile to a user for Cisco Extension Mobility, follow these steps:

Procedure

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

Step 2 Click **Add New**.

Step 3 Enter the appropriate settings as described in Multilevel Precedence and Preemption, on page 907 in the Cisco Unified Communications Manager Administration Guide.

Step 4 To save your changes and add the user, click **Save.**

Note To choose an existing end user, click **Find** and then choose the end user to whom you want to associate a user device profile. See the Cisco Unified Communications Manager Administration Guide.

Subscribe Cisco Unified IP Phones to Cisco Extension Mobility

Before you begin

You must configure the Cisco Unified IP Phones in Cisco Unified Communications Manager before you subscribe the phones to Cisco Extension Mobility. To configure the phones, see topics related to Cisco Unified IP Phone configuration in the *Cisco Unified Communications Manager Administration Guide*.

For a review of device profiles, see the Device Profiles, on page 466.

To subscribe to the Cisco Extension Mobility service, perform the following procedure.

Procedure

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

Step 2 Click **Add New**.

Note You can also search and update a configured phone as described in the *Cisco Unified Communications Manager Administration Guide*.

The Add a New Phone window displays.

Step 3 From the Phone Type drop-down list box, choose the phone type to which you want to subscribe extension mobility and click **Next.**

Step 4 From the Select the device protocol drop-down list box, choose the protocol of the phone and click **Next.**

Step 5 In Extension Information, check the Enable Extension Mobility check box.

Note For descriptions of all fields, see topics related to configuring Speed-Dial buttons or Abbreviated Dialing in the *Cisco Unified Communications Manager Administration Guide*.

Step 6 From the Log Out Profile drop-down list box, choose the profile that you want the phone to use when no extension mobility user is logged in. You can choose either Use Current Device Settings or one of the specific configured profiles that are listed.

Note If you select a specific configured profile, a mapping between the login device and the login profile gets retained after the user logs out. If you select Use Current Device Settings, no mapping gets retained.

The remaining fields show the current device information with regard to the login status of the device: Log in Time, Log out Time.

Step 7 On the Cisco Unified Communications Manager Phone Configuration window, to enable the Call Party Restrictions feature, check the Ignore Presentation Indicators check box.

Note To enable the Call Display Restrictions feature, check the Ignore Presentation Indicators (internal calls only) check box on the Phone Configuration window and also on the Device Profile Configuration window (see the Create the Device Profile for a User, on page 489). For information about this feature, see the Call Display Restrictions, on page 103 chapter.

Step 8 Click **Save.**

You must now subscribe the extension mobility IP phone service to both the device profile that you created in the Create the Device Profile for a User, on page 489 and to the IP phone target device.

Step 9 To subscribe extension mobility to the IP phone, go to the Related Links drop-down list box in the upper, right corner of the window and choose Subscribe/Unsubscribe Services; then, click **Go.**

A separate Subscribed Cisco IP Phone Services for window displays.

Step 10 From the Select a Service drop-down list box, choose the Extension Mobility service.

Step 11 Click **Next.**

Step 12 Click **Subscribe.**

The new service displays under Subscribed Services.

Step 13 Click **Save.**

Step 14 To unsubscribe a service, click **Unsubscribe** and **Save.**

Note To subscribe/unsubscribe services to a device profile, see the Create the Device Profile for a User, on page 489

You have now configured Cisco Extension Mobility.

Configure the Change Credential IP Phone Service

Configure the Change Credential IP Phone service and associate this phone service with a user, a user device profile, or a Cisco Unified IP Phone, so that a Cisco Extension Mobility user can change the user PIN on the Cisco Unified IP Phone to which they have logged in.

The Change Credential IP phone service allows an end user to change the user PIN on the Cisco Unified IP Phone with both Cisco Extension Mobility and Cisco Extension Mobility Cross Cluster.

Before you begin

You must configure the Cisco Unified IP Phones in Cisco Unified Communications Manager before you subscribe the phones to Cisco Extension Mobility. To configure the phones, see the Cisco Unified Communications Manager Administration Guide.

For a review of device profiles, see the Device Profiles, on page 466.

To add the Change Credential IP Phone service, perform the following procedure.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Device** > **Device Settings** > **Phone Services**.

Step 2 Click **Add New**.

The IP Phone Services Configuration window displays.

Step 3 In the Service Name field, enter Change Credential.

Note For descriptions of all fields, see the Device Profiles, on page 466 section in the Cisco Unified Communications Manager Administration Guide.

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 In the Secure-Service URL field, enter the following value, where server designates 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 click **Save.**

You must now subscribe the Change Credential IP phone service to both the IP phone target device and to the user device profile that you created in the Create the Device Profile for a User, on page 489.

Step 7 To subscribe the Cisco Unified IP Phone to the Change Credential IP phone service, display the Phone Configuration window for the phone (**Device** > **Phone**).

Step 8 In the Phone Configuration window, go to the Related Links drop-down list box in the upper, right corner of the window and choose Subscribe/Unsubscribe Services; then, click **Go.**

A separate Subscribed Cisco IP Phone Services for window displays.

Step 9 From the Select a Service drop-down list box, choose the Change Credential IP phone service.

Step 10 Click **Next.**

Step 11 Click **Subscribe.**

Step 12 The Change Credential IP phone service displays under Subscribed Services.

Step 13 Click **Save.**

Note To subscribe/unsubscribe services to a user device profile, see the Create the Device Profile for a User, on page 489.

Note To subscribe/unsubscribe services to an end user, see the Cisco Unified Communications Manager Administration Guide.

Provide Information to Cisco Extension Mobility Users

After you have configured the system for Cisco Extension Mobility, provide your phone users with the following information:

- Notification of feature availability and the phone types that support Cisco Extension Mobility. Include the name that you gave the Cisco Extension Mobility feature (for example, extension mobility). In addition, notification of changes with respect to activation and deactivation of extension mobility service.
- User password, UserID, and PIN
- URL for the Cisco Unified Communications Self Care Portal window for the user to change user password and PIN

Note Be aware that user passwords and PINs can only contain characters that the IP phones support: the digits 0 - 9 and their corresponding letters, the asterisk (*), and the octothorpe or pound sign (#).

- Their phone user guide that contains a Cisco Extension Mobility overview and instructions on logging in, logging out, and troubleshooting the feature. The phone user guide also contains information on using Cisco Unified Communications Self Care Portal window.

- Description of the feature login and logout behavior that you defined in the Set the Service Parameters, on page 480.

Note When a user logs in from a phone and the phone displays a “Change PIN” message, the end user must change the end user PIN. When a user logs in from a phone and the phone displays a “Change Password” message, the Cisco Unified Communications Manager administrator must change the CCMSysUser password.

CHAPTER 22

Extension Mobility Cross Cluster

This chapter provides information about Cisco Extension Mobility Cross Cluster feature which allows an enterprise user of one Cisco Unified Communications Manager cluster (the home cluster) to log in to a Cisco Unified IP Phone of another Cisco Unified Communications Manager cluster (the visiting cluster) during travel as if the user is using the IP phone at the home office.

Note If a user remains in a single cluster, configuration of the Cisco Extension Mobility feature suffices to provide the user with extension mobility capabilities. See the Extension Mobility, on page 463 chapter for a description and configuration details of the Cisco Extension Mobility feature.

Configure EMCC

Perform the following steps to configure Cisco Extension Mobility Cross Cluster in your network. Use the following procedure in conjunction with the Extension Mobility Cross Cluster, on page 497.

Procedure

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

Step 2 Choose a server and activate the following CM Services by checking the check box next to each service name:

- Cisco CallManager
- Cisco Tftp
- Cisco Extension Mobility

- Cisco Bulk Provisioning Service (can activate only on the publisher)

Step 3 Click **Save**, click **OK** in response to the popup window, and wait for the services to get activated.

Step 4 Create an Extension Mobility phone service:

a) In Cisco Unified Communications Manager Administration, choose **Device** > **Device Settings** > **Phone Services**.

b) Click **Add New**, and fill in the fields in the IP Phone Services Configuration window as follows:

- Service Name: Extension Mobility
- ASCII Service Name: Extension Mobility
- Service Description: Extension Mobility
- Service URL: `http://10.89.80.19:8080/emapp/EMAppServlet?device=#DEVICENAME#&EMCC=#EMCC#`

Note Change the IP address in both the Service URL and Secure-Service URL fields, unless you do not want the secure-service URL, in which case you can omit the https:// URL that follows.

Secure-Service URL: `https://10.89.80.19:8443/emapp/EMAppServlet?device=#DEVICENAME#&EMCC=#E`

Check the Enable check box.

Note If you click on the Enterprise Subscription check box when configuring the Extension Mobility IP phone service for the first time, you will set up this IP phone service as an enterprise subscription service. If you do this, all phones and device profiles in the enterprise will automatically subscribe to this IP phone service without needing to subscribe individually.

c) Click **Save** to save the Extension Mobility phone service.

Step 5 Add a device profile for users who need Extension Mobility. The device profile gets used to overlay with a real device when the user logs in (both for Extension Mobility and Extension Mobility Cross Cluster). Follow these steps:

a) In Cisco Unified Communications Manager Administration, choose **Device** > **Device Settings** > **Device Profile**.

b) Add a new device profile for a specific device type with a specific protocol, assigning a meaningful name to the new device profile.

Example: 7975 SCCP Device Profile

c) In the new device profile, configure the Extension Mobility Cross Cluster CSS field.

This calling search space (CSS) gets applied to the real device configuration when the user travels and uses an IP phone of a different (visiting) cluster. Configure this field as if setting the Calling Search Space field in the Phone Configuration window of a local IP phone.

d) Add a directory number (DN) to the new device profile.

Example: 4001

e) In the Directory Number Configuration window, choose the Configure Device (<your new device profile name>) option in the Related Links drop-down list box, then click **Go.**
You return to the Device Profile Configuration window.

f) In the Device Profile Configuration window, choose the Subscribe/Unsubscribe Services option in the Related Links drop-down list box, then click **Go.**

g) In the popup window that displays, choose the Extension Mobility service in the Select a Service drop-down list box.
h) Click **Next**, then click **Subscribe.**
i) Click **Save** and close the popup window.
j) In the Device Profile Configuration window, click **Save.**

Step 6 Add users for Cisco Extension Mobility Cross Cluster:

a) In Cisco Unified Communications Manager Administration, choose User Management > End User.
b) Click Add New to add a new end user.
c) In the End User Configuration window that displays, configure at least the following fields:
   - User ID
   - Password
   - PIN
   - Last name
   - First name
d) In the Extension Mobility pane, check the Enable Extension Mobility Cross Cluster check box.
e) Choose the device profile that you configured from the Available Profiles list pane in the Extension Mobility pane.
f) Use the Down arrow to move the device profile to the Controlled Profiles list pane.
g) Click **Save** to save the end user configuration.

Step 7 Enable Extension Mobility on the devices:

a) In Cisco Unified Communications Manager Administration, choose **Device** > **Phone**.
b) Find the phone on which users can perform Extension Mobility or Extension Mobility Cross Cluster.
c) For this device, check the Enable Extension Mobility check box in the Extension Information pane.
d) In the Phone Configuration window, choose the Subscribe/Unsubscribe Services option in the Related Links drop-down list box, then click **Go**.
e) In the popup window that displays, choose the Extension Mobility service in the Select a Service drop-down list box.
f) Click **Next**, then click **Subscribe**.
g) Click **Save** and close the popup window.
h) In the Phone Configuration window, click **Save**. If indicated, click **OK** in the popup window that displays.

Note This step completes the configuration necessary for a user to perform intra-cluster extension mobility login.

Note The Phone Configuration window provides a Secure Services URL. If left blank, the URL Services enterprise parameter gets used.

Step 8 Configure Bulk Certificate Management:

a) In Cisco Unified Communications Operating System Administration, choose **Security** > **Bulk Certificate Management**.
b) In the Bulk Certificate Management window that displays, configure the fields as follows:
   - IP Address: Specify the IP address of the SFTP server.

     Note This is the centralized secure FTP server that all participating clusters must share.

   - Port: 22 (for SSH default port)

- User ID: User ID of user that has write access
- Password: Password of user that has write access
- Directory: Directory of user that has write access (Example: /tmp)

c) Click **Save**.

Step 9 Configure Bulk Certificate Export:

a) In Cisco Unified Communications Operating System Administration, choose **Security** > **Bulk Certificate Management**.
b) Click the **Export** icon.
c) In the Bulk Certificate Export window that displays, configure the following field: Certificate Type: All
d) Click **Export**, then click **Close**.

This step creates a PKCS12 file that contains certificates for all nodes in the cluster.

Every participating cluster must export certificates to the same SFTP server and SFTP directory.

A cluster must export its certificates whenever the Tomcat, TFTP, or Capf certificate(s) gets regenerated on any of its nodes.

Step 10 Consolidate certificates:

a) In Cisco Unified Communications Operating System Administration, choose **Security** > **Bulk Certificate Management** > **Consolidate** > **Bulk Certificate Consolidate**.

   Consolidate certificates when all participating clusters have exported their certificates. This option is available only if two or more clusters have exported their certificates to the SFTP server.
b) In the window that displays, configure the following field: Certificate Type: All
c) Click **Consolidate**.

   This step consolidates all PKCS12 files in the SFTP server to form a single file.

   Only one of the participating clusters needs to perform consolidation.

   If new certificates are exported after they are consolidated, consolidation needs to be performed again to pick up the newly exported certificates.

Step 11 Import certificates:

a) In Cisco Unified Communications Operating System Administration, choose **Security** > **Bulk Certificate Management** > **Import** > **Bulk Certificate Import**.
b) In the window that displays, configure the following field: Certificate Type: All
c) Click **Import**.

Note After you import all the certificates on each cluster, for each cluster, you need to restart Cisco CallManager service and Cisco Tomcat service to activate the services for each node on each cluster.

Note After an upgrade, these certificates are preserved. Users do not need to reimport or reconsolidate certificates.

This step imports the consolidated PKCS12 file from the SFTP server into the local cluster.

All clusters should re-import when any participating cluster makes an export.

Perform import after a central administrator consolidates the certificates.

Step 12 To enable EMCC for video calls, configure Common Phone Profile (**Device** > **Device Settings** > **Common Phone Profile**) or configure Enterprise Phone Configuration (**System** > **Enterprise Phone Configuration**) to enable video calls.

In either window, set the Video Capabilities drop-down list box as Enabled and check the Override Common Settings checkbox. (Although this setting may be enabled by default per cluster, it may be necessary to check the Override Common Settings checkbox and save the change)

Step 13 Add EMCC devices - Add EMCC Templates:

a) In Cisco Unified Communications Manager Administration, choose **Bulk Administration** > **EMCC** > **EMCC Template**.
b) Click **Add New**.
c) In the EMCC Template Configuration window, configure the fields as follows:

- Template Name: EMCC Device Template
- Device Pool: Default
- SIP Profile: Standard SIP Profile
- Common Device Configuration: Default Common Device Configuration

d) Click **Save**.

Step 14 Add EMCC devices - Set default EMCC template.

a) In Cisco Unified Communications Manager Administration, choose **Bulk Administration** > **EMCC** > **Insert/Update EMCC**.
b) Click **Update EMCC Devices**.
c) In the Default EMCC Template drop-down list box, choose the EMCC Device Template that you configured.
d) Click **Run Immediately**.
e) Click **Submit**.
f) Verify whether the job ran successfully:

Choose **Bulk Administration** > **Job Scheduler** and look for the Job ID of your job. Check that your job ran successfully.

Step 15 Add EMCC devices - Insert the EMCC Devices:

a) In Cisco Unified Communications Manager Administration, choose **Bulk Administration** > **EMCC** > **Insert/Update EMCC**.
b) Click **Insert EMCC Devices**.
c) Change the value in the Number of EMCC Devices to be added field (for example, to 5).
d) Click **Run Immediately** and click **Submit**.
e) Refresh this window and check that the Number of EMCC Devices already in database value now displays the number of devices that you added (for example, 5).
f) Alternately, choose **Bulk Administration** > **Job Scheduler** to check on whether the job completed successfully.

Maximum Number of EMCC Base Devices To Add

Include EMCC in the total number of devices that get supported in the cluster, using the following calculation:

phones + (2 x EMCC devices) <= MaxPhones

Cisco Unified Communications Manager systems specify a MaxPhones value of 60,000.

EMCC login does not affect the number of licenses that get used in the home cluster.

Step 16 Configure enterprise parameters and add a geolocation filter:

a) In Cisco Unified Communications Manager Administration, choose **System** > **Enterprise Parameters**.
b) For the Cluster ID enterprise parameter, configure a unique cluster ID for every participating cluster.
c) In Cisco Unified Communications Manager Administration, choose **System** > **Geolocation Filter**.
d) Click **Add New**.
e) Create a new geolocation filter.

Example name: EMCC Geolocation Filter.

Specify criteria for matching, such as Country, State, and City.

Step 17 Configure EMCC feature parameters:

a) In Cisco Unified Communications Manager Administration, choose **Advanced Features** > **EMCC** > **EMCC Feature Configuration**.
b) In the EMCC Feature Configuration window that displays, configure the following feature parameters:

- Default TFTP Server for EMCC Login Device
- EMCC Geolocation Filter
- Default Server for Remote Cluster Update

Note Each feature parameter must be previously configured before you can choose them in the drop-down list box that associates with each feature parameter.

Note You can keep the default values for other EMCC feature parameters or you can change as needed.

Step 18 Configure one or two intercluster SIP trunks for EMCC.

Note You may configure one trunk for both PSTN Access and RSVP Agent services or one trunk for each service. You need no more than two EMCC SIP trunks.

a) In Cisco Unified Communications Manager Administration, choose **Device** > **Trunk**.
b) Click **Add New**.
c) Specify the following settings:

- Trunk Type: SIP Trunk
- Trunk Service Type: Extension Mobility Cross Clusters

d) Click **Next**.
e) In the Trunk Configuration window that displays, specify the following settings in the Device Information pane. The following values show example values.

- Name: EMCC-ICT-SIP-Trunk-1
- Device Pool: Default

In the SIP Information pane, specify the following example settings:

- SIP Trunk Security Profile: Non Secure SIP Trunk Profile
- SIP Profile: Standard SIP Profile

In the Geolocation Configuration pane, specify the following setting:

- Send Geolocation Information: Check this check box.

Note EMCC trunk must specify SendGeolocation as True, MTPRequired as False, and UnattendedPort as False.

f) Click **Save** to save the intercluster SIP trunk for EMCC.

Step 19 Configure EMCC intercluster service profile:

a) In Cisco Unified Communications Manager Administration, choose **Advance Features** > **EMCC** > **EMCC Intercluster Service Profile**.
b) Check the Active check box in the EMCC pane.
c) Check the Active check box in the PSTN Access pane.
d) In the PSTN Access SIP Trunk drop-down list box, choose a SIP trunk that you configured.
e) Check the Active check box in the RSVP Agent pane.
f) In the RSVP Agent SIP Trunk drop-down list box, choose another SIP trunk that you configured.

Note If you configured only one trunk, you can choose the same trunk for RSVP Agent SIP Trunk as for PSTN Access SIP Trunk.

g) Click **Validate** to validate your settings.
h) If no failure messages display in the popup window, click **Save**.

Step 20 Configure EMCC remote cluster services:

a) In Cisco Unified Communications Manager Administration, choose **Advance Features** > **Cluster View**.
b) Click **Find** to display a list of known remote clusters.
c) If the remote cluster that you want configure appears, click on the remote cluster and verify the settings.
d) If the remote cluster that you want to configure does not appear, click **Add New** and configure the following settings:

- Cluster ID: Ensure that this cluster ID matches the enterprise parameter value of the cluster ID of the other cluster(s).
- Fully Qualified Name: Use the IP address of the remote cluster or a domain name that can resolve to any node on the remote cluster.

Note During EMCC, TFTP check box should always be disabled.

Step 21 Configure service parameters:

a) In Cisco Unified Communications Manager Administration, choose **System** > **Service Parameters**.
b) From the Server drop-down list box, choose a server.
c) From the Service drop-down list box, choose the Cisco Extension Mobility service.
d) Click the **Advanced** button at the top of the window.
e) As needed, configure the following service parameters in the Clusterwide Parameters (Parameters that apply to all servers) pane:

- Inter-cluster Maximum Login Time
- EMCC Allow Proxy: Set this value as True.

Note For EMCC, the call logs always get cleared.

Note For EMCC, multiple logins are always allowed.

EMCC does not require any special configuration for SRST to function.

If SRST configuration is required for your system, configure as usual.

Related Topics

Extension Mobility Cross Cluster, on page 497
EMCC Call Routing, on page 515
Configure EMCC Feature Configuration, on page 528
EMCC Intercluster Service Profile Configuration Settings, on page 533
Remote Cluster Configuration, on page 535
Set the Service Parameters, on page 480
Cisco Extension Mobility Service Parameters, on page 486

EMCC Feature

This section contains information about the EMCC feature and configuration, supported phones, login instructions and summaries, call processing, and phone security.

EMCC vs. Cisco Extension Mobility

Release 3.1 of Cisco CallManager first offered the Cisco Extension Mobility feature. Cisco Extension Mobility continues to apply only to intra-cluster users and devices. Customers, however, want a seamless experience, no matter where they log in:

- User wants the same set of features and services: all lines, speed dials, message button, MWI, and features.
- Administrator wants security, CAC, local gateway access, local media resources, and serviceability.

EMCC Challenges

With intra-cluster Cisco Extension Mobility, the following characteristics apply:

- Device information is available in the local database.
- User information is available in the local database.
- Global information is available in the local database.

With inter-cluster Cisco Extension Mobility, the following characteristics apply:

- Device information is in one cluster database.
- User information is in another cluster database.
- Global information, such as routing configuration and service parameters, is in the database of both clusters.

Cisco Extension Mobility presents the following challenge: either device information needs to be moved to the cluster that manages user information or vice-versa.

EMCC Solution

The solution to address the problem of extension mobility across clusters specifies cross-registration. Cross-registration implies the following characteristics:

- User from home cluster logs in to a phone at visiting cluster.
- Login procedure conveys the device information into the home cluster database.
- Home cluster database builds a temporary device with user device profile.
- Home cluster TFTP server builds the phone configuration file.
- After login, visiting cluster directs the phone to home cluster TFTP server.
- Phone downloads its TFTP configuration from home cluster (HC) TFTP server and then cross-registers with home cluster Cisco Unified Communications Manager.

Note Clusters are designated as home or visiting relative to the login user.

Cisco Extension Mobility Cross Cluster Interactions

See the EMCC Interactions, on page 524 for a list of the interactions between the Cisco Extension Mobility Cross Cluster feature and other features.

Scope of EMCC

Cisco Extension Mobility Cross Cluster supports the following features:

- Cisco Extension Mobility login and logout
    - User authentication takes place across clusters.
- Security
    - Cross-cluster security gets provided by default.
    - Cisco Unified IP Phones with secure and nonsecure phone security profiles are supported.
- PSTN access is suitable for the visiting phone.
    - Routing E911 to the right part of the PSTN (that is, to local gateways) takes place.
    - Routing local calls to the right part of the PSTN takes place.
    - Calls terminating to local route groups route to local gateways in the visiting cluster.
- Media resources suitable for the visiting phone get presented, such as the following:
    - RSVP Agent, TRP, Music On Hold (MOH), MTP, transcoder, conference bridge
- Call Admission Control (CAC)
    - Home cluster remains ignorant 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 using RSVP agents in the visiting cluster

- Call features and services that home cluster can reasonably support
  - Example restriction: Intercom configuration specifies configuration to a static device, so Cisco Extension Mobility Cross Cluster does not support the Intercom feature.
- Default max audio bit-rate for EMCC login device is set to 8 kbps (G.729).

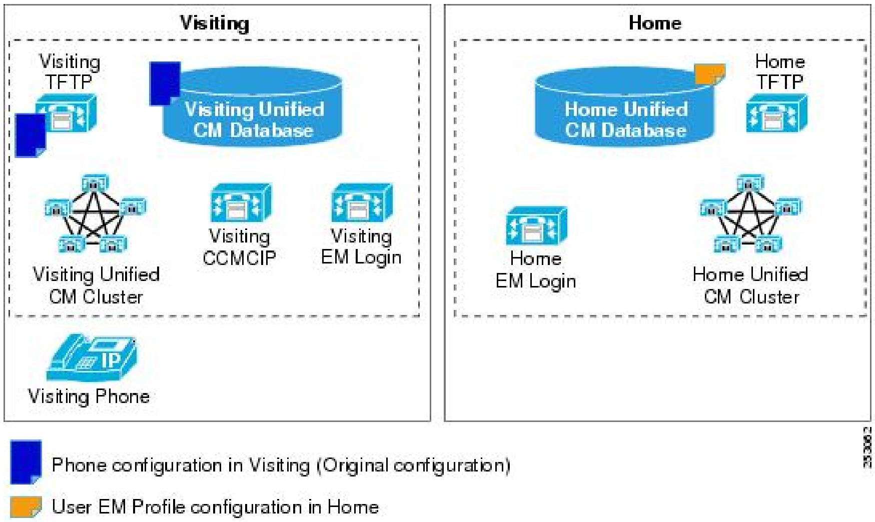
EMCC Login

This section provides information about EMCC login.

EMCC Login Terminology

The following figure illustrates the visiting cluster versus a home cluster in Cisco Extension Mobility Cross Cluster.

Figure 35: Visiting Cluster vs. Home Cluster


Visiting
Visiting TFTP
Visiting Unified CM Database
Visiting Unified CM Cluster
Visiting CCMCIP
Visiting EM Login
IP
Visiting Phone
Home
Home TFTP
Home Unified CM Database
Home EM Login
Home Unified CM Cluster
253062
Phone configuration in Visiting (Original configuration)
User EM Profile configuration in Home

Visiting Cluster

For the visiting cluster, the following characteristics apply:

- Phone is geographically present here.
- Phone configuration resides here in the visiting Cisco Unified Communications Manager database.
- The resources that the phone needs reside here, such as gateways and RSVP agents.
- The visiting phone normally registers with the visiting Cisco Unified Communications Manager cluster that manages this geographic location (prior to EMCC login).
- CCMCIP specifies the Cisco CallManager Cisco IP Phone service.

Home Cluster

For the home cluster, the following characteristics apply:

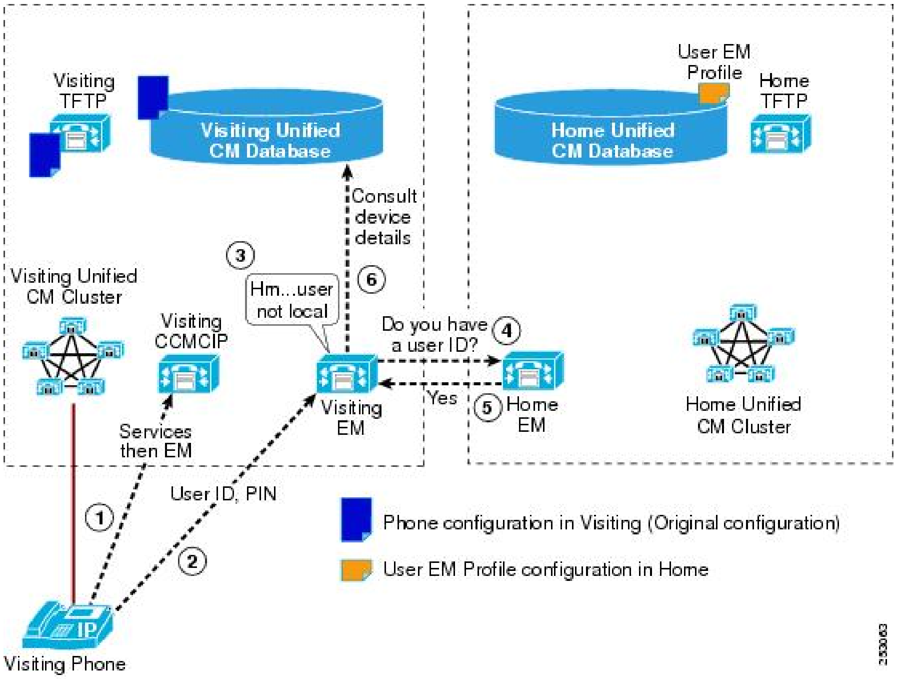
- End user configuration resides here.
- User device profile (lines, speed dials, features, and many more user characteristics) reside here.
- User dialing habits make sense in the home context.
- User locale resides here.

Cross-registration specifies the process of importing the device data into the home cluster and building a device record that is combined with the end user Extension Mobility (EM) profile in the home cluster, then directing the phone to register directly with the home cluster Cisco Unified Communications Manager.

EMCC Login Progress

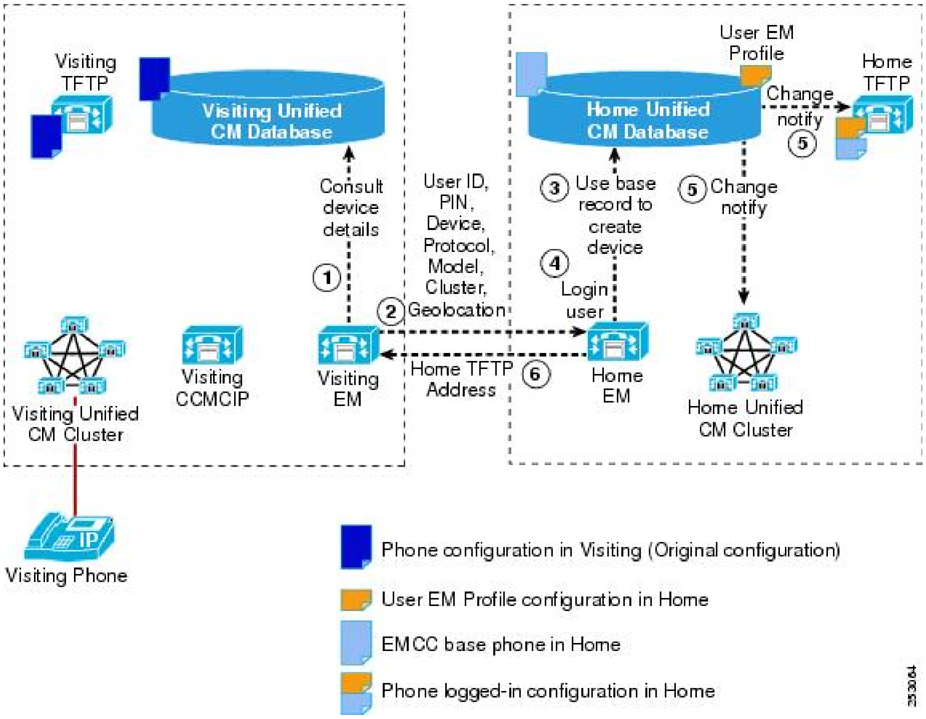
The following figure illustrates Cisco Extension Mobility Cross Cluster login when extension mobility finds the home cluster.

Figure 36: EMCC Login - Extension Mobility Finds Home Cluster



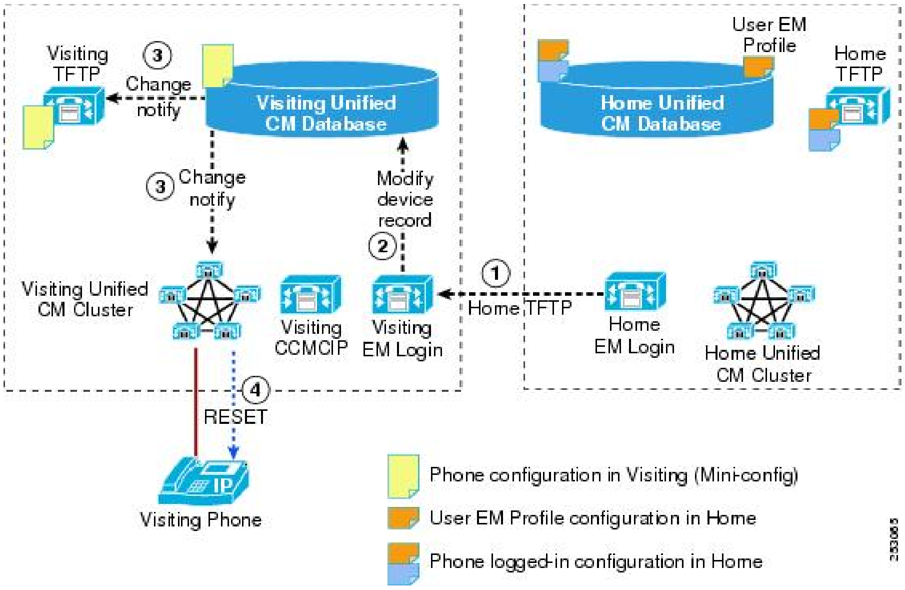
The following figure illustrates Cisco Extension Mobility Cross Cluster login when extension mobility authenticates, gives information to home cluster, and prepares home cluster.

Figure 37: EMCC Login - Extension Mobility Authenticates, Gives Information to Home, Prepares Home


Visiting TFTP
Visiting Unified CM Database
User EM Profile
Home TFTP
Home Unified CM Database
Change notify
5
Consult device details
1
User ID, PIN, Device, Protocol, Model, Cluster,
2 Geolocation
3 Use base record to create device
4 Login user
5 Change notify
Visiting Unified CM Cluster
Visiting CCMCIP
Visiting EM
Home TFTP Address
6
Home EM
Home Unified CM Cluster
Visiting Phone
Phone configuration in Visiting (Original configuration)
User EM Profile configuration in Home
EMCC base phone in Home
Phone logged-in configuration in Home
253064

The following figure illustrates Cisco Extension Mobility Cross Cluster login when extension mobility modifies the visiting cluster and initiates reregistration.

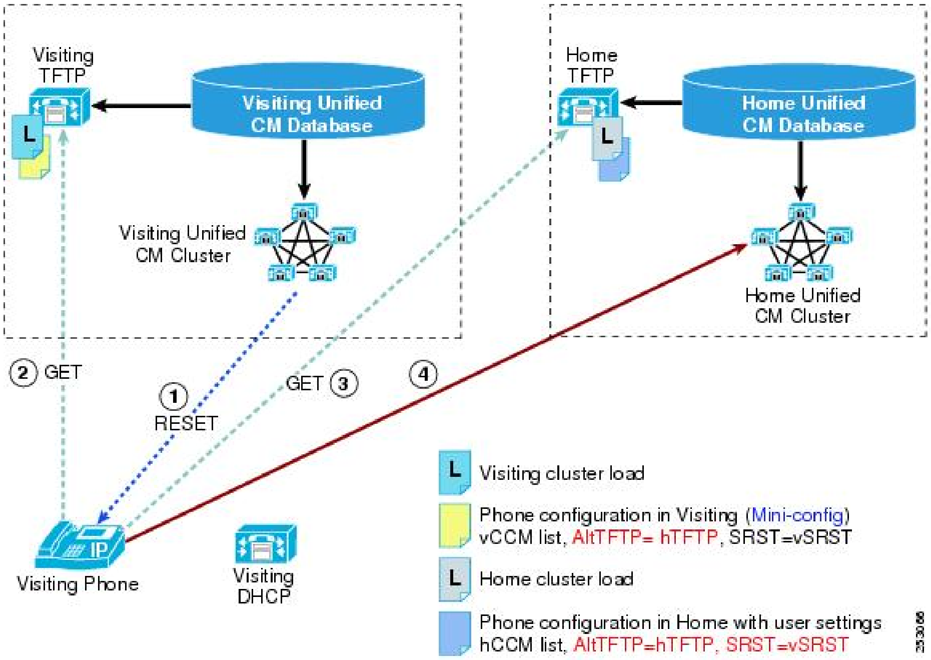
Figure 38: EMCC Login - Extension Mobility Modifies Visiting and Initiates Reregistration



Mini-config specifies a small configuration file built by the visiting cluster to redirect the phone to the home cluster after login.

The following figure illustrates Cisco Extension Mobility Cross Cluster login when extension mobility login services complete processing and the phone reregisters.

Figure 39: EMCC Login - Extension Mobility Login Services Complete Processing and the Phone Reregisters


Visiting TFTP
Visiting Unified CM Database
Visiting Unified CM Cluster
Home TFTP
Home Unified CM Database
Home Unified CM Cluster
2 GET
1 RESET
GET 3
4
Visiting Phone
Visiting DHCP
L Visiting cluster load
Phone configuration in Visiting (Mini-config) vCCM list, AltTFTP= hTFTP, SRST=vSRST
L Home cluster load
Phone configuration in Home with user settings hCCM list, AltTFTP=hTFTP, SRST=vSRST
253086

Determine EMCC Supported Phones

The list of devices that support the Cisco Extension Mobility Cross Cluster varies per version and device pack.

Use the Cisco Unified Reporting application to generate a complete list of devices that support Cisco Extension Mobility Cross Cluster for a particular release and device pack. To do so, follow these steps:

1. Start Cisco Unified Reporting by using any of the methods that follow.

   The system uses the Cisco Tomcat service to authenticate users before allowing access to the web application. You can access the application

   - by choosing Cisco Unified Reporting in the Navigation menu in Cisco Unified Communications Manager Administration and clicking **Go**.
   - by choosing **File** > **Cisco Unified Reporting** at the Cisco Unified Real Time Monitoring Tool (RTMT) menu.
   - by entering `https://<server name or IP address>:8443/cucreports/` and then entering your authorized username and password.

2. Click **System Reports** in the navigation bar.
3. In the list of reports that displays in the left column, click the **Unified CM Phone Feature List** option.
4. Click the Generate a new report link to generate a new report, or click the Unified CM Phone Feature List link if a report already exists.

5. To generate a report of all devices that support Cisco Extension Mobility Cross Cluster, choose these settings from the respective drop-down list boxes and click the **Submit** button:

   Product: All

   Feature: Extension Mobility Cross Cluster

   The List Features pane displays a list of all devices that support the Cisco Extension Mobility Cross Cluster feature. You can click on the Up and Down arrows next to the column headers (Product or Protocol) to sort the list.

For additional information about the Cisco Unified Reporting application, see the *Cisco Unified Reporting Administration Guide*.

EMCC Configuration

See topics related to configuring EMCC for an overview of the configuration steps to configure Cisco Extension Mobility Cross Cluster, both in Cisco Unified Communications Manager Administration and in the other Cisco Unified Communications components, such as Cisco Unified Serviceability and the Cisco Unified Communications Operating System.

Related Topics

Configure EMCC, on page 528

View EMCC Active and Remote Login Summary

In the user home cluster, the administrator can view a list of the cluster users who have logged in from remote devices.

To do so, the administrator performs the following steps:

Procedure

Step 1 In Cisco Unified Communications Manager Administration, execute **Device** > **Phone**.
The Find and List Phones window displays.

Step 2 From the Related Links drop-down list box, choose **Remotely Logged In Device**, then click **Go**.

For additional information about the remotely logged-in devices report, see the Cisco Unified Communications Manager Administration Guide.

Step 3 In any cluster, the administrator can view a list of the cluster devices that have been logged in to either Cisco Extension Mobility or Cisco Extension Mobility Cross Cluster To do so, the administrator performs the following steps:.

a) In Cisco Unified Communications Manager Administration, execute **Device** > **Phone**.
The Find and List Phones window displays.

b) From the Related Links drop-down list box, choose **Actively Logged In Device Report**, then click **Go**.

For additional information about the actively logged-in devices report, see the Cisco Unified Communications Manager Administration Guide.

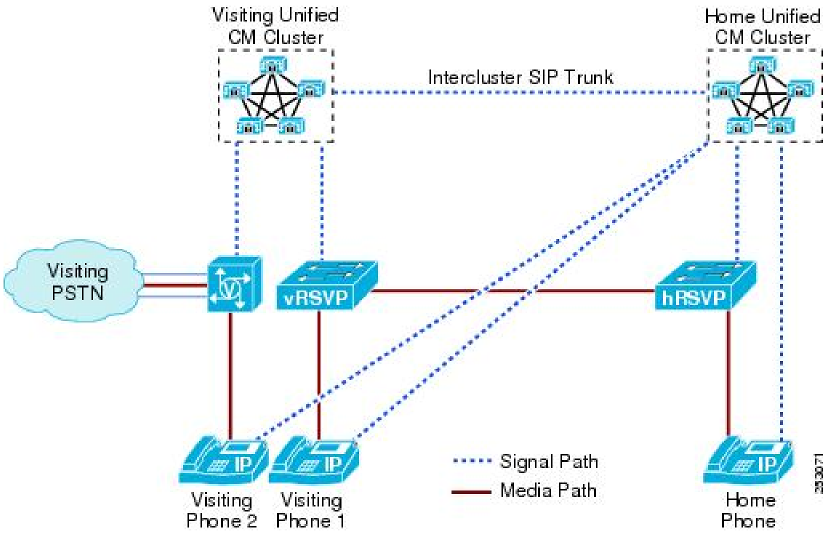
EMCC Call Processing

This section contains information about EMCC call processing and includes how to obtain help for call processing issues.

EMCC Call Processing Overview

The following figure provides an overview of EMCC call processing.

Figure 40: EMCC Call Processing



EMCC Call Processing Characteristics

EMCC call processing exhibits the following characteristics:

- Call control on the home cluster
  - Visiting phone registers with home cluster.
- RSVP Agent gets allocated from visiting cluster but is indirectly controlled by home cluster.
  - Visiting phone registers with home cluster.
  - Follows home cluster policy for RSVP-based CAC.
- Codec selection by both home cluster and visiting cluster
  - Media processes on both home cluster and visiting cluster.
  - Codec selected based on EMCC region configuration of both clusters
- Emergency call routing is visiting phone/visiting cluster dependent.
  - Home cluster supports both home cluster and visiting cluster emergency pattern.
  - Route emergency calls back to visiting cluster with local route group via EMCC SIP intercluster trunk.

- Uses local route group of visiting phone that is configured in visiting cluster.

- Device-dependent PSTN access in visiting cluster
    - Route call from SIP trunk to local gateway colocated with visiting phone

EMCC Call Processing Requirements

Cisco Extension Mobility Cross Cluster fulfills the following call-processing requirements:

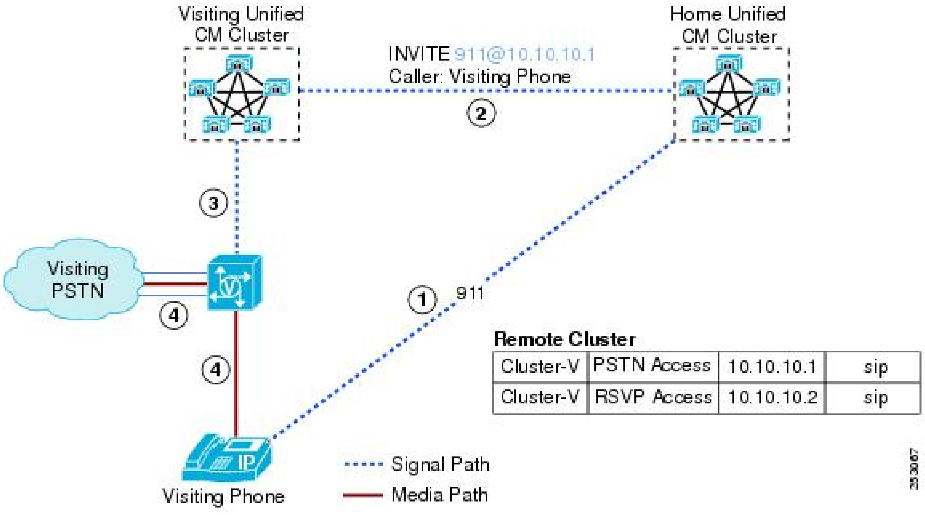
- Emergency call routing
    - Allows user to dial either home cluster emergency pattern or visiting cluster emergency pattern (for example, 999 in the United Kingdom or 911 in the United States).
    - Call must route to the local gateway in the visiting cluster no matter which cluster emergency pattern gets dialed.
- RSVP agent based CAC
    - RSVP Agents in the visiting cluster must get allocated based on the visiting phone media resource group list (MRGL) in the visiting cluster.

Note Whereas the phone registers with the home cluster, moving the phone location in the visiting cluster may cause incorrect association to the local gateway or media resource group list (MRGL) in the visiting cluster.

EMCC Call Processing for Emergency Calls

The following figure illustrates Cisco Extension Mobility Cross Cluster call processing for emergency calls.

Figure 41: EMCC Call Processing for an Emergency Call



Remote Cluster

Cluster-V	PSTN Access	10.10.10.1	sip
Cluster-V	RSVP Access	10.10.10.2	sip

Find the Roaming Device Pool

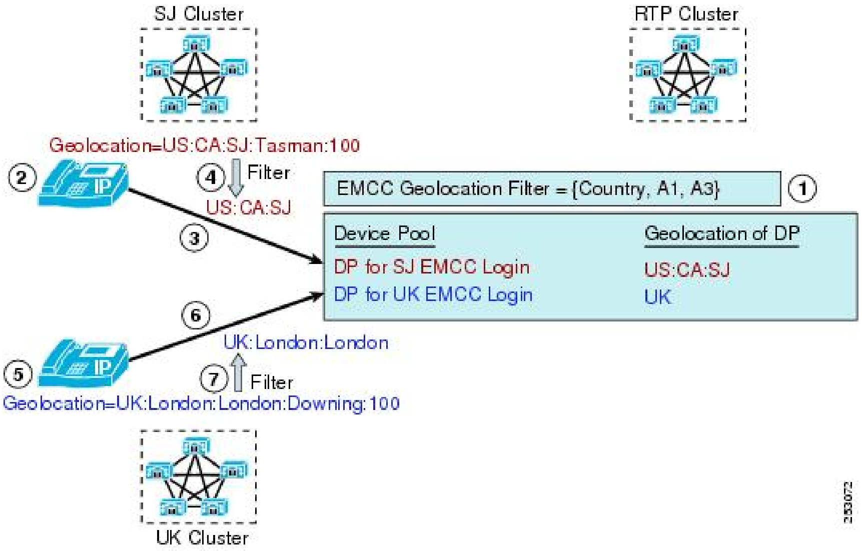
Finding the roaming device pool exhibits the following characteristics:

- EMCC phone finds roaming-sensitive attributes from its roaming device pool in home cluster.
- Home cluster configures one roaming device pool per remote cluster, with distinct geolocation characterizing that cluster, for example:
    - DPforUKCluster (country=UK)
    - DPforSJCluster (country=US, A1=CA, A3=SJ)
- Phone that is enabled for extension mobility in visiting cluster configures its geolocation in visiting cluster.
- Login process sends phone geolocation from visiting cluster to home cluster.
- EMCC geolocation filter that is configured in home cluster filters phone geolocation.
- Home cluster uses filtered phone geolocation to find the most suitable device pool as phone roaming device pool while phone registers in home cluster.

Match the Roaming Device Pool

The following figure illustrates matching the roaming device pool by using the geolocation in the home cluster.

Figure 42: Match Roaming Device Pool Using Geolocation in Home Cluster



EMCC Call Processing Configuration

Visiting cluster configures geolocation for phones that are enabled for extension mobility. This configuration takes place in the Geolocation field of the Phone Configuration window (**Device** > **Phone**) or in the Geolocation field of the Geolocation Configuration pane of the Device Pool Configuration window (**System** > **Device Pool**).

Configuration of the following entities is also required for extension mobility enabled phones in the visiting cluster:

- Local route group in the associated Device Pool Configuration window (**System** > **Device Pool**)
- RSVP device (transcoder or MTP) in the phone media resource group list if RSVP policy is enabled.

Home cluster configures EMCC geolocation filter. Use the **Advanced Features** > **EMCC** > **EMCC Feature Configuration** menu option to configure the EMCC Geolocation Filter setting.

One device pool per remote cluster serves as the roaming device pool for login phones.

Example

Device pool specifies EMCC Device Pool for UK Cluster.

Geolocation for this device pool specifies UK Geolocation.

The UK Geolocation geolocation in this device pool allows UK phones to match and choose this device pool as the roaming device pool when the phones log in.

List EMCC Phones

The home cluster administrator can list all remote devices that are currently registered to this cluster. To do so, execute **Device** > **Phone**. From the Related Links drop-down list box, choose **Remotely Logged In Device**; then, click **Go**.

The Remotely Logged-In Device Report displays the following information:

- Device Name
- Logged In Profile
- User ID
- Remote Cluster ID
- Roaming Device Pool
- Device Security Mode

EMCC Call Processing

Logged-in EMCC phones in home cluster acquire the following attributes and preferences:

- Shared attributes from EMCC base device (Bulk Administration)
- Roaming-sensitive attributes from its roaming device pool
  - One roaming device pool per remote cluster
  - EMCC phones of same visiting cluster choose the same roaming DP
  - Allows country-specific emergency dialing plan (for example, 999 for UK)
- User preferences from User Device Profile (lines and speed dials)
- Feature-specific attributes from EMCC Feature Configuration
  - Codec preference for all EMCC phone of all clusters
  - RSVP policy for EMCC phones

EMCC Call Routing

Call routing gets based on calling search space (CSS) home cluster builds for the phone.

Home cluster concatenates the CSS in the following priority order:

1. Adjunct CSS (new)
    - Configured in roaming device pool to support country-specific emergency dialing plan (for example, UK phone remotely registers back to US cluster; user dials 9.999 (UK emergency number) that US cluster will normally not recognize. Home cluster=US, visiting cluster=UK.
    - May skip Adjunct CSS configuration if home cluster and visiting cluster share the same emergency pattern.
2. Line CSS
3. Device CSS
    - Device-specific; gets configured in Phone Configuration window or its static device pool.
    - Allows phone to perform normal dialing in home cluster.
    - Visiting phone does not have phone device configured in home cluster.
    - Home cluster takes EMCC CSS (new) from user login device profile and uses this CSS as its static device CSS.

Adjunct Calling Search Space Functionality

To configure the adjunct CSS, execute **System** > **Device Pool** and configure the Adjunct CSS field in the Device Pool Settings pane.

In this example, the following configuration applies:

- Adjunct CSS specifies Adjunct CSS for UK Cluster.
- Selected Partitions (in Route Partitions for this Calling Search Space) specifies EMCC Emergency Partition for UK.

The adjunct CSS, which you configure in the device pool, enables UK emergency dialing from UK phone that registers to US cluster after login and binding to the roaming device pool. US cluster specifies the home cluster.

Calling search space specifies only one member partition, EMCC Emergency Partition for UK.

Configure Visiting Cluster Emergency Pattern

Configure a visiting cluster emergency pattern in the home cluster.

Example

Configure the route for 9.999/{EMCC emergency partition for UK}. This route contain only one member, Standard LRG.

If visiting phone (in UK) that registers to home cluster (in US) dials 9.999, this pattern matches route pattern 9.999/{EMCC emergency partition for UK} because of the adjunct CSS in the phone roaming device pool. As a result, home cluster (US cluster) routes the call to the device local route group.

Local Route Group of EMCC

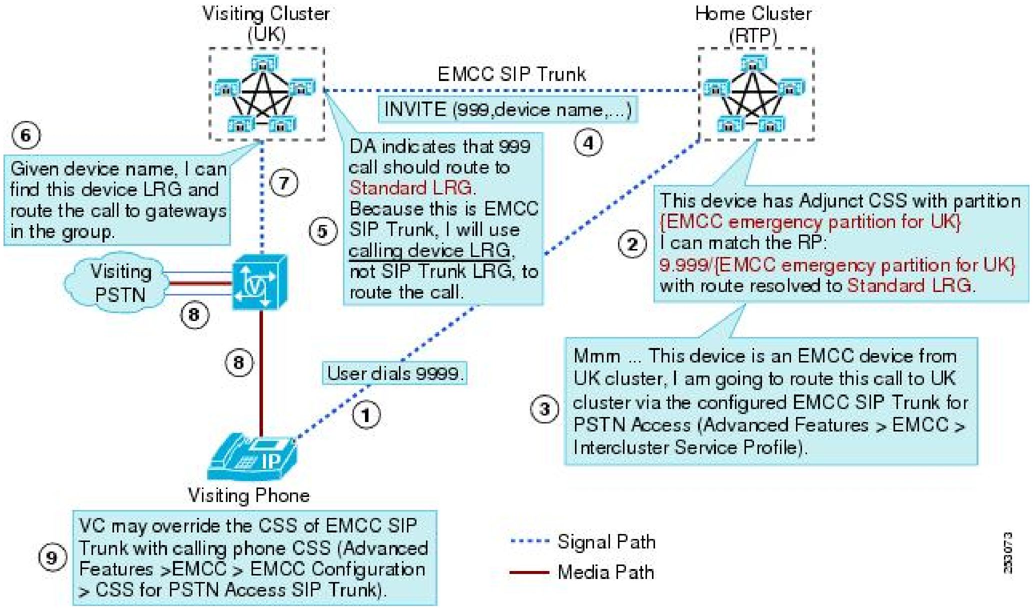
The local route group of EMCC visiting phone in the home cluster specifies the following:

- Local route group of a device comprises gateways to the device local PSTN.
- Calls that terminate to Standard LRG get directed to calling device LRG (that is, to gateways that connect to the local PSTN).
- A normal phone and its local route group register to the same cluster.
- EMCC visiting phone and its local route group register to different clusters.
  - Home cluster has no configured local route group of visiting phone.
  - Home cluster has no direct access to local PSTN gateways of visiting phone.
  - Calls that terminate to Standard LRG of EMCC visiting phone in home cluster get directed to visiting cluster via PSTN access SIP trunk (EMCC Configuration).
  - Visiting cluster finds local route group that is configured for visiting phone. (Remember that any phone that is enabled for extension mobility must configure its local route group in the visiting cluster.)
  - Visiting cluster routes the call to gateways in that local route group like a normal phone.

Local Route Group Using EMCC SIP Trunk

The following figure illustrates local route group routing that uses an EMCC SIP trunk.

Figure 43: Local Route Group Routing Using EMCC SIP Trunk


Visiting Cluster (UK)
Home Cluster (RTP)
EMCC SIP Trunk
INVITE (999,device name,...)
6
Given device name, I can find this device LRG and route the call to gateways in the group.
7
4
DA indicates that 999 call should route to Standard LRG. Because this is EMCC SIP Trunk, I will use calling device LRG, not SIP Trunk LRG, to route the call.
5
2
This device has Adjunct CSS with partition {EMCC emergency partition for UK} I can match the RP: 9.999/{EMCC emergency partition for UK} with route resolved to Standard LRG.
Visiting PSTN
8
8
User dials 9999.
1
3
Mmm ... This device is an EMCC device from UK cluster, I am going to route this call to UK cluster via the configured EMCC SIP Trunk for PSTN Access (Advanced Features > EMCC > Intercluster Service Profile).
IP
Visiting Phone
9
VC may override the CSS of EMCC SIP Trunk with calling phone CSS (Advanced Features >EMCC > EMCC Configuration > CSS for PSTN Access SIP Trunk).
Signal Path
Media Path
253073

EMCC Calling Search Space in Device Profile

The Extension Mobility Cross Cluster CSS field, which you define in the Device Profile Configuration window (**Device** > **Device Settings** > **Device Profile**), gets used as the device CSS of the remote phone when the user selects this device profile during EMCC login.

Region Configuration for EMCC Phones

Region configuration for EMCC phones specifies the following:

- EMCC login phones do not have region configured in home cluster.
- All EMCC login phones, from any cluster, are assigned with common region configuration (**Advanced Features** > **EMCC** > **EMCC Feature Configuration**) that overrides normal region configuration.
- EMCC feature parameters for regions must get configured with identical values in all clusters. If EMCC feature parameters for regions are set with different values, the Remote Cluster Update operation disables RSVP Agent for the cluster in question.
- The following EMCC feature parameters for regions apply:
  - EMCC Region Max Audio Bit Rate (See the EMCC Solution, on page 504 for a details of a suggested workaround configuration that involves this feature parameter.)
  - EMCC Region Max Video Call Bit Rate (includes Audio)
  - EMCC Region Link Loss Type

RSVP Configuration for EMCC Phones

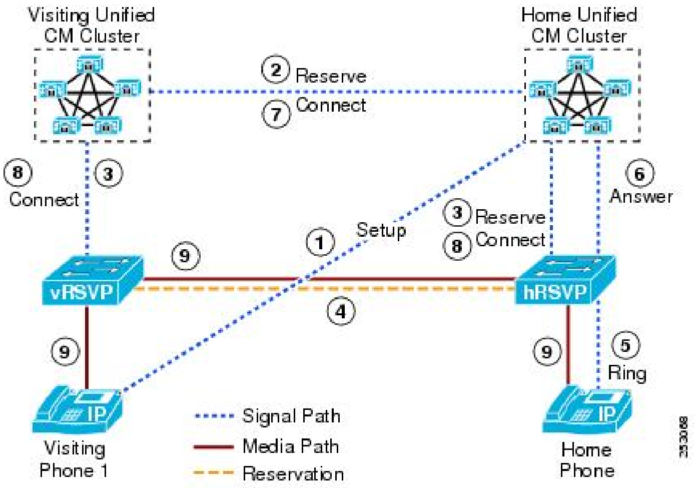
RSVP configuration for EMCC phones presents the following characteristics:

- In home cluster, RSVP policy for EMCC phones follow the same configuration steps as normal phones:
  - Configure a common location (for example, Remote-cluster-location) or cluster-specific location (for example, UK-location).
  - Set Unlimited audio and video bandwidth for the location(s) such that location-based CAC gets disabled.
  - Set RSVP policy for location pairs (no reservation, optional, mandatory).
- In visiting cluster, add RSVP devices to the media resource group list (MRGL) of the visiting phone.
- When allocating RSVP agent, home cluster Cisco Unified Communications Manager recognizes the RSVP agent is for EMCC phone and redirects the request to visiting cluster over RSVP SIP trunk.
- When allocating all other media resources, home cluster Cisco Unified Communications Manager allocate media resources based on the media resource group list that is configured in the home cluster.

RSVP Agent-Based CAC

The following figure illustrates Cisco Extension Mobility Cross Cluster for an RSVP Agent-based Call Admission Control (CAC) basic call.

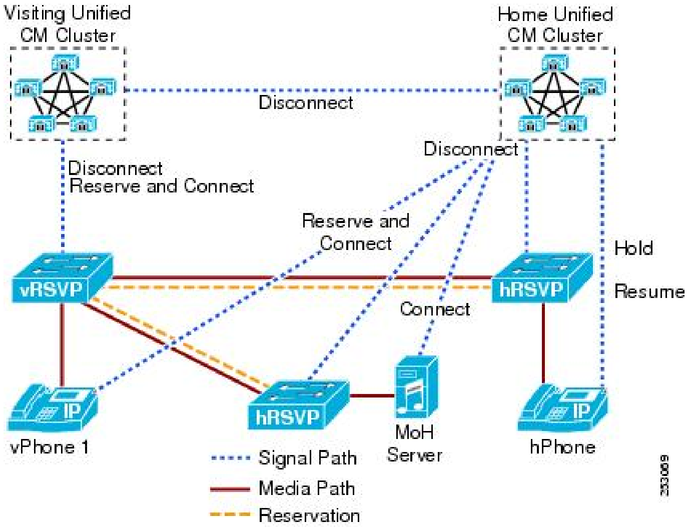
Figure 44: EMCC for RSVP Agent-Based CAC Basic Call



RSVP Agent CAC Hold/Resume by Home Phone

The following figure illustrates Cisco Extension Mobility Cross Cluster for an RSVP Agent-based Hold/Resume call by the home phone.

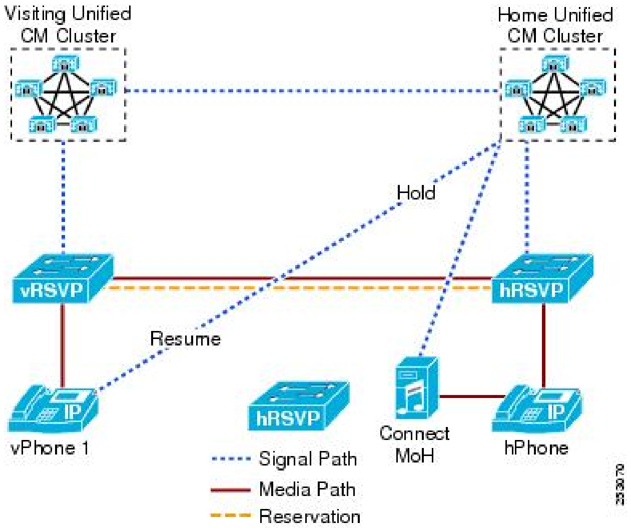
Figure 45: EMCC for an RSVP Agent-Based CAC Hold/Resume Call by the Home Phone



RSVP Agent CAC Hold/resume by Visiting Phone

The following figure illustrates Cisco Extension Mobility Cross Cluster for an RSVP Agent-based Hold/Resume call by the visiting phone.

Figure 46: EMCC for an RSVP Agent-Based CAC Hold/Resume Call by the Visiting Phone



EMCC Call Processing Issues

This section discusses the following common call processing issues that EMCC can present:

- Cannot make normal call.
  - EMCC phone does not bind to the correct roaming device pool (**Device** > **Phone**, then choose **Remotely Logged In Device**).
  - Login device profile does not set EMCC CSS (**Device** > **Device Setting** > **Device Profile**).
  - RSVP reservation fails if configured (for example, no RSVP device in visiting phone media resource group list in visiting cluster).
  - EMCC login phone does not support G.729 codec and no transcoder is configured for the phone in the visiting cluster.
- Cannot make emergency call.
  - EMCC phone does not bind to the correct roaming device pool (**Device** > **Phone**, then choose **Remotely Logged In Device**).
  - Adjunct CSS in roaming device pool of EMCC phone is missing.
  - Verify routing configuration in home cluster based on Adjunct CSS.
  - Local route group configuration is missing in phone static device pool in visiting cluster.
- No media or one-way media is present.
  - Check whether all clusters have the same value in EMCC Region configuration window (**Advanced Features** > **EMCC** > **EMCC Feature Configuration**).
  - Check RSVP policy in home cluster (only RSVP policy in home cluster matters).

Help for EMCC Call Processing Issues

Take the following steps to obtain help for call processing issues:

Procedure

Step 1 Collect detailed traces from both home cluster and visiting cluster.

Step 2 Provide detailed description of the call scenario:

a) Identify the EMCC device and the non-EMCC device and its cluster. For example, the EMCC phone does not bind to the correct roaming device pool. Use the **Device** > **Phone** menu option, then choose **Remotely Logged In Device** from the Related Links drop-down list box.

Phone Behavior with EMCC

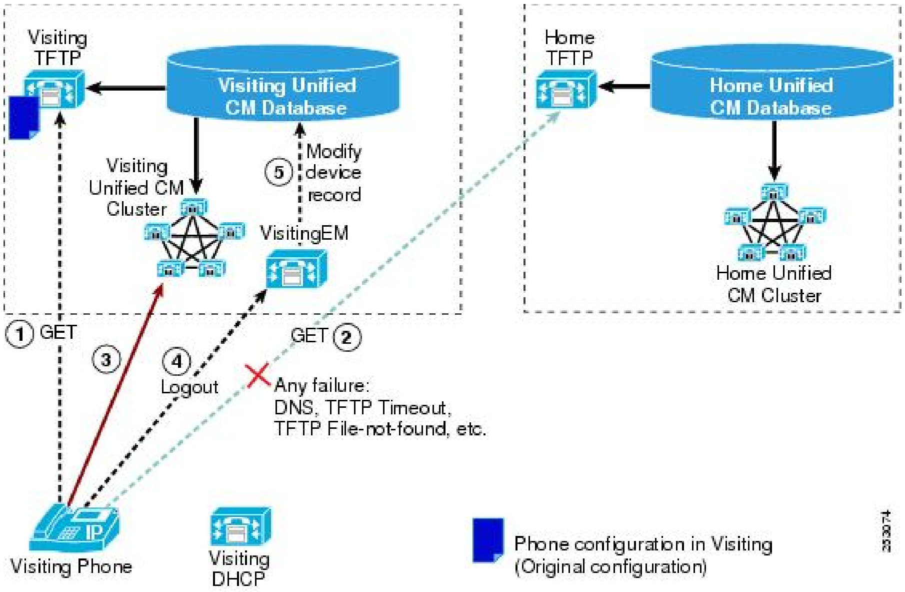
This section provides information about phone behaviors in an EMCC environment, such as during a WAN network failure.

WAN Network Failure

The following figure illustrates WAN network failure when the configuration file is unavailable.

The phone reregisters with the visiting cluster.

Figure 47: WAN Network Failure—Configuration File Unavailable



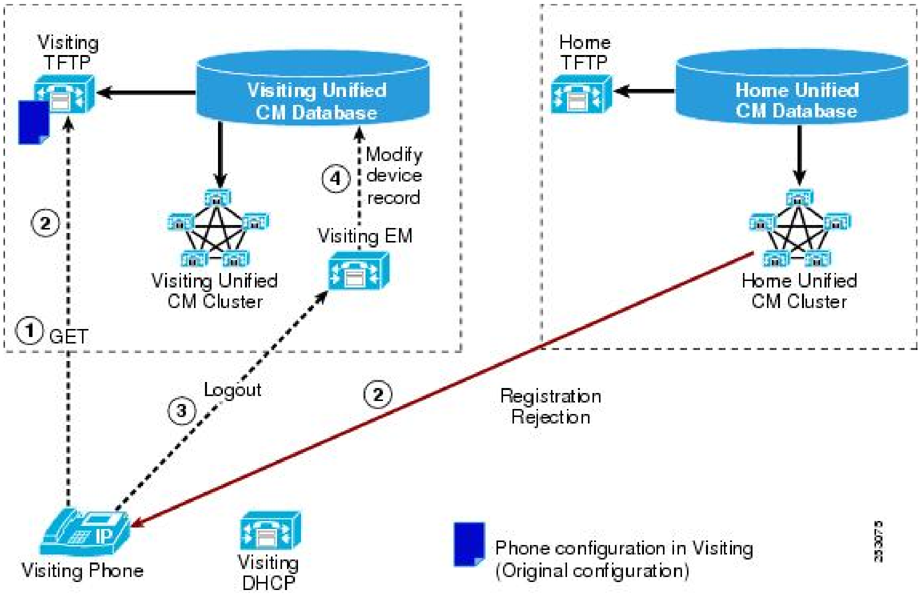
In EMCC login mode, if the phone detects a connection failure to the home cluster, the phone tries to reestablish connection to the home cluster. After several failed attempts, such as failures due to WAN failure, the phone issues a logout request to the visiting cluster automatically, then the phone reregisters with the visiting cluster as logged out.

EMCC Failure - Registration Rejection

The following figure illustrates EMCC failure when registration rejection occurs.

The phone reregisters with the visiting cluster.

Figure 48: EMCC Failure - Registration Rejection

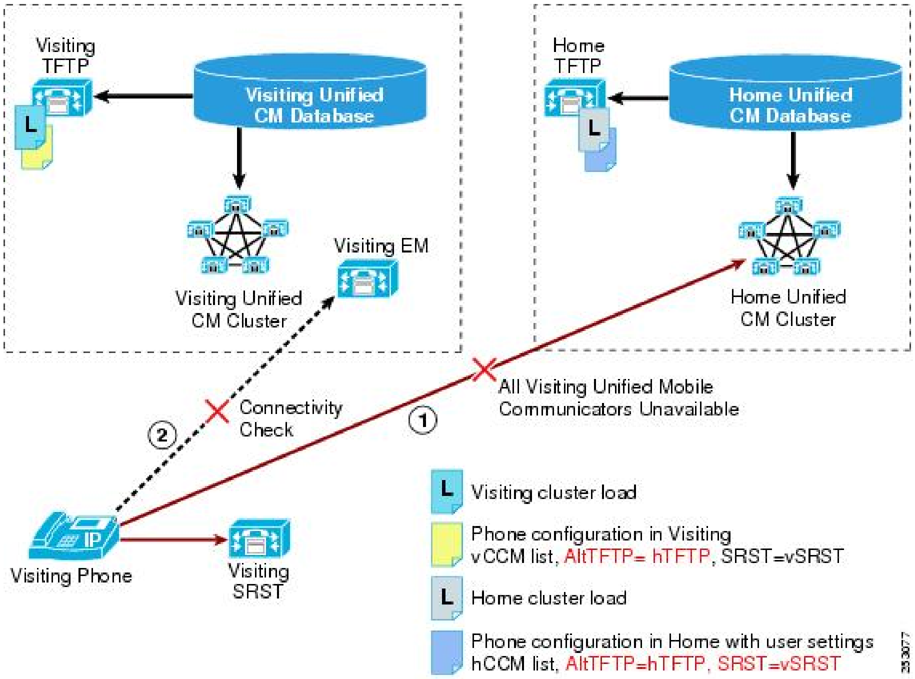


EMCC Failure - Home CUCM Unavailable/Interoffice Failure

The following figure illustrates EMCC failure when the home Cisco Unified Communications Manager is unavailable and an interoffice failure occurs.

The phone fails over to SRST.

Figure 49: EMCC Failure - Home Cisco Unified Communications Manager Unavailable/Interoffice Failure

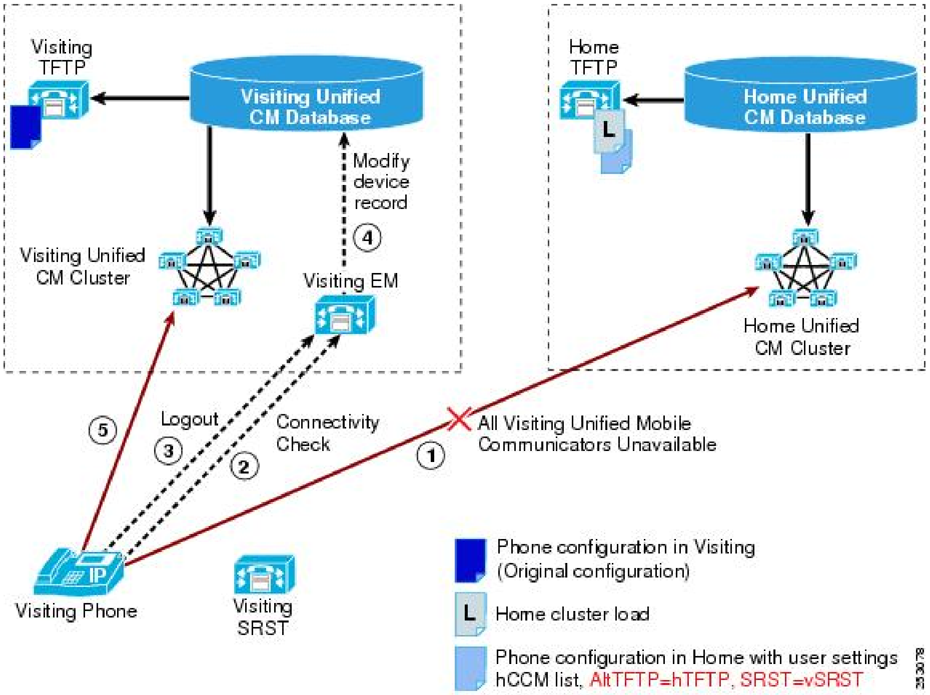

Visiting TFTP
L
Visiting Unified CM Database
Visiting Unified CM Cluster
Visiting EM
Home TFTP
L
Home Unified CM Database
Home Unified CM Cluster
All Visiting Unified Mobile Communicators Unavailable
Connectivity Check
2
1
IP
Visiting Phone
Visiting SRST
L
Visiting cluster load
Phone configuration in Visiting vCCM list, AltTFTP= hTFTP, SRST=vSRST
L
Home cluster load
Phone configuration in Home with user settings hCCM list, AltTFTP=hTFTP, SRST=vSRST
253077

EMCC Failure - Home CUCM Unavailable/inter-Cluster Failure

The following figure illustrates EMCC failure when the home Cisco Unified Communications Manager is unavailable and an inter-cluster failure occurs.

The phone reregisters with the visiting cluster.

Figure 50: EMCC Failure - Home Cisco Unified Communications Manager Unavailable/Inter-Cluster Failure

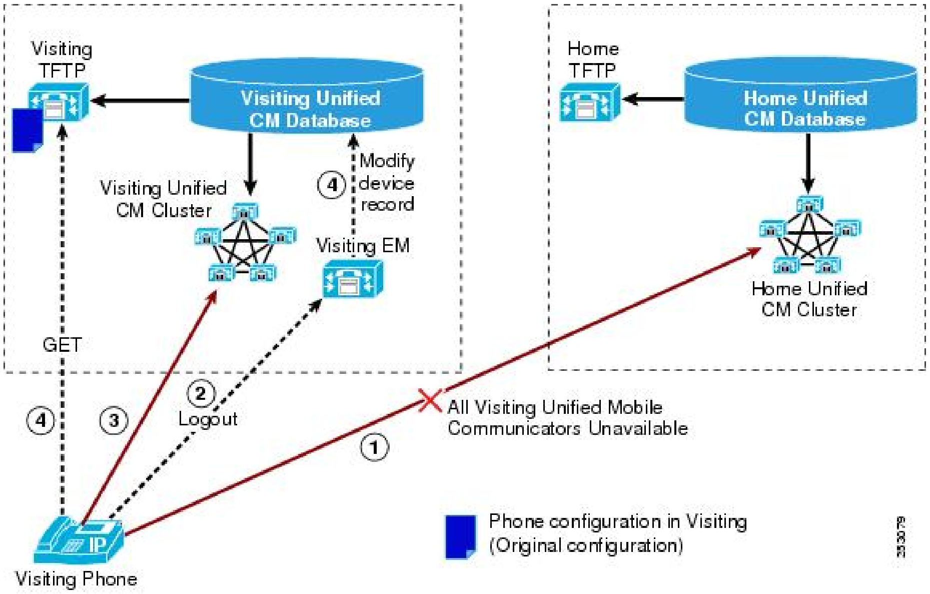

Visiting TFTP
Visiting Unified CM Database
Modify device record
4
Visiting Unified CM Cluster
Visiting EM
Home TFTP
L
Home Unified CM Database
Home Unified CM Cluster
5
Logout
3
Connectivity Check
2
All Visiting Unified Mobile Communicators Unavailable
1
IP
Visiting Phone
Visiting SRST
Phone configuration in Visiting (Original configuration)
L Home cluster load
Phone configuration in Home with user settings hCCM list, AltTFTP=hTFTP, SRST=vSRST
253078

EMCC Failure - Home CUCM Unavailable/Inter-Cluster Failure (No Visiting SRST)

The following figure illustrates EMCC failure when the home Cisco Unified Communications Manager is unavailable, an inter-cluster failure occurs, and no visiting SRST applies.

The phone reregisters with the visiting cluster.

Figure 51: EMCC Failure - Configuration File Unavailable, Inter-Cluster Failure Occurs, and No Visiting SRST Applies


Visiting TFTP
Visiting Unified CM Database
Modify device record
4
Visiting Unified CM Cluster
Visiting EM
Home TFTP
Home Unified CM Database
Home Unified CM Cluster
GET
4
3
2
Logout
All Visiting Unified Mobile Communicators Unavailable
1
IP
Visiting Phone
Phone configuration in Visiting (Original configuration)
253079

Phone Security with EMCC

See the Cisco Unified Communications Manager Security Guide for details of phone security issues in an EMCC environment.

System Requirements for EMCC

The following system requirements exist for Cisco Unified Communications Manager:

- Cisco Unified Communications Manager, Release 8.0(1) or higher
- Cisco Extension Mobility service
- Cisco Unified Communications Operating System
- Cisco Bulk Provisioning service
- Other call-control entities that support and use the Cisco Extension Mobility Cross Cluster configuration; for example, other Cisco Unified Communications Manager clusters, EMCC intercluster service profiles, and EMCC remote cluster services

Interactions and Restrictions

This section provides the details of interactions and restrictions for Cisco Extension Mobility Cross Cluster.

EMCC Interactions

This section lists the interactions of the Cisco Extension Mobility Cross Cluster with other Cisco Unified Communications Manager Administration components.

With the Cisco Extension Mobility Cross Cluster cross-registration solution, user features function as expected across clusters. The following list specifies some of the user features that function across clusters:

- Shared lines
- Hunt lists
- Transfer/Conference/Hold
- Call Forward
- Cisco Unified Mobility
- Barge/cBarge
- iDivert
- Applications
- Speed dials
- Services
- Address book

- Device labels
- Line appearance management
- MWI
- Voice mail
- Do Not Disturb
- Monitoring and Recording
- Callback Busy/NR
- Multilevel Precedence and Preemption (MLPP)

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 53: 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 54: 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 55: 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

EMCC Restrictions

This section lists the restrictions and limitations of the Cisco Extension Mobility Cross Cluster with other Cisco Unified Communications Manager Administration components.

EMCC Logout Limitations

Observe the following EMCC logout limitations:

- If the home cluster administrator disables the EMCC capability of an end user while the end user is logged in with EMCC, the system does not automatically log this end user out. (In this scenario, the administrator unchecks the Enable Extension Mobility Cross Cluster check box in the End User Configuration window for the end user.) Instead, the system only fails future EMCC attempts by this end user. The current EMCC session continues until the end user logs out.

- In the visiting cluster, the current Phone Configuration window has a Log Out button for intracluster EM. This button is also used by the visiting cluster administrator to logout an EMCC phone. Because the EMCC phone is not currently registered with the visiting Cisco Unified Communications Manager, this operation is equivalent to a DB cleanup in the visiting cluster. The EMCC phone will remain registered with the home Cisco Unified Communications Manager until it comes back to the visiting cluster due to a reset or a logout from the home cluster by other means.

EMCC Does Not Support Intercom Feature

Intercom configuration specifies configuration to a static device, so Cisco Extension Mobility Cross Cluster does not support the Intercom feature.

EMCC Does Not Support Location-Based CAC

Location CAC does not get supported.

RSVP-based CAC does get supported.

EMCC Limitations and Configuration Requirements with Local Route Groups

See the following sections for details of EMCC limitations and configuration requirements in routing EMCC calls with local route groups:

- EMCC Call Processing Configuration, on page 513
- Configure Visiting Cluster Emergency Pattern, on page 515
- Local Route Group of EMCC, on page 516
- Local Route Group Using EMCC SIP Trunk, on page 516

EMCC Device Cannot Be Provisioned in More Than One Cluster

Cisco Systems recommends that autoregistration be disabled (to avoid accidental provisioning).

EMCC and Security Mode Among Clusters

All clusters must specify the same security mode; either

- Clusters can be non-secure or mixed-mode clusters.
- Phones that allow Cisco Extension Mobility Cross Cluster can be in secure and non-secure mode.

Visiting Phone Login Limitation

The Cisco Extension Mobility service in participating clusters performs a periodic remote cluster update. The EMCC Feature Configuration feature parameter, Remote Cluster Update Interval, controls the update interval, for which the default value specifies 30 minutes.

If the Cisco Extension Mobility service on cluster A does not get back a reply from a remote cluster (such as cluster B) for this update, the Remote Cluster window for cluster A shows that 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 as 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 (23) message.

At this point, trying to log in EMCC from a visiting phone may fail with the error, Login is unavailable (23), which displays on the phone. This occurs because the visiting cluster has not yet detected the change of home cluster Cisco Unified Communications Manager from out-of-service to in-service.

Detection of status change of remote clusters is based on the value of the Remote Cluster Update Interval EMCC feature parameter and on when the visiting Cisco Extension Mobility service performed the last query/update.

You can also click the Update Remote Cluster Now button on 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.

EMCC and Product Specific Configuration Layout

Install and Activate EMCC

After you install Cisco Unified Communications Manager, your network can support the Cisco Extension Mobility Cross Cluster feature if you perform the necessary configuration tasks. For information on configuration tasks that you must perform, see the Configure EMCC, on page 497.

Configure EMCC

This section contains information about configuring EMCC.

Configure EMCC Feature Configuration

The following table provides detailed descriptions of the EMCC feature parameters that you configure in the EMCC Feature Configuration window (**Advanced Features** > **EMCC** > **EMCC Feature Configuration**).

Table 56: EMCC Feature Parameter Configuration Settings

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 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.

EMCC Parameter	Description
Default Interval for Expired EMCC Device Maintenance	Specify the number of minutes that elapse between checks of the system for expired EMCC devices. An expired EMCC device specifies a device that logged in to EMCC from a remote cluster, but that, due to WAN failure or a connectivity issue, the phone logged out of the visiting cluster and, when connectivity was restored, logged back into the visiting cluster. During this maintenance job, the Cisco Extension Mobility service checks the Cisco Unified Communications Manager database for any expired EMCC devices and automatically logs such devices out. Default value specifies 1440 minutes. Valid values range from 10 minutes to 1440 minutes.
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 specify 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 Cisco Unified Communications Manager Administration). You may prefer to enable the services manually so that you have time to configure the EMCC feature completely before enabling the remote services. Default value specifies False.

EMCC Parameter	Description
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 specifies the SIP trunk that has been configured for PSTN access in the Intercluster Service Profile window in Cisco Unified Communications Manager Administration. Calls over this trunk are intended for and only get routed to the local PSTN that is co-located with the EMCC logged-in phone that initiates the call. Valid values specify 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 get 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). Default value specifies Use trunk CSS.
EMCC Geolocation Filter	Choose the geolocation filter that you have configured for use with the Cisco Extension Mobility Cross Cluster feature. You must previously configure the EMCC geolocation filters to be able to choose a value in this drop-down list box. Based on the information in the geolocation that associates with a phone that is logged in via 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 gets applied.

EMCC Parameter	Description
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. Default value specifies 8 kbps (G.729). **Note** Communicate your EMCC Region Max Audio Bit Rate to the other clusters with which your cluster interacts. All participating EMCC clusters must specify the same EMCC Region Max Audio Bit Rate.
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. Default value specifies 384. Valid values range from 0 to 8128. **Note** Communicate your EMCC Region Max Video Call Bit Rate to the other clusters with which your cluster interacts. All participating EMCC clusters must specify the same EMCC Region Max Video Call Bit Rate.

EMCC Parameter	Description
EMCC Region Link Loss Type	This parameter specifies the link loss type between any EMCC phone and devices in any remote cluster. **Note** Communicate your EMCC Region Link Loss Type to the other clusters with which your cluster interacts. 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 chosen, 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 specify 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 this parameter is set 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, given the assumption that 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, given the assumption that 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 iSAC (Internet Speech Audio Codec) 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. Default value specifies Low Loss.

EMCC Parameter	Description
RSVP SIP Trunk KeepAlive Timer	Specify the number of seconds that Cisco 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 specifies 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, Cisco Unified Communications Manager releases the RSVP resources with the remote cluster. Default value specifies 15 seconds. Valid values range from 1 second to 600 seconds.
Default Server For Remote Cluster Update	Choose the default server name or IP address of the primary Cisco Unified Communications Manager 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 Cisco Unified Communications Manager 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 get information about this local cluster.
Remote Cluster Update Interval	Specify an interval, in minutes, during which the Cisco Extension Mobility service on the local Cisco Unified Communications Manager node collects information about the remote EMCC cluster. Collected information includes such details as the remote cluster Cisco Unified Communications Manager version and service information. Default value specifies 30. Valid values range from 15 minutes to 10,080 minutes.

EMCC Intercluster Service Profile Configuration Settings

In the Intercluster Service Profile Configuration window, you configure an EMCC intercluster service profile. In Unified Communications Manager, use the **Advanced Features** > **EMCC** > **EMCC Intercluster Service Profile** menu option to display this window.

Table 57: EMCC Intercluster Service Profile Configuration Settings

Field	Description
EMCC	
Active	Check this check box to activate the Cisco Extension Mobility Cross Cluster feature.
PSTN Access	
Active	Check this box to activate PSTN access.
SIP trunk	From the drop-down list box, choose the SIP trunk to use for PSTN access. You must first specify a SIP trunk (**Device** > **Trunk**) and configure it for PSTN access
RSVP Agent	
Active	Click this box to activate RSVP Agent.
SIP trunk	From the drop-down list box, choose the SIP trunk to use for RSVP Agent. You must first specify a SIP trunk (**Device** > **Trunk**).
EMCC Setup Validation Report	
Configuration(s)	After you click **Save**, this pane displays the EMCC Setup Validation Report. If you click **Validate**, a popup window, displays the EMCC Setup Validation Report. Click **Close** to close the popup window. The Configuration(s) column of the report displays the following entities that get validated: • EMCC PSTN Access Service • Default TFTP Server for EMCC Login Device • EMCC Geolocation Filter • EMCC Service Default Server for Remote Cluster • EMCC Devices • ClusterId
Status	Displays the status of each configuration upon validation of the EMCC intercluster service profile. For each entity, valid values include Success and Failure.
Error Message	For each failed configuration, an error message explains the configuration that must take place in order to achieve success.

Remote Cluster Configuration

In Cisco Unified Communications Manager Administration, use the **Advanced Features** > **Cluster View** menu path to configure remote clusters.

Tips About Finding Remote Clusters

The Find operation locates only those remote clusters that you added previously. The Find operation does not locate the clusters that belong to the enterprise automatically.

Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the Cisco Unified Communications Manager Administration Guide and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration Settings Table

The following table provides detailed descriptions of the remote cluster configuration settings that you configure in the Remote Cluster Configuration window (**Advanced Features** > **Cluster View**).

Table 58: Remote Cluster Configuration Settings

Field	Description
Remote Cluster Information	
Cluster Id	Enter the cluster ID of the remote cluster. Valid values include alphanumeric characters, period (.), and hyphen (-).
Description	Enter a description for the remote cluster. This field accepts up to 128 characters. You may use all characters except quotes (“), close angle bracket (>), open angle bracket (<), backslash (\), dash (-), ampersand (&), and percent sign (%).
Fully Qualified Name	Enter the fully qualified name of the remote cluster. This field accepts up to 50 characters and allows the following characters: alphanumeric (a through z, A through Z, and 0 through 9), period (.), dash (-), asterisk (*), and space ( ).
Remote Cluster Service Information	

Field	Description
EMCC	For the EMCC service, the following column headings detail the configuration for this service: • Enabled - If the EMCC service is enabled, this box gets checked. • Service - This entry specifies the EMCC service. • Remote Activated - Valid values specify true or false. • Address 1 - This column lists the first address for this service. • Address 2 - This column lists the second address for this service. • Address 3 - This column lists the third address for this service.
PSTN Access	For PSTN access, the following column headings detail the configuration for this service: • Enabled - If PSTN access is enabled, this box gets checked. • Service - This entry specifies PSTN access. • Remote Activated - Valid values specify true or false. • Address 1 - This column lists the first address for this service. • Address 2 - This column lists the second address for this service. • Address 3 - This column lists the third address for this service.
RSVP Agent	For the RSVP Agent, the following column headings detail the configuration for this service: • Enabled - If RSVP Agent is enabled, this box gets checked. • Service - This entry specifies RSVP Agent. • Remote Activated - Valid values specify true or false. • Address 1 - This column lists the first address for this service. • Address 2 - This column lists the second address for this service. • Address 3 - This column lists the third address for this service.

Field	Description
TFTP	For the TFTP service, the following column headings detail the configuration for this service: • Enabled—If the TFTP service is enabled, this box gets checked. • Service—This entry specifies the EMCC service. • Remote Activated—Valid values specify true or false. **Note** The value of the Remote Activated column is set to true whenever remote IP addresses are configured either manually or dynamically. • Address 1—This column lists the first address for this service. **Note** When you upgrade from Cisco Unified Communications Manager 8.6 (1) to Cisco Unified Communications Manager 8.6 (2) or later, Address 1 is automatically updated by the system. However, if this field is blank after the upgrade due to some reason such as DNS lookup failure, you must manually update it with the appropriate IP address of the TFTP service. • Address 2—This column lists the second address for this service. • Address 3—This column lists the third address for this service.

Field	Description
UDS	This check box toggles remote cluster lookup for User Data Services (UDS) on the remote cluster. • Enabled - If UDS is enabled, this box is checked. • Service - This entry specifies UDS. • Remote Activated - Valid values specify true or false. • Address 1 - This column lists the first address for this service. • Address 2 - This column lists the second address for this service. • Address 3 - This column lists the third address for this service. Consider the following example configuration: • A three node cluster (A, B, C), with node A having entries for B and C in cluster view • UDS is checked for B and unchecked for C. • When you search for user B on node A using the HTTPS GET method, the search result is a user found on cluster B. • When you search for user C on node A using the HTTPS GET method, the search result is a no user found on cluster B.
Enabled All Services	Click this button to enable all services.
Disabled All Services	Click this button to disable all services.
Update Remote Cluster Now	Click this button to update the remote cluster immediately.

Provide Information to Users

End users log in and out of Extension Mobility Cross Cluster feature just as they do from the Extension Mobility feature, and they receive no indication of which cluster they are using.

Troubleshooting EMCC

This section provides information about error codes for EMApp and EMService.

For information on troubleshooting Cisco Extension Mobility Cross Cluster, refer to the *Cisco Unified Communications Manager Troubleshooting Guide*.

Error Codes for EMApp

The following table lists and describes the error codes that apply to the Cisco Extension Mobility application (EMApp).

Table 59: Error Codes for the Cisco Extension Mobility Application (EMApp)

Error Code	Phone Display	Quick Description	Description
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 in the Inter-cluster Service Profile page.
202	Please try to login again (202)	Blank userid or pin	User enters blank user ID or PIN.
204	Login is unavailable (204)	Directory server error	EMApp sends this error to 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 could not be retrieved either from the cache or from the database.
207	Login is unavailable(207) Logout is unavailable(207)	Device Name Empty	Occurs when device or name tag is missing in the request URI. This cannot happen with real devices and can occur only if request is sent from third-party applications.
208	Login is unavailable(208) Logout is unavailable(208)	EMService Connection Error	Visiting EMApp could not connect to any Visiting EMService. (Service is down or not activated.) Visiting EMService could not connect to Home EMService (WAN is down or certificates are not trusted.)

Error Code	Phone Display	Quick Description	Description
210	Login is unavailable(210) Logout is unavailable(210)	Init Fail-Contact Admin	Some error (like database connection failure) occurred while initializing EMApp. The error may occur because of failure in connecting to the database during startup. This represents a catastrophic error.
211	Login is unavailable(211) Logout is unavailable(211)	EMCC Not Activated	Occurs when 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 updated (keep-alive) fails by sending an incorrect cluster ID to remote cluster.
213	Login is unavailable(213) Logout is unavailable(213)	Device does not support EMCC	Occurs when a device (phone load) does not have EMCC capability (for example, for legacy phones or for TNP phones with older phone load).

Error Codes for EMService

The following table lists and describes the error codes that apply to the Cisco Extension Mobility service (EMService).

Table 60: Error Codes for the Cisco Extension Mobility Service (EMService)

Error Code	Phone Display	Quick Description	Description
0	Login is unavailable(0) Logout is unavailable(0)	Unknown Error	EMService failed in some totally unexpected scenario. It is catastrophic.

Error Code	Phone Display	Quick Description	Description
1	Login is unavailable(1) Logout is unavailable(1)	Error on parsing	When EMService could not parse the XML request from EMApp/EMService. This happens when 3rd party applications sends an incorrect query/login XML (EM API) or it can occur because of mis-match in version between home and visiting CUCM versions (for EMCC).
2	Login is unavailable(2)	EMCC Authentication Error	EMCC user credentials could not be authenticated as the user has entered wrong pin.
3	Login is unavailable(3) Logout is unavailable(3)	Invalid App User	Invalid application user. This can be seen commonly when using EM API.
4	Login is unavailable(4) Logout is unavailable(4)	Policy Validation error	EM Service sends this error when it could not validate the login/logout request due to some unknown reason (Error while querying the database or error while retrieving info from cache).
5	Login is unavailable(5) Logout is unavailable(5)	Dev. logon disabled	EM / EMCC Login is requested for a device which has “Enable extension mobility” unchecked in phone configuration page.
6	Login is unavailable(6) Logout is unavailable(6)	Database Error	Whenever database throws an exception while executing the query or stored procedure requested by EM Service (login/logout or device/user query), EM Service sends this error code to EM App.

Error Code	Phone Display	Quick Description	Description
8	Login is unavailable(8) Logout is unavailable(8)	Query type undetermined	No Valid query has been sent to the EMService (DeviceUserQuery & UserDeviceQuery are valid ones). This is ideally seen when using EM API with incorrect XML input.
9	Login is unavailable(9) Logout is unavailable(9)	Dir. User Info Error	This error is displayed in two cases: **1.** IMS throws an exception when it tries to authenticate a particular user. **2.** When information about a particular user could not be retrieved either from cache or database.
10	Login is unavailable(10) Logout is unavailable(10)	User lacks app proxy rights	User tries to do login/query on behalf of some other user (By default, only CCMSysUser has the admin rights.)
11	Login is unavailable(11) Logout is unavailable(11)	Device Does not exist	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 (EMCC Login)
18	Login is unavailable(18)	Another user logged in	Another user is already logged in on that particular phone
19	Logout is unavailable(19)	No user logged in	Trying to logout a user which has not logged in. This can ideally happen when sending logout requests from the 3rd party applications (EM API).
20	Login is unavailable(20) Logout is unavailable(20)	Hoteling flag error	“Enable extension mobility” is unchecked in phone configuration page.

Error Code	Phone Display	Quick Description	Description
21	Login is unavailable(21) Logout is unavailable(21)	Hoteling Status error	Current user status could not be retrieved from either local cache or database (when PolicyValidator tried to check current login User or login time).
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	User has currently logged in on some other phone
26	Login is unavailable(26) Logout is unavailable(26)	Busy, please try again	When EMService has currently reached the threshold level of “Maximum Concurrent Requests” service parameter
28	Login is unavailable(28) Logout is unavailable(28)	Untrusted IP Error	When “Validate IP Address” service parameter is set to true and user tries to login/logout from a machine whose IP address is not trusted (for example, 3rd party app / EM API from a machine which is not listed in Trusted List of Ips service parameter).
29	Login is unavailable(29) Logout is unavailable(29)	ris down-contact admin	RISDC Cache has not been created and initialized and EMService is unable to connect to RISDC

Error Code	Phone Display	Quick Description	Description
30	Login is unavailable(30) Logout is unavailable(30)	Proxy not allowed	When login/logout comes through proxy (“Via” is set in HTTP header) and “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 Enable Extension Mobility Cross Cluster check box is not checked in the End User 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 (for example, legacy phones)
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.
36	Login is unavailable(36) Logout is unavailable(36)	No Remote Cluster	Occurs when the administrator has not added any remote cluster.
37	Login is Unavailable (37) Logout is Unavailable (37)	Duplicate Device Name	Occurs when the same device name exists in both home cluster and visiting cluster.
38	Login is unavailable(38) Logout is unavailable(38)	EMCC Not Allowed	Occurs when home cluster does not want to allow EMCC login (Enable Extension Mobility Cross Cluster check box is not checked in the home cluster).
42	Login is unavailable(42) Logout is unavailable(42)	Invalid ClusterID	Occurs when the remote cluster ID is not valid (happens during remote cluster update)

Error Code	Phone Display	Quick Description	Description
43	Login is unavailable(43)	Device Security mode error	Device Security Profile associated to the EMCC device should be Non Secure for its Device Security Mode. **Note** This error code does not apply for Cisco Unified Communications Manager Release 9.x and above.
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 non-secure mode.

CHAPTER 23

External Call Control

This chapter provides information about the external call control feature, which enables an adjunct route server to make call-routing decisions for Cisco Unified Communications Manager by using the 8.0(2) Cisco Unified Routing Rules Interface. When you configure external call control, Cisco Unified Communications Manager issues a route request that contains the calling party and called party information to the adjunct route server. The adjunct route server receives the request, applies appropriate business logic, and returns a route response that instructs Cisco Unified Communications Manager on how the call should get routed, along with any additional call treatment that should get applied.

The adjunct route server can instruct Cisco Unified Communications Manager to allow, divert, or deny the call, modify calling and called party information, play announcements to callers, reset call history so adjunct voicemail and IVR servers can properly interpret calling/called party information, and log reason codes that indicate why calls were diverted or denied. The following examples show how external call control can work:

- Best Quality Voice Routing - The adjunct route server monitors network link availability, bandwidth usage, latency, jitter, and MOS scores to ensure calls are routed through voice gateways that deliver the best voice quality to all call participants.
- Least Cost Routing - The adjunct route server is configured with carrier contract information such as Lata and Inter-Lata rate plans, trunking costs, and burst utilization costs to ensure calls are routed over the most cost effective links.
- Ethical Wall - The adjunct route server is configured with corporate policies that determine reachability; for example, Is user 1 allowed to call user 2?. When Cisco Unified Communications Manager issues a route request, the route server sends a response that indicates whether the call should be allowed, denied, or redirected to another party.

For more information on the Cisco Unified Routing Rules interface, see the *Cisco Unified Communications Manager XML Developers Guide for Release 8.0(2)*.

Configure External Call Control

Cisco Unified Communications Manager, Release 8.0(2) (or higher), supports the external call control feature, which enables an adjunct route server to make call-routing decisions forCisco Unified Communications Manager by using the 8.0(2) Cisco Unified Routing Rules Interface. When you configure external call control, Cisco Unified Communications Manager issues a route request that contains the calling party and called party information to the adjunct route server. The adjunct route server receives the request, applies appropriate business logic, and returns a route response that instructs Cisco Unified Communications Manager on how the call should get routed, along with any additional call treatment that should get applied.

The adjunct route server can instruct Cisco Unified Communications Manager to allow, divert, or deny the call, modify calling and called party information, play announcements to callers, reset call history so adjunct voicemail and IVR servers can properly interpret calling/called party information, and log reason codes that indicate why calls were diverted or denied. The following examples show how external call control can work:

- Best Quality Voice Routing - The adjunct route server monitors network link availability, bandwidth usage, latency, jitter, and MOS scores to ensure calls are routed through voice gateways that deliver the best voice quality to all call participants.
- Least Cost Routing - The adjunct route server is configured with carrier contract information such as Lata and Inter-Lata rate plans, trunking costs, and burst utilization costs to ensure calls are routed over the most cost effective links.
- Ethical Wall - The adjunct route server is configured with corporate policies that determine reachability; for example, Is user 1 allowed to call user 2?. When Cisco Unified Communications Manager issues a route request, the route server sends a response that indicates whether the call should be allowed, denied, or redirected to another party.

Perform the following steps to configure external call control in your network.

Procedure

Step 1 Set up the Cisco Unified Routing Rules Interface so that the route server can direct Cisco Unified Communications Manager on how to handle calls.

Step 2 Configure a calling search space that Cisco Unified Communications Manager uses when the route server sends a divert obligation to Cisco Unified Communications Manager. (**Call Routing** > **Class of Control** > **Calling Search Space**) You assign this calling search space to the external call control profile when you configure the profile.

Step 3 Configure the external call control profile(s). (**Call Routing** > **External Call Control Profile**)

Step 4 For the translation patterns that you want to use with external call control, assign an external call control profile to the pattern. (**Call Routing** > **Translation Pattern**)

Step 5 If the route server uses https, import the certificate for the route server into the trusted store on the Cisco Unified Communications Manager server. (In Cisco Unified Communications Operating System, choose **Security** > **Certificate Management**.) You must perform this task on each node in the cluster that can send routing queries to the route server.

Step 6 If the route server uses https, export the Cisco Unified Communications Manager self-signed certificate to the route server. (In Cisco Unified Communications Operating System, choose **Security** > **Certificate Management**.) You must perform this task for each node in the cluster that can send routing queries to the route server.

Step 7 If your routing rules from the route server state that a chaperone must monitor and/or record a call, configure chaperone functionality in Cisco Unified Communications Manager Administration.

- For phones where you want to enable recording, set the Built-in-Bridge to On in the Phone Configuration window.
- Create a recording profile. Choose **Device** > **Device Settings** > **Recording Profile**, and create a Call Recording Profile for the phones that can record chaperoned conferences.
- Apply the recording profile to the line appearance.
- Add a SIP trunk to point to the recorder, and create a route pattern that points to the SIP Trunk.
- Configure the Play Recording Notification Tone to Observed Target and Play Recording Notification Tone to Observed Connected Target service parameters.
- Assign the Standard Chaperone Phone softkey template to the phone that the chaperone uses.
- Make sure that the chaperone phone does not have shared lines or multiple directory numbers/lines configured for it. Configure only one directory number for the chaperone phone. (**Call Routing** > **Directory Number** or **Device** > **Phone** if the phone is already configured)
- For the directory number on the chaperone phone, choose Device Invoked Call Recording Enabled from the Recording Option drop-down list box. (**Call Routing** > **Directory Number** or **Device** > **Phone** if the phone is already configured)
- For the directory number on the chaperone phone, enter 2 for the Maximum Number of Calls setting, and enter 1 for the Busy Trigger setting. (**Call Routing** > **Directory Number** or **Device** > **Phone** if the phone is already configured)
- For Cisco Unified IP Phones that support the Record softkey, make sure that the Standard Chaperone Phone softkey template is configured so that only the conference, record, and end call softkeys display on the phone in a connected state.
- For Cisco Unified IP Phones that support the Record programmable line keys (PLK), configure the PLK in the Phone Button Template Configuration window.
- If you have more than one chaperone in your cluster, add the chaperone DN to the chaperone line group that you plan to assign to the chaperone hunt list. Adding the chaperone to the line group, which belongs to the hunt list, ensures that an available chaperone monitors the call.

Step 8 If your routing rules require that an announcement get played for some calls and you do not want to use the Cisco-provided announcements, overwrite the Cisco-provided announcements with your customized announcements in the Announcements window. (**Media Resources** > **Announcements**) If you do not use the Cisco-provided announcements, configure annunciator so that you can use your customized announcements. (**Media Resources** > **Annunciator**)

Related Topics

Interactions and Restrictions, on page 553
External Call Control Profile Configuration, on page 557
Find Configuration Records for External Call Control Profiles, on page 561
Configure an External Call Control Profile, on page 562
Assign the External Call Control Profile to the Translation Pattern, on page 563
Generate a CUCM Self-Signed Certificate for Export, on page 564
Chaperone Support for Routing Rules, on page 551
Announcement Support for Routing Rules, on page 552

External Call Control Feature

CUCM Connections to the Adjunct Route Server

Cisco Unified Communications Manager maintains persistent connections to the adjunct route server to reduce delays with call setup. Each node in a Cisco Unified Communications Manager cluster may establish multiple connections to the adjunct route server for parallel/simultaneous queries at a high call rate. The Cisco Unified Communications Manager server may establish multiple connections to the adjunct route server for parallel/simultaneous queries at a high call rate. Cisco Unified Communications Manager manages a thread pool for the persistent connections, which is determined by the configuration for the following service parameters:

- External Call Control Initial Connection Count To PDP - This parameter specifies the minimum number of connections that Cisco Unified Communications Manager establishes to a adjunct route server for handling call routing requests.
- External Call Control Maximum Connection Count To PDP - This parameter specifies the maximum number of connections that Cisco Unified Communications Manager establishes to a adjunct route server for handling call routing requests.

For more information on these and other external call control service parameters, see the Service Parameters for External Call Control, on page 555.

External Call Control Profiles

In Cisco Unified Communications Manager Administration, you enable external call control by assigning a configured external call control profile to the translation pattern. The translation pattern is the trigger point for external call control; that is, if the translation pattern has an external call control profile assigned to it, when the called number on the call matches the translation pattern, Cisco Unified Communications Manager immediately sends a call-routing query to an adjunct route server, and the adjunct route server directs Cisco Unified Communications Manager on how to handle the call.

The external call control profile provides the URIs for a primary and redundant adjunct route server (called the web service in the GUI), a calling search space that is used for diverting calls, a timer that indicates how long Cisco Unified Communications Manager waits for a response from the adjunct route server, and so on.

In the external call control profiles that you configure in Cisco Unified Communications Manager Administration, you must provide the URI(s) for the adjunct route server(s) that provides the route decisions and obligations to the Cisco Unified Communications Manager. If you want to do so, you can configure one URI, known as the primary web service in Cisco Unified Communications Manager Administration, or you can configure primary and secondary URIs to create active and standby links to the adjunct route server(s). If you configure primary and secondary URIs, the route servers can load balance the call-routing queries in a round robin fashion. For the URIs, you can use http or https. If you specify https, Cisco Unified Communications Manager uses certificates to mutually authenticate via a TLS connection to the adjunct route server.

Tip If you use https, Cisco Unified Communications Manager verifies that the certificate subject name matches the hostname of the adjunct route server. Additionally, Cisco Unified Communications Manager verifies whether the signature of the certificate is issued by a trusted CA or if the signature matches a self-signed, imported certificate in the trusted store.

Tip To establish https connections, you must import certificates from each adjunct route server into the trusted store on each Cisco Unified Communications Manager node. Likewise, you must export a self-signed certificate from each Cisco Unified Communications Manager node and import it to the trusted store on each adjunct route server. For more information on these tasks, see the External Call Control Profile Configuration, on page 557 and the Generate a CUCM Self-Signed Certificate for Export, on page 564.

If Cisco Unified Communications Manager must redirect a call because the adjunct route server issues a divert routing directive, the configuration for the Diversion Rerouting CSS gets used.

In the external call control profile, you can configure the time that Cisco Unified Communications Manager waits for a response from the adjunct route server. If the timer expires, Cisco Unified Communications Manager either allows or blocks the call, based on how you configured the Call Treatment on Failure setting in the external call control profile.

Chaperone Support for Routing Rules

If routing rules from the adjunct route server state that a chaperone must be present on a call, you must configure chaperone support in Cisco Unified Communications Manager Administration. In this case, the adjunct route server sends the following routing directive to Cisco Unified Communications Manager:

- Permit decision
- Divert obligation that contains reason = chaperone.

A chaperone is a designated phone user who can announce company policies to the call, monitor the call, and record the call, if required. Cisco Unified Communications Manager provides the following capabilities to support chaperone functionality, as directed by the adjunct route server:

- Cisco Unified Communications Manager can redirect an incoming call to a chaperone or hunt group/list of chaperones.
- Cisco Unified Communications Manager can provide a chaperone with the ability to record a call.

When the chaperone is connected to the caller or when the chaperoned conference is established, the Record softkey or PLK (depending on the phone model) becomes active on the phone so that the chaperone can invoke call recording. Call recording occurs for the current call only, and call recording stops when the current call ends. Messages that indicate the status of recording may display on the phone when the chaperone presses the recording softkey/PLK.

Tip For a list of configuration tasks that you must perform in Cisco Unified Communications Manager Administration to set up chaperon support, see the Configure External Call Control, on page 548.

Chaperone restrictions exist so that the parties that are involved in the call cannot converse without the presence of the chaperone. The following restrictions exist for chaperones:

- The chaperone cannot use the phone to put the conference call on hold.
- The chaperone cannot use the phone to add parties to a conference after the conference begins because the call must be put on hold for the chaperone to add parties.

  After the chaperone creates a conference, the conference softkey gets disabled on the phone; that is, if the phone uses the conference softkey.

  Be aware that the other parties on the conference may be able to add additional parties to the conference. The configuration for the Advanced Ad Hoc Conference Enabled service parameter, which supports the Cisco CallManager service, determines whether other parties can add participants to the conference. If the service parameter is set to True, other parties can add participants to the conference.
- The chaperone cannot use the phone to transfer the conference call to another party.
- When the chaperone leaves the conference, the entire conference drops.
- If the chaperone starts recording before making a consultative call to the party that should join the conference, Cisco Unified Communications Manager suspends recording while the chaperone makes the consultative call; recording resumes after the conference is established.

Announcement Support for Routing Rules

Routing rules on the adjunct route server may require that Cisco Unified Communications Manager play an announcement for the call; for example, an announcement that states that the call is rejected or an announcement that issues a greeting to the caller before connecting the caller to the called party. When you install Cisco Unified Communications Manager, Cisco-provided announcements and tones install, and the Find and Lists Announcements window in Cisco Unified Communications Manager Administration displays these announcements and tones, which can be used for external call control. (**Media Resources** > **Announcements**) All announcements that display in the window support external call control, but the obligation that the adjunct route server issues determines which announcement Cisco Unified Communications Manager plays; for example, the obligation from the adjunct route server indicates that Cisco Unified Communications Manager must reject the call and play the Custom_05006 announcement.

Tip If you want to use customized announcements, not the Cisco-provided announcements, you can upload the customized announcements in the Announcements Configuration window.

Related Topics

Configure External Call Control, on page 548

System Requirements for External Call Control

The following system requirements exist for external call control:

- Cisco Unified Communications Manager 8.0(2) (or higher)
- Cisco Unified Routing Rules XML Interface, which provides the route decisions and obligation for the calls

Interactions and Restrictions

Annunciator

If your routing rules require that an announcement get played for calls, upload or customize the standard announcements in the Announcements window; that is, if you do not want to use the Cisco-provided announcements. (**Media Resources** > **Announcements**)

In you upload customized announcements, configure annunciator so that you can use the announcements. (**Media Resources** > **Annunciator**)

Best Call Quality Routing for Cisco Unified Communications Manager Calls

If you want to do so, you can set up routing rules on the adjunct route server that determine which gateway should be used for a call when voice quality is a consideration; for example, gateway A provides the best voice quality, so it gets used for the call. In this case, the adjunct route server monitors network link availability, bandwidth usage, latency, jitter, and MOS scores to ensure calls are routed through voice gateways that deliver the best voice quality to all call participants.

Call Detail Records

External call control functionality can display in call detail records; for example, the call detail record can indicate whether the adjunct route server permitted or rejected the call. In addition, the call detail record can indicate whether Cisco Unified Communications Manager blocked or allowed calls when Cisco Unified Communications Manager did not receive a decision from the adjunct route server. For more information on call detail records and external call control, see the *Cisco Unified Communications Manager Call Detail Records Administration Guide*.

Call Forward

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; that is, for calls that where call forward is invoked, Cisco 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 gets triggered only when the adjunct route server sends a Permit decision with a Continue obligation to the Cisco Unified Communications Manager.

Be aware that 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; that is, they work separately.

Call Pickup

When Cisco Unified Communications Manager recognizes that a phone user is trying to pick up a call by using the call pickup feature, external call control does not get invoked; that is, Cisco Unified Communications Manager does not send a routing query to the adjunct route server for that portion of the call.

Chaperones

A chaperone is a designated phone user who can announce company policies to the call, monitor the call, and record the call, if required. Chaperone restrictions exist so that the parties that are involved in the call cannot converse without the presence of the chaperone. For chaperone restrictions, see the Chaperone Support for Routing Rules, on page 551.

Cisco Unified Mobility

Cisco Unified Communications Manager honors the route decision from the adjunct route server for the following Cisco Unified Mobility features:

- Mobile Voice Access
- Enterprise Feature Access
- Dial-via-Office Reverse Callback
- Dial-via-Office Forward

Tip To invoke Mobile Voice Access or Enterprise Feature Access, the end user must dial a feature directory number that is configured in Cisco Unified Communications Manager Administration. When the Cisco Unified Communications Manager receives the call, Cisco Unified Communications Manager does not invoke external call control because the called number, in this case, is the feature DN. After the call is anchored, the Cisco Unified Communications Manager asks for user authentication, and the user enters the number for the target party. When Cisco Unified Communications Manager tries to extend the call to the target party, external call control gets invoked, and Cisco Unified Communications Manager sends a call routing query to the adjunct route server to determine how to handle the call.

Cisco Unified Communications Manager does not send a routing query for the following Cisco Unified Mobility features:

- Cell pickup
- Desk pickup
- Session handoff

Cisco Unified Serviceability

Alarm definitions for external call control display in Cisco Unified Serviceability under the Cisco CallManager alarm catalog. For information on the alarm definitions, see the Troubleshooting Guide for Cisco Unified Communications Manager.

Conferences

When a phone user creates a conference, external call control may get invoked for the primary call and consultative call.

Directory Numbers

When you configure directory numbers as 4- or 5- digit extensions (enterprise extensions), you need to configure 2 translation patterns if on-net dialing supports 4 or 5 digits. One translation pattern supports globalizing the calling/called numbers, and a second translation pattern supports localizing the calling/called numbers. Assign external call control profile on the translation pattern that is used for globalizing the calling/called numbers.

Do Not Disturb

By default, the DND setting for the user takes effect when the user rule on the adjunct route server indicates that the adjunct route server send a continue obligation. For example, if the adjunct route server sends a continue obligation, and the user has DND-R enabled, Cisco Unified Communications Manager rejects the call.

Emergency Call Handling (for Example, 911 or 9.11)

Caution Cisco strongly recommends that you configure a very explicit set of patterns for emergency calls (for example, 911 or 9.911) so that the calls route to their proper destination (for example, to Cisco Emergency Responder or a gateway) without having to contact the route server for instructions on how to handle the call.

Real Time Monitoring Tool

For external call control, performance monitoring counters display under the External Call Control object and the Cisco CallManager object in RTMT. For information on these counters, see the Troubleshooting Guide for Cisco Unified Communications Manager.

Transfer

When a phone user transfers a call, external call control may get invoked for both the primary call and consultative call. However, Cisco Unified Communications Manager cannot enforce any routing rules from the adjunct route server between the party that transfers and the target of the transfer.

Install and Activate External Call Control

After you install Cisco Unified Communications Manager, your network can support external call control if you perform the necessary configuration tasks. For information on configuration tasks that you must perform, see the Configure External Call Control, on page 548.

External Call Control Configuration

This section provides information to configure External Call Control.

Tip Before you configure External Call Control, review the configuration summary task for External Call Control.

Related Topics

Configure External Call Control, on page 548

Service Parameters for External Call Control

To access the service parameters that support the external call control feature, choose **System** > **Service Parameters**. Choose the server and the Cisco CallManager service. Then, locate the Clusterwide Parameters

(Feature - External Call Control) pane. This table describes the service parameters for the external call control feature. For additional information, you can click the question mark help in the Service Parameters window.

Table 61: External Call Control Service Parameters

Service Parameter	Description
External Call Control Diversion Maximum Hop Count	This parameter specifies the maximum number of times the adjunct route server can issue a divert obligation for a single call. The default equals 12. The minimum value is 1, and the maximum value is 500.
Maximum External Call Control Diversion Hops to Pattern or DN	This parameter specifies the maximum number of times that the adjunct route server can issue the divert obligation for a call to a directory number, route pattern, translation pattern, or hunt pilot. The default is 12; the minimum is 1, and the maximum is 60.
External Call Control Routing Request Timer	This parameter specifies the maximum time, in milliseconds, that Cisco Unified Communications Manager should wait for the call routing directive from the adjunct route server before allowing or blocking the call, as configured in the Call Treatment on Failures setting in the external call control profile. The default is 2000; the minimum value is 1000, and the maximum value is 5000.
External Call Control Fully Qualified Role And Resource	This parameter specifies the fully qualified role and the resource that Cisco Unified Communications Manager sends to the adjunct route server in the XACML call routing request. The value that you enter matches your configuration on the adjunct route server, and it ensures that the Cisco Unified Communications Manager query points to the correct routing rules on the adjunct route server. The default equals CISCO:UC:UCMPolicy:VoiceOrVideoCall, where CISCO:UC:UCMPolicy represents the role on the adjunct route server and VoiceOrVideoCall represents the resource on the adjunct route server. You can enter up to 100 characters, which include alphanumeric characters (A-Z,a-z,0-9) or colons (:). Colons are only allowed between alphanumeric characters.

Service Parameter	Description
External Call Control Initial Connection Count To PDP	This parameter specifies the initial number of connections that Cisco Unified Communications Manager establishes to a adjunct route server for handling call routing requests. Ensure that the value for this parameter is less than or equal to the External Call Control Maximum Connection Count To PDP value. If it is not less than or equal to the External Call Control Maximum Connection Count To PDP value, the External Call Control Maximum Connection Count To PDP value gets ignored. This setting applies to each URI that is configured in each external call control profile. The default is 2; the minimum value is 2, and the maximum value is 20.
External Call Control Maximum Connection Count To PDP	This parameter specifies the maximum number of connections that Cisco Unified Communications Manager establishes to a adjunct route server for handling call routing requests. Ensure that the value for this parameter is greater than or equal to the External Call Control Initial Connection Count To PDP value. If it is not greater than the External Call Control Initial Connection Count To PDP value, the value gets ignored. This setting applies to each URI that is configured in each external call control profile. The default is 4; the minimum value is 2, and the maximum value is 20.

External Call Control Profile Configuration

Cisco Unified Communications Manager, Release 8.0(2) (or higher), supports the external call control feature, which enables an adjunct route server to make call-routing decisions for Cisco Unified Communications Manager by using the 8.0(2) Cisco Unified Routing Rules Interface. When you configure external call control, Cisco Unified Communications Manager issues a route request that contains the calling party and called party information to the adjunct route server. The adjunct route server receives the request, applies appropriate business logic, and returns a route response that instructs Cisco Unified Communications Manager on how the call should get routed, along with any additional call treatment that should get applied.

The adjunct route server can instruct Cisco Unified Communications Manager to allow, divert, or deny the call, modify calling and called party information, play announcements to callers, reset call history so adjunct voicemail and IVR servers can properly interpret calling/called party information, and log reason codes that indicate why calls were diverted or denied.

The external call control profile provides the URI(s) for the adjunct route server(s), a calling search space that is used for diverting calls, a timer that indicates how long Cisco Unified Communications Manager waits for a response from the adjunct route server, and so on.

The following table describes the settings that display in the External Call Control Profile window (**Call Routing** > **External Call Control Profile**).

Before You Begin

Before you configure the external call control profile, configure a calling search space that Cisco Unified Communications Manager uses when the adjunct route server sends a divert obligation to Cisco Unified Communications Manager. (**Call Routing** > **Class of Control** > **Calling Search Space**)

Before you configure the external call control profile, review the Configure External Call Control, on page 548.

Next Step

After you configure the external call control profile, assign the profile to the translation pattern. (Call Routing > Translation Pattern)

Table 62: External Call Control Profile Configuration Settings

Field	Description
Name	Enter the name of the external call control profile. Valid entries include alphanumeric characters, hyphen, period, underscore, and blank spaces. The name that you enter displays in the Find and List External Call Control Profile window and in the External Call Control Profile drop-down list box in the Translation Pattern Configuration window.
Primary Web Service	Enter the URI for the primary adjunct route server, which is the adjunct route server where Cisco Unified Communications Manager sends routing queries to determine how to handle the call. You can enter http or https in this field. If you enter https, you must import a self-signed certificate from the adjunct route server, and you must export a Cisco Unified Communications Manager self-signed certificate to the adjunct route server. Enter the URI by using the following formula: `https://<hostname or IPv4 address of primary route server>:<port that is configured on primary route server>/path from route server configuration` For example, enter `https://primaryrouteserver:8443/pdp/AuthenticationEndPoint` If you use https, make sure that you enter the hostname that exists in the certificate in this field. (for example, the CN or Common Name in the certificate)

Field	Description
Secondary Web Service	Enter the URI for the redundant adjunct route server, which is the redundant adjunct route server where Cisco Unified Communications Manager sends routing queries to determine how to handle the call. The secondary web service is optional and gets used for load balancing between the primary and secondary route servers if you check the Enable Load Balancing check box. Configuring a secondary web service also ensures redundancy; that is, that an active/standby link is available. You can enter http or https in this field. If you enter https, you must import a self-signed certificate from the adjunct route server, and you must export a Cisco Unified Communications Manager self-signed certificate to the adjunct route server. If you use https, make sure that you enter the hostname that exists in the certificate in this field. Enter the URI by using the following formula: `https://<hostname or IPv4 address of secondary route server>:<port that is configured on secondary route server>/path from route server configuration` For example, enter https://secondaryrouteserver:8443/pdp/AuthenticationEndPoint If you use https, make sure that you enter the hostname that exists in the certificate in this field (for example, the CN or Common Name in the certificate)
Enable Load Balancing	If you want load balancing to occur between the primary and redundant adjunct route server, check this check box. If checked, load balancing occurs in a round robin fashion.

Field	Description
Routing Request Timer	This parameter specifies the maximum time, in milliseconds, that Cisco Unified Communications Manager should wait for the call routing directive from the adjunct route server before allowing or blocking the call, as configured in the Call Treatment on Failures setting in the external call control profile. The default is 2000; the minimum value is 1000, and the maximum value is 5000. If this field is left blank, Cisco Unified Communications Manager uses the configuration for the External Call Control Routing Request Timer service parameter, which supports the Cisco CallManager service.
Diversion Rerouting Calling Search Space	From the drop-down list box, choose the calling search space that Cisco Unified Communications Manager uses when the adjunct route server sends a divert obligation to Cisco Unified Communications Manager.
Call Treatment on Failure	From the drop-down list box, choose whether Cisco Unified Communications Manager allows or blocks calls under the following circumstances: • When the adjunct route server does not send the call routing directive to Cisco Unified Communications Manager • When Cisco Unified Communications Manager cannot contact the adjunct route server • When Cisco Unified Communications Manager fails to parse the routing directive (or supplements of the routing directive) • When Cisco Unified Communications Manager receives a 4xx or 5xx message from the adjunct route server Choosing Allow Calls routes the call to the current destination, as if the adjunct route server issued a Permit decision with Continue obligation. Choosing Block Calls causes Cisco Unified Communications Manager to clear the call, as if the adjunct route server issued a Deny decision with a Reject obligation. When failure occurs, an alarm gets logged.

Find Configuration Records for External Call Control Profiles

Cisco Unified Communications Manager supports the external call control feature, which enables an adjunct route server to make call-routing decisions for Cisco Unified Communications Manager by using the 8.0(2) Cisco Unified Routing Rules Interface. When you configure external call control, Cisco Unified Communications Manager issues a route request that contains the calling party and called party information to the adjunct route server. The adjunct route server receives the request, applies appropriate business logic, and returns a route response that instructs Cisco Unified Communications Manager on how the call should get routed, along with any additional call treatment that should get applied.

The adjunct route server can instruct Cisco Unified Communications Manager to allow, divert, or deny the call, modify calling and called party information, play announcements to callers, reset call history so adjunct voicemail and IVR servers can properly interpret calling/called party information, and log reason codes that indicate why calls were diverted or denied.

Tip Be aware that routing rules and business logic on the adjunct route server determine how the call is handled. If your configuration in Cisco Unified Communications Manager Administration conflicts with the routing rule, the routing rule gets used for the call.

To locate external call control profiles in Cisco Unified Communications Manager Administration, perform the following procedure:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Call Routing** > **External Call Control Profile**.

Step 2 The Find and List window displays. Records from an active (prior) query may also display in the window.

Step 3 To filter or search records

a) From the first drop-down list box, select a search parameter.
b) From the second drop-down list box, select a search pattern.
c) Specify the appropriate search text, if applicable.

Note To add additional search criteria, click the **+** button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the **–** button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

Step 4 To find all records in the database, ensure the dialog box is empty, click **Find.**

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

Note You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking **Delete Selected**. You can delete all configured records for this selection by clicking **Select All** and then clicking **Delete Selected**.

Step 5 From the list of records that display, click the link for the record that you want to view.

Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Configure an External Call Control Profile

External call control, which is a rules-based routing feature, requires that Cisco Unified Communications Manager send call-routing queries to an adjunct route server before routing the call. Routing rules that are set on the adjunct route server determine how the call gets handled. The adjunct route server uses the Cisco Unified Routing Rules XML interface to communicate with Cisco Unified Communications Manager. After the adjunct route server receives the query from Cisco Unified Communications Manager, the adjunct route server directs Cisco Unified Communications Manager on how to handle the call.

Tip Be aware that routing rules and business logic on the adjunct route server determine how the call is handled. If your configuration in Cisco Unified Communications Manager Administration conflicts with the routing rule, the routing rule gets used for the call.

The external call control profile provides the URIs for the adjunct route server(s), a calling search space that is used for diverting calls, a timer that indicates how long Cisco Unified Communications Manager waits for a response from the adjunct route server, and so on.

Before you begin

Before you configure the external call control profile, configure a calling search space that Cisco Unified Communications Manager uses when the adjunct route server sends a divert obligation to Cisco Unified Communications Manager.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Call Routing** > **External Call Control Profile**.

Step 2 From the Find and List window, perform one of the following tasks:

a) To copy an existing record related to external call control profiles, locate the record as described in the Find Configuration Records for External Call Control Profiles, on page 561, click the **Copy** button next to the record that you want to copy.
b) To add a new external call control profile, click the **Add New** button.
c) To update an existing external call control profile, locate the appropriate record as described in the Find Configuration Records for External Call Control Profiles, on page 561.

Step 3 Configure the appropriate fields, as described in External Call Control Profile Configuration, on page 557.

Step 4 To save the configuration information to the database, click **Save.**

What to do next

Assign the external call control profile to the translation pattern.

Assign the External Call Control Profile to the Translation Pattern

To assign the external call control profile to the translation pattern in Cisco Unified Communications Manager Administration:

Procedure

Step 1 Choose **Call Routing** > **Translation Pattern**.

Step 2 In the Translation Pattern Configuration window, choose the external call control profile that you want to assign to the pattern from the External Call Control Profile drop-down list box.

Delete Configuration Records for External Call Control Profiles

This section describes how to delete a configured external call control profile in Cisco Unified Communications Manager Administration.

Note You can delete multiple records from the Find and List window by checking the check boxes next to the appropriate records and clicking **Delete Selected**. You can delete all records in the window by clicking **Select All** and then clicking **Delete Selected**.

Before you begin

Before you can delete the external call control profile, you must unassign the profile from the translation pattern(s) that refer(s) to it. If you attempt to delete a profile that is assigned to a translation pattern, an error message displays in Cisco Unified Communications Manager Administration.

Procedure

Step 1 If you want to delete the record from the Find and List window, perform the following tasks:

a) Find the record that you want to delete by using the procedure in the Find Configuration Records for External Call Control Profiles, on page 561.
b) Click the record that you want to delete.
c) Click **Delete Selected**.

   You receive a message that asks you to confirm the deletion.

d) Click **OK.**

   The window refreshes, and the record gets deleted from the database.

Step 2 If you want to delete the record from the configuration window, perform the following tasks:

a) Find the record that you want to delete by using the procedure in the Find Configuration Records for External Call Control Profiles, on page 561.
b) Access the configuration window; click **Delete** in the configuration window.

You receive a message that asks you to confirm the deletion.

c) Click **OK.**

The window refreshes, and the record gets deleted from the database.

Import the Adjunct Route Server Certificate

If you specify https for the primary or secondary web service URIs in the external call control profile in Cisco Unified Communications Manager Administration, Cisco Unified Communications Manager uses certificates to mutually authenticate via a TLS connection to the adjunct route server(s).

To import the self-signed certificate for the adjunct route server into the Cisco Unified Communications Manager trusted store, perform the following procedure:

Procedure

Step 1 In Cisco Unified Communications Operating System, choose **Security** > **Certificate Management**.

Step 2 In the Certificate List window, click **Upload Certificate**.

Step 3 When the Upload Certificate popup window displays, choose CallManager-trust from the Certificate Name drop-down list box, and browse to the certificate for the adjunct route server; after the certificate displays in the Upload File field, click the **Upload File** button.

Step 4 Perform this procedure again if Cisco Unified Communications Manager can contact a redundant adjunct route server.

Generate a CUCM Self-Signed Certificate for Export

To ensure that the primary and redundant route servers can authenticate with Cisco Unified Communications Manager through https, you must generate a self-signed certificate that you can import to each adjunct route server that sends directives to Cisco Unified Communications Manager.

You do not need to perform this procedure if the adjunct route server uses http, as indicated in the external call control profile in Cisco Unified Communications Manager Administration.

To generate a Cisco Unified Communications Manager self-signed certificate that you can export to adjunct route server, perform the following procedure:

Procedure

Step 1 In Cisco Unified Communications Operating System, choose **Security** > **Certificate Management**.

Step 2 In the Certificate List window, click **Generate New**.

Step 3 From the Certificate Name drop-down list box, choose CallManager; then, click **Generate New**.

Step 4 From the Find and List Certificates window, click the CallManager.pem certificate that you just created.

Step 5 After the certificate file data displays, click Download to download the certificate to a location that you can use for exporting the certificate to the adjunct route server.

Step 6 Export the certificate to each adjunct route server that sends directives.

Step 7 Perform this task for each node in the Cisco Unified Communications Manager cluster that can contact the primary and redundant adjunct route server.

Provide Information to Users

Because limitations and restrictions exist for chaperones, notify users that you designated as chaperones.

Troubleshooting External Call Control

For information on troubleshooting external call control, see the *Troubleshooting Guide for Cisco Unified Communications Manager*.

CHAPTER 24

External Call Transfer Restrictions

This chapter provides information about External Call Transfer Restrictions feature which allows you 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.

Configure External Call Transfer Restrictions

The External Call Transfer Restrictions feature allows you 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.

Perform the following steps to configure external call transfer restrictions.

Procedure

Step 1 To block external calls from being transferred to external devices, perform the following steps:

a) Set the Block OffNet to OffNet Transfer clusterwide service parameter to True.

b) For incoming calls, configure individual gateways or trunks as OffNet.

c) For outgoing calls, configure route pattern Call Classification field as OffNet. The Allow Device Override check box can be checked or unchecked, depending on the requirements (for example, if the check box is checked, the setting on the associated gateway or trunk is considered; if it is unchecked, the call classification value of the route pattern classifies the call).

Step 2 To configure all gateways or trunks to be OffNet (external) or OnNet (internal), perform the following steps:

a) Set the Cisco Unified Communications Manager clusterwide service parameter Call Classification to OffNet (if all gateways and trunks are to be external) or OnNet (if all gateways and trunks are to be internal).

b) Configure individual gateways or trunks to Use System Default in the Call Classification field.

Step 3 On the Route Pattern Configuration window, set the Call Classification field as OffNet. The Allow Device Override check box can be checked or unchecked, depending on the requirements and the configurations of the gateway or trunk.

Related Topics

Set the Block OffNet to OffNet Transfer Service Parameter, on page 572
Configure Transfer Capabilities with Gateway Configuration, on page 573
Configure Transfer Capabilities with Trunk Configuration, on page 573
Configure Transfer Capabilities with Call Classification Service Parameter, on page 572

External Call Transfer Restrictions Feature

External call transfer restrictions block call transfer between external parties. Setting service parameters and configuring gateways, trunks, and route patterns as OffNet (external) devices provide external call transfer blocking. This feature provides an OnNet or OffNet alerting tone to the terminating end of the call (determined by the configuration of the device as either OnNet or OffNet, respectively). This chapter uses the following terms:

- 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.
- 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.

Gateways and Trunks

You can configure gateways and trunks as OnNet (internal) or OffNet (external) by using Gateway Configuration or Trunk Configuration or by setting a clusterwide service parameter. 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 or trunk.

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

- Intercluster trunk
- SIP trunk

Route Patterns

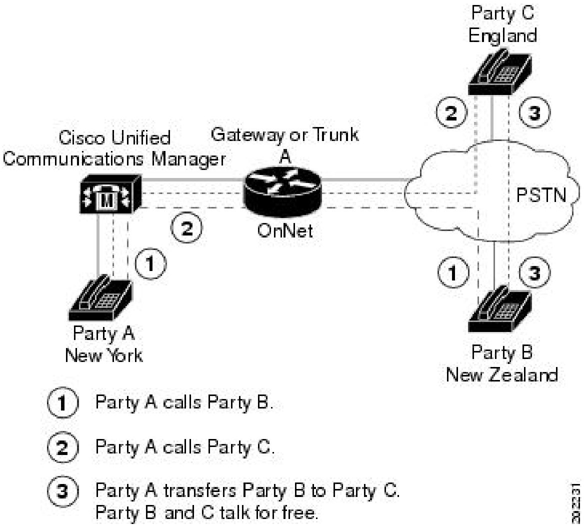
To classify a call as OnNet or OffNet, administrators can set the Call Classification field to OnNet or OffNet, respectively, on the Route Pattern Configuration window. Administrators can override the route pattern setting and use the trunk or gateway setting by checking the Allow Device Override check box on the Route Pattern Configuration window.

For more information, see the Configure External Call Transfer Restrictions, on page 572.

Example

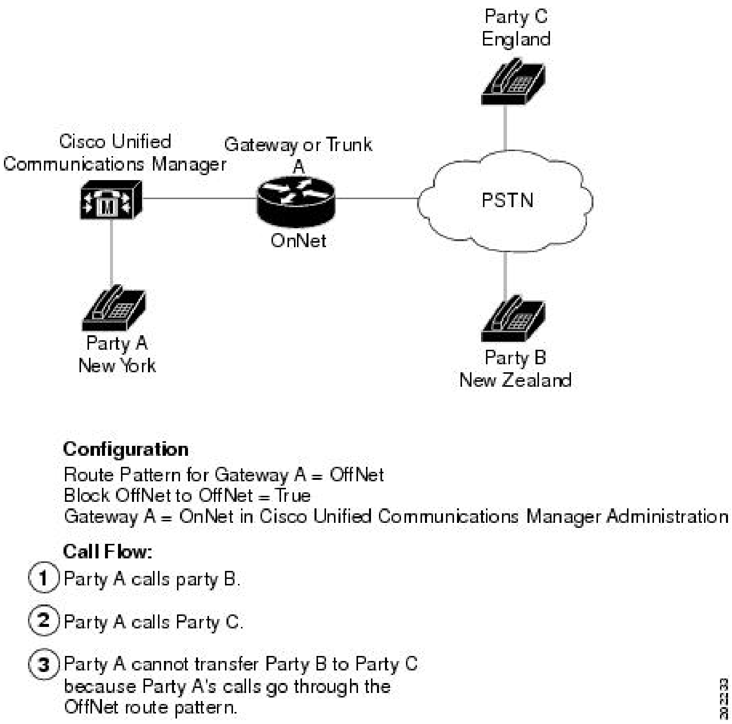
The following example illustrates how callers use transfer to avoid paying for long-distance calls. In the following figure, Party A from ABC Company in New York calls Party B, a friend in New Zealand. After the call connects, Party A transfers the call to Party C, another friend who lives in England. When transfer completes, Party B and Party C are connected, and Party A gets disconnected. As a result, ABC Company gets billed for the call between New Zealand and England.

Figure 52: Transferring External Calls to an External Party



In the following figure, the system prevents transferring an external call to an external party because, regardless of how the gateway or trunk is configured, the route pattern was configured as OffNet, and the service parameter Block OffNet to OffNet Transfer is set to True.

Figure 53: Blocking an External Call from Transferring to an External Party



Configuration

Route Pattern for Gateway A = OffNet
Block OffNet to OffNet = True
Gateway A = OnNet in Cisco Unified Communications Manager Administration

Call Flow:

1. Party A calls party B.
2. Party A calls Party C.
3. Party A cannot transfer Party B to Party C because Party A's calls go through the OffNet route pattern.

System Requirements for External Call Transfer Restrictions

The external call transfer restriction requires the following software component to operate:

- Cisco Unified Communications Manager 5.0 or later

External Call Transfer Interactions and Restrictions

Interactions

The following sections describe how external call transfer restrictions feature interacts with Cisco Unified Communications Manager applications and call processing.

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 *Cisco Unified Communications Manager System Guide*.

Bulk Administration

Bulk Administration inserts gateway configuration (OffNet or OnNet) on the Gateway Template. See the *Cisco Unified Communications Manager Bulk Administration Guide* for more information.

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. See the *Cisco Unified Communications Manager Dialed Number Analyzer Guide* for more information.

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.
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).

Install and Activate External Call Transfer Restrictions

To activate external call transfer restrictions, perform the following steps:

Procedure

Step 1 Set the Block OffNet to OffNet Transfer service parameter to True.

Step 2 In Route Pattern Configuration window, set the Call Classification field to OffNet. Leave the Allow Device Override check box unchecked, so the device uses the Call Classification setting of the route pattern.

Step 3 Configure the trunks and gateways that you want to be identified as OffNet.

What to do next

See the Configure External Call Transfer Restrictions Service Parameters, on page 572 for details.

Configure External Call Transfer Restrictions

This section contains the following information:

Tip Before you configure external call transfer restrictions, review the Configure External Call Transfer Restrictions, on page 567.

Configure External Call Transfer Restrictions Service Parameters

This section provides information to configure external call transfer restrictions service parameters. You can set two service parameters for the external call transfer restrictions feature: Call Classification and Block OffNet to OffNet Transfer.

Configure Transfer Capabilities with Call Classification 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 two steps:

Procedure

Step 1 Using the Cisco Unified Communications Manager clusterwide service parameter Call Classification, choose either OffNet or OnNet (the default specifies OffNet).

Step 2 In the Call Classification field on the Gateway Configuration and Trunk Configuration windows, configure each gateway and trunk to Use System Default (this reads the setting in the Call Classification service parameter and uses that setting for the gateway and trunk).

Set the Block OffNet to OffNet Transfer Service Parameter

The Cisco Unified Communications Manager clusterwide service parameter Block OffNet to OffNet Transfer allows administrators to prevent users from transferring external calls to another external number. This parameter specifies values as True or False. Setting the parameter to True blocks external calls from being transferred to another external device. The default value specifies False. You modify the Block OffNet to OffNet Transfer service parameter by using the Service Parameter Configuration window.

When a user tries 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.

Configure Transfer Capabilities with Gateway Configuration

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.

Procedure

Step 1 From Cisco Unified Communications Manager 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 Cisco 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 the setting.

Step 5 Click **Save**.

Configure Transfer Capabilities with Trunk Configuration

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.

Procedure

Step 1 From Cisco Unified Communications Manager 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 Cisco Unified Communications Manager display.

Step 3 Choose the trunk that you want to configure as OffNet or OnNet.

Step 4 In the Call Classification field, choose the setting.

Step 5 Click **Save.**

Table 63: Call Classification Configuration Settings

Setting Name	Description
OffNet	This setting 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.

Setting Name	Description
OnNet	This setting identifies the gateway as an internal gateway. When a call comes in from a gateway that is configured as OnNet, the system sends inside ring to the destination device.
Use System Default	This setting uses the Cisco Unified Communications Manager clusterwide service parameter Call Classification.

Configure Transfer Capabilities with Route Pattern Configuration

The Route Pattern Configuration window provides the following fields:

- Call Classification - Use this drop-down list box to classify the call that uses this route Pattern as OffNet or OnNet.
- Provide Outside Dial Tone - If Call Classification is set to OffNet, this check box gets checked.
- 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.

CHAPTER 25

Geolocations and Location Conveyance

This chapter provides information about the following concepts:

- Geolocations
- Geolocation filters
- Location conveyance

Tip Do not confuse locations with geolocations. Locations, which you configure by using the **System** > **Location** menu option, allow you to define entities that a centralized call-processing system uses to provide call admission control (CAC). Geolocations, which you configure by using the **System** > **Geolocation Configuration** menu option, allow you to specify geographic locations that you use to associate Cisco Unified Communications Manager devices for features such as logical partitioning.

Configure Geolocations

Geographical location information, or geolocation, describes a physical position in the world that may correspond to the past, present, or future location of a person, event, or device.

Cisco Unified Communications Manager Administration allows you to specify a geolocation for every device.

The Request for Comments (RFC) 4119 standard provides the basis for geolocations. Geolocations use the civic location format that specifies the following fields: country, A1, A2, A3, A4, A5, A6, PRD, POD, STS, HNO, HNS, LMK, LOC, FLR, NAM, and PC.

In Cisco Unified Communications Manager Administration, geolocations get configured manually.

Tip Do not confuse locations with geolocations. Locations, which you configure by using the **System** > **Location** menu option, allow you to define entities that a centralized call-processing system uses to provide call admission control (CAC). Geolocations, which you configure by using the **System** > **Geolocation Configuration** menu option, allow you to specify geographic locations that you use to associate Cisco Unified Communications Manager devices for features such as logical partitioning.

Perform the following steps to configure geolocations.

Procedure

Step 1 Define a set of geolocations on a new Geolocation Configuration window.

Step 2 Assign geolocations to device pools, devices, trunks, gateways, or MGCP ports.

Step 3 Assign geolocations to the default geolocation that the Default Geolocation enterprise parameter specifies.

Step 4 For devices that do not participate in features that require geolocations, define the geolocation as Unspecified or leave undefined.

Note You can define this lack of association at the individual-device level, the device-pool level, or the enterprise-parameter level.

Related Topics

Geolocation Configuration, on page 582

Enterprise Parameters for Logical Partitioning, on page 802

Configure Geolocation Filters

Cisco Unified Communications Manager administrators define a geolocation filter for every device that participates in a feature that uses geolocation filters. Geolocation filters allow selection of specific fields from the 17 geolocation fields for the purpose of creating an identifier from the selected fields. Geolocation filters get configured manually.

Cisco Unified Communications Manager administrators then assign geolocation filters to devices.

Use the **System** > **Geolocation Filter** menu option in Cisco Unified Communications Manager Administration to configure geolocation filters.

Perform the following steps to configure geolocation filters.

Procedure

Step 1 Define a set of filter rules in a new Geolocation Filter Configuration window.

Step 2 Assign geolocation filters to device pools, trunks, intercluster trunks, gateways, or MGCP ports.

Step 3 For the logical partitioning feature, assign geolocation filter to the default filter that the Logical Partitioning Default Filter enterprise parameter specifies.

Related Topics

Geolocation Filter Configuration, on page 588
Enterprise Parameters for Logical Partitioning, on page 802

Configure Location Conveyance

Location conveyance involves configuration to make the following behavior possible:

- Communicate geolocation information across clusters
  - Allow communication of geolocation information from one cluster to another, at call establishment as well as midcall joins and redirects.

Note Enterprise parameters and logical partitioning configuration do not control location conveyance. If a device that communicates through a trunk associates with geolocation information, check the Send Geolocation Information check box when you configure the trunk (either SIP or ICT) to convey the geolocation information across clusters.

Note For the logical partitioning feature in the current release, the Cisco Unified Communications Manager does not send the configured geolocation information to line devices (phones that are running SIP or SCCP).

Perform the following steps to configure location conveyance in a multicluster logical partitioning environment.

Procedure

Step 1 Define a set of geolocations in a new Geolocation Configuration window.

Step 2 Assign geolocations to device pools, devices, SIP trunks, intercluster trunks, gateways, or MGCP ports for the devices that need to participate in location conveyance.

Step 3 Assign geolocations to a default geolocation that the Default Geolocation enterprise parameter specifies.

This assignment allows you to specify a default geolocation for a cluster. For devices for which no associated geolocation exists at the device or device-pool level, the value that is specified by the Default Geolocation enterprise parameter applies.

Step 4 If geolocation information about devices needs to be communicated across clusters, ensure that location conveyance is configured. To do so, check the Send Geolocation Information check box in the intercluster trunk (ICT) or SIP trunk for the devices that need to pass geolocation information across clusters as follows:

- Check the Send Geolocation Information check box in the intercluster trunk (ICT) or SIP trunk of the local cluster.

- Check the Send Geolocation Information check box in the ICT or SIP trunk of the remote cluster.

Related Topics

Geolocation Configuration, on page 582
Enterprise Parameters for Logical Partitioning, on page 802

Geolocations Feature

Geographical location information, or geolocation, describes a physical position in the world that may correspond to the past, present, or future location of a person, event, or device.

Cisco Unified Communications Manager Administration allows you to specify a geolocation for every device.

The Request for Comments (RFC) 4119 standard provides the basis for geolocations. Geolocations use the civic location format that specifies the following fields: country, A1, A2, A3, A4, A5, A6, PRD, POD, STS, HNO, HNS, LMK, LOC, FLR, NAM, and PC.

In Cisco Unified Communications Manager Administration, geolocations get configured manually.

Tip Do not confuse locations with geolocations. Locations, which you configure by using the **System** > **Location** menu option, allow you to define entities that a centralized call-processing system uses to provide call admission control (CAC). Geolocations, which you configure by using the **System** > **Geolocation Configuration** menu option, allow you to specify geographic locations that you use to associate Cisco Unified Communications Manager devices for features such as logical partitioning.

Overview of Geolocations

Configuration of geolocations entails provisioning the following elements:

- Configure geolocation identifiers
  - You can define sets of geolocations (civic addresses).
  - You can assign these geolocations to VoIP phones, VoIP gateways, IP trunks, device pools, and enterprise parameters.
  - You can define geolocation filters that select a subset of fields from geolocation and associate with VoIP gateways, IP trunks, device pools, and enterprise parameters.

Geolocation Characteristics

Cisco Unified Communications Manager administrators must define the following item:

- A geolocation for every device that participates in any feature that requires geolocations. The Request for Comments (RFC) 4119 standard provides the basis for geolocations. Geolocations use the civic location format that specifies the following fields: country, A1, A2, A3, A4, A5, A6, PRD, POD, STS, HNO, HNS, LMK, LOC, FLR, NAM, and PC. Geolocations get configured manually.

Cisco Unified Communications Manager administrators then assign geolocations to devices.

The following entities in a Cisco Unified Communications Manager system can have geolocation and geolocation filter values that are assigned:

- Device pools
- CTI route points
- Phones (optional)
- CTI ports

Note Phones do not specify a drop-down list box for associating a phone with a geolocation filter.

- SIP trunks
- Intercluster trunks (ICT)
- H.323 gateways
- MGCP ports of the following types: T1, E1, PRI, FXO

You do not need to associate media devices, such as media termination points (MTP), conference bridges (CFB), annunciators, and music on hold (MOH) servers, with geolocations.

Internally, the device layer of Cisco Unified Communications Manager associates with geolocation values that call processing uses. The following sequence takes place:

1. Devices read the GeolocationPkid and GeolocationFilterPkid for its configuration at device or device pool level.
2. The devices communicate this Pkid and deviceType information in CC (for example, CcRegisterPartyA) and PolicyAndRSVPRegisterReq messages during call signaling.
3. The intercluster trunk (ICT) or SIP trunk device layer that receives this information uses the information for location conveyance.
4. No communication of geolocation from Cisco Unified Communications Manager to a phone takes place.

Source of Geolocation Information

The following logic determines the geolocation value:

1. Read the value for geolocation from the device window. If it is not configured on device page, for phone device in roaming, read the device pool (DP) from the roaming configuration. For phone device that is not in roaming, read the DP from the device configuration.
2. For trunk, ICT, or MGCP port device, read the DP from the device configuration.
3. From the selected DP, read the value of geolocation from DP configuration window.
4. If DP is not configured with a value for Geolocation, use blank value.
5. If available geolocation value is blank, call processing uses the configured value that the Default Geolocation enterprise parameter specifies.

The standard record for a geolocation specifies Unspecified. Use this value when no geolocation needs to associate with a device. In such scenarios, any features that are based on geolocations do not execute. Also, devices for which no geolocation gets specified do not participate in geolocation information conveyance across clusters for intercluster calls.

Be aware that the Default Geolocation enterprise parameter can be configured from drop-down list boxes on the Enterprise Parameters Configuration window.

Geolocation Usage for Shared Lines and Route Lists

When the called party specifies a group device, a different geolocation can apply for each device in a group. For the early attended scenarios, you do not know the actual connected device until the device gets answered. Thus, the Geolocation information gets aggregated until the device answers.

- The Call Control and Feature layer receives temporary geolocation information (“MixedDevice”) until the device answers.
- When a device answers, the actual geolocation information for the device becomes available and gets communicated to call control and to any features that are involved.

Geolocation Examples

The following table specifies examples of geolocations.

Table 64: Geolocation Examples

Geolocation Name	Geolocation Data
IN-KA-BLR-BLD1	(country=IN, A1=KA, A3=Bangalore, A4= A4, A5=12, A6=Langford Road, PRD=12, LOC=BLD1, NAM=unified comm, PC=560001)
IN-KA-BLR-BLD2	(country=IN, A1=KA, A3=Bangalore, A4= A4, A6=Outer Ring Road, LOC=BLD2, NAM=unified comm, PC=560002)
IN-MH-MUM-BLD1	(country=IN, A1=MH, A3=Mumbai, A4= A4, LOC=bld1, NAM=unified comm, PC=220001)
IN-KA-BLR-ICTtoSJ	(country=IN, A1=KA, A3=Bangalore, NAM=ICTToSJ)

Geolocation Identifiers

Geolocation identifiers get constructed from a combination of geolocations, geolocation filters, and device types of Cisco Unified Communications Manager devices.

See the following sections for detailed descriptions of geolocations and geolocation filters:

- Geolocations Feature, on page 578
- Geolocation Filters Feature, on page 588

Geolocation filters allow selection of specific fields from the 17 geolocation fields. Use the **System** > **Geolocation Filter** menu option in Cisco Unified Communications Manager Administration to configure geolocation filters manually. Specific Cisco Unified Communications Manager features associate the geolocation filters by using drop-down list boxes in the configuration windows of the devices that get configured for a particular feature.

The Cisco Unified Communications Manager device type of a device specifies one of the following values:

- Border - Use this value to specify accessing PSTN trunks, intercluster trunks (ICTs), gateways, and MGCP ports.
- Interior - Use this value for VoIP phones or internal endpoints.

See Logical Partitioning Feature, on page 796 for a detailed listing of the Cisco Unified Communications Manager devices that associate with the Border and Interior device types.

The following object specifies an example geolocation identifier:

{geolocPkid=9dc76052-3a37-78c2-639a-1c02e8f5d3a2, filterPkid=d5bdda76-6a86-56c5-b5fd-6dff82b37493, geolocVal=, devType=8}

where:

The geolocVal field gets used in cases where the Cisco Unified Communications Manager database does not reference the geolocation record but data for a geolocation comes from another source (for example, location conveyance PIDF-LO XML from a remote cluster).

In such cases, Cisco Unified Communications Manager constructs the name value pair for the geolocation fields.

Example: “country=US:A1=Texas:A3=Richardson:LOC=Building 6” where the value gets communicated through the geolocVal field.

Note In such a case, the geolocPkid is kept null and call control or features access the geolocVal field from a geolocation identifier.

The following string specifies the logical representation of a geolocation identifier:

“Border:country=US:A1=Texas:A3=Richardson:LOC=Building 6”

Note This geolocation identifier gets constructed from the member fields of a geolocation identifier.

Geolocation Interactions

The following interaction applies to geolocations:

- Location conveyance

See the Location Conveyance Feature, on page 592 for a detailed discussion of location conveyance.

Geolocation Configuration

Use the **System** > **Geolocation Configuration** menu option in Cisco Unified Communications Manager Administration to configure geolocations.

Tip Do not confuse locations with geolocations. Locations, which you configure by using the **System** > **Location** menu option, allow you to define entities that a centralized call-processing system uses to provide call admission control (CAC). Geolocations, which you configure by using the **System** > **Geolocation Configuration** menu option, allow you to specify geographic locations that you use to associate Cisco Unified Communications Manager devices for features such as logical partitioning.

Tip Before you configure geolocations, review the configuration summary task for geolocations and topics related to configuring geolocation filters.

Related Topics

Configure Geolocations, on page 575

Configure Geolocation Filters, on page 576

Find a Geolocation

Because you might have multiple geolocations in your network, Cisco Unified Communications Manager lets you search for geolocations on the basis of specified criteria. Follow these steps to search for a specific geolocations in the Cisco Unified Communications Manager database.

Note During your work in a browser session, Cisco Unified Communications Manager Administration retains your geolocation search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your geolocation search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **System** > **Geolocation Configuration**.

The Find and List Geolocations window displays. Records from an active (prior) query may also display in the window.

Step 2 To filter or search records

a) From the first drop-down list box, choose a search parameter.

b) From the second drop-down list box, choose a search pattern.

c) Specify the appropriate search text, if applicable.

Note To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

Step 3 To find all records in the database, ensure the dialog box is empty, click **Find.**

All matching records display. You can change the number of items that display by choosing a different value from the Rows per Page drop-down list box.

Note You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking **Delete Selected**. You can delete all configurable records for this selection by clicking **Select All** and then clicking **Delete Selected**.

Step 4 From the list of records that display, click the link for the record that you want to view.

Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Configure a Geolocation

Perform the following procedure to add or update a geolocation.

Procedure

Step 1 Choose **System** > **Geolocation Configuration**.

The Find and List Geolocations window displays.

Step 2 Perform one of the following tasks:

a) To add a new geolocation, click **Add New**.

The Geolocation Configuration window displays.

b) To update a geolocation, locate a specific geolocation as described in the Find a Geolocation, on page 582.

Step 3 Enter the appropriate settings as described in Geolocation Configuration, on page 584.

Step 4 Click **Save.**

If you added a geolocation, the list box at the bottom of the window now includes the new geolocation.

Delete a Geolocation

Perform the following procedure to delete an existing geolocation.

Procedure

Step 1 Choose **System** > **Geolocation Configuration**.

The Find and List Geolocations window displays.

Step 2 To locate a specific geolocation, enter search criteria and click **Find.**

A list of geolocations that match the search criteria displays.

Step 3 Perform one of the following actions:

a) Check the check boxes next to the geolocations that you want to delete and click **Delete Selected**.
b) Delete all geolocations in the window by clicking **Select All** and then clicking **Delete Selected**.
c) From the list, choose the name of the geolocation that you want to delete and click **Delete.**

A confirmation dialog displays.

Step 4 Click **OK.**

The specified geolocation gets deleted.

Geolocation Configuration

Geographical location information, or geolocation, describes a physical position in the world that may correspond to the past, present, or future location of a person, event, or device. In Cisco Unified Communications Manager Administration, geolocations get configured manually. Cisco Unified Communications Manager Administration allows you to specify a geolocation for every device.

Tip Do not confuse locations with geolocations. Locations, which you configure by using the **System** > **Location** menu option, allow you to define entities that a centralized call-processing system uses to provide call admission control (CAC). Geolocations, which you configure by using the **System** > **Geolocation Configuration** menu option, allow you to specify geographic locations that you use to associate Cisco Unified Communications Manager devices for features such as logical partitioning.

The following table describes the configuration settings that are used for configuring geolocations.

Table 65: Geolocation Configuration Settings

Field	Description
Geolocation Configuration	
Name	Enter a unique name for this geolocation. The name can contain up to 50 ASCII characters. You can use all characters except quotes (“), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).

Field	Description
Description	Enter a description for this geolocation. This field can contain up to 50 ASCII or unicode characters. Default value specifies blank.
Country using the two-letter abbreviation	Enter the two-letter country abbreviation for the country where this geolocation is located. Use the ISO 3166 code. The country must comprise two ASCII characters. Default value specifies blank. Example: US for United States, IN for India
State, Region, or Province (A1)	Enter a national subdivision for this geolocation, such as a state, region, province, or prefecture. This field can contain up to 50 ASCII or unicode characters. Default value specifies blank. Example: Texas, Karnataka, Maharashtra
County or Parish (A2)	Enter a county, parish, gun (JP), or district (IN) for this geolocation. This field can contain up to 50 ASCII or unicode characters. Default value specifies blank. Example: Tarrant, Harris, Plaquemines
City or Township (A3)	Enter a city, township, or shi (JP) for this geolocation. This field can contain up to 50 ASCII or unicode characters. Default value specifies blank. Example: Bangalore, New Delhi, Mumbai, Dallas, Tokyo, Sydney
Borough or City District (A4)	Enter a city division, borough, city district, ward, or chou (JP) for this geolocation. This field can contain up to 50 ASCII or unicode characters. Default value specifies blank. Example: Manhattan, Brooklyn, Westminster, Hollywood

Field	Description
Neighborhood (A5)	Enter a neighborhood or block for this geolocation. This field can contain up to 50 ASCII or unicode characters. Default value specifies blank. Example: Midtown, Soho, Southbank
Street (A6)	Enter a street for this geolocation. This field can contain up to 50 ASCII or unicode characters. Default value specifies blank. Example: Main, Commerce, Champs-Elysees, Broadway
Leading Street Direction, such as N or W (PRD)	Enter a leading street direction for this geolocation. This field can contain up to 10 ASCII or unicode characters. Default value specifies blank. Example: N, S, E, W (as in 43 N Wabash Avenue)
Trailing Street Suffix, such as SW (POD)	Enter a trailing street suffix for this geolocation. This field can contain up to 10 ASCII or unicode characters. Default value specifies blank. Example: SW, NE, NW, SE (as in 245 E 45th St NW)
Address Suffix, such as Avenue, Platz (STS)	Enter an address suffix for this geolocation. This field can contain up to 50 ASCII or unicode characters. Default value specifies blank. Example: Avenue, Boulevard, Platz, rue
Numeric house number (HNO)	Enter a numeric house number for this geolocation. This field can contain up to 10 numeric characters. Default value specifies blank. Example: 2666, 14, 12345

Field	Description
House Number Suffix, such as A, 1/2 (HNS)	Enter a house number suffix for this geolocation. This field can contain up to 20 ASCII or unicode characters. Default value specifies blank. Example: A, 1/2, bis
Landmark (LMK)	Enter a landmark or vanity address for this geolocation. This field can contain up to 50 ASCII or unicode characters. Default value specifies blank. Example: Central Library
Additional Location Information, such as Room Number (LOC)	Enter additional location information, such as a room number, for this geolocation. This field can contain up to 50 ASCII or unicode characters. Default value specifies blank. Example: Room 222, Suite 555
Floor (FLR)	Enter a floor for this geolocation. This field can contain up to 10 ASCII characters. Default value specifies blank. Example: 23, 2nd
Name of Business or Resident (NAM)	Enter a business name or resident name or office occupant for this geolocation. This field can contain up to 50 ASCII or unicode characters. Default value specifies blank. Example: Cisco Systems, Joe’s Barbershop
Zip or Postal Code (PC)	Enter a zip code or postal code for this geolocation. This field can contain up to 20 ASCII or unicode characters. Default value specifies blank. Example: 75042-0401, SW1V 1RP

Geolocation Filters Feature

Cisco Unified Communications Manager administrators define the following item:

- A geolocation filter for every device that participates in a feature that uses geolocation filters. Filters allow selection of specific fields from the 17 geolocation fields for the purpose of creating an identifier from the selected fields. Geolocation filters get configured manually.

Cisco Unified Communications Manager administrators then assign geolocation filters to devices.

The following logic determines the geolocation filter value:

1. For phone device that is in roaming, read the geolocation filter value from DP in roaming configuration. For phone device that is not in roaming, read the geolocation filter value from DP in device configuration.
2. For trunk, intercluster trunk, or MGCP port device, read geolocation filter value from device window. If no value is configured, read from DP.
3. If DP is not configured with a geolocation filter value, use blank value.
4. If available filter is blank, call processing uses the value that the Default Geolocation Filter enterprise parameter specifies.

Geolocation Filter Examples

The following table specifies examples of geolocation filters.

Table 66: Geolocation Filter Examples

Geolocation Name	Geolocation Filter Data
India-Filter1	(UseCountry, UseA1, UseA3, UseLOC)
India-GW-Filter2	(UseCountry, UseA1, UseA3, UseLOC, UseNAM)
India-ICT-Trunk-Filter3	(UseCountry, UseA1, UseA3, UseNAM)

Geolocation Filter Configuration

Tip Before you configure geolocations filters, review the Configure Geolocation Filters, on page 576.

Use the **System** > **Geolocation Filter** menu option in Cisco Unified Communications Manager Administration to configure geolocation filters.

Find a Geolocation Filter

Because you might have multiple geolocation filters in your network, Cisco Unified Communications Manager lets you search for geolocation filters on the basis of specified criteria. Follow these steps to search for a specific geolocation filters in the Cisco Unified Communications Manager database.

Note During your work in a browser session, Cisco Unified Communications Manager Administration retains your geolocation filter search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your geolocation filter search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **System** > **Geolocation Filter**.

The Find and List Geolocation Filters window displays. Records from an active (prior) query may also display in the window.

Step 2 To filter or search records

a) From the first drop-down list box, choose a search parameter.
b) From the second drop-down list box, choose a search pattern.
c) Specify the appropriate search text, if applicable.

Note To add additional search criteria, click the **+** button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the **–** button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

Step 3 To find all records in the database, ensure the dialog box is empty, click **Find.**

All matching records display. You can change the number of items that display by choosing a different value from the Rows per Page drop-down list box.

Note You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking **Delete Selected**. You can delete all configurable records for this selection by clicking **Select All** and then clicking **Delete Selected**.

Step 4 From the list of records that display, click the link for the record that you want to view.

Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Configure a Geolocation Filter

Perform the following procedure to add or update a geolocation filter.

Procedure

Step 1 Choose **System** > **Geolocation Filter**.

The Find and List Geolocation Filters window displays.

Step 2 Perform one of the following tasks:

a) To add a new geolocation filter, click **Add New**.

   The Geolocation Filter Configuration window displays.

b) To update a geolocation filter, locate a specific geolocation filter as described in the Find a Geolocation Filter, on page 589.

Step 3 Enter the appropriate settings as described in Geolocation Filter Configuration, on page 590.

Step 4 Click **Save.**

If you added a geolocation filter, the list box at the bottom of the window now includes the new geolocation filter.

Delete a Geolocation Filter

Perform the following procedure to delete an existing geolocation filter.

Procedure

Step 1 Choose **System** > **Geolocation Filter**.

The Find and List Geolocation Filters window displays.

Step 2 To locate a specific geolocation filter, enter search criteria and click **Find.**

A list of geolocation filters that match the search criteria displays.

Step 3 perform one of the following actions:

a) Check the check boxes next to the geolocation filters that you want to delete and click **Delete Selected**.
b) Delete all geolocation filters in the window by clicking **Select All** and then clicking **Delete Selected**.
c) From the list, choose the name of the geolocation filter that you want to delete and click **Delete.**

   A confirmation dialog displays.

Step 4 Click **OK.**

The specified geolocation filter gets deleted.

Geolocation Filter Configuration

Cisco Unified Communications Manager administrators define the following item:

- A geolocation filter for every device that participates in a feature that uses geolocation filters. Filters allow selection of specific fields from the 17 geolocation fields for the purpose of creating an identifier from the selected fields. Geolocation filters get configured manually.

Cisco Unified Communications Manager administrators then assign geolocation filters to devices.

The following table describes the configuration settings that are used for configuring geolocation filters.

Table 67: Geolocation Filter Configuration Settings

Field	Description
Geolocation Filter Configuration	
Name	Enter a unique name for this geolocation filter. Default name cannot be blank. This field can contain up to 50 ASCII characters. You can use all characters except quotes (“), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).
Description	Enter a description for this geolocation filter. This field can contain up to 50 ASCII or unicode characters. Default value specifies blank.
Country using the two-letter abbreviation	Check this box to use the Country field of a specified geolocation to create this geolocation filter.
State, Region, or Province (A1)	Check this box to use the State, Region, or Province (A1) field of a specified geolocation to create this geolocation filter.
County or Parish (A2)	Check this box to use the County or Parish (A2) field of a specified geolocation to create this geolocation filter.
City or Township (A3)	Check this box to use the City or Township (A3) field of a specified geolocation to create this geolocation filter.
Borough or City District (A4)	Check this box to use the Borough or City District (A4) field of a specified geolocation to create this geolocation filter.
Neighborhood (A5)	Check this box to use the Neighborhood (A5) field of a specified geolocation to create this geolocation filter.
Street (A6)	Check this box to use the Street (A6) field of a specified geolocation to create this geolocation filter.

Field	Description
Leading Street Direction, such as N or W (PRD)	Check this box to use the Leading Street Direction, such as N or W (PRD) field of a specified geolocation to create this geolocation filter.
Trailing Street Suffix, such as SW (POD)	Check this box to use the Trailing Street Suffix, such as SW (POD) field of a specified geolocation to create this geolocation filter.
Address Suffix, such as Avenue, Platz (STS)	Check this box to use the Address Suffix, such as Avenue, Platz (STS) field of a specified geolocation to create this geolocation filter.
Numeric house number (HNO)	Check this box to use the Numeric house number (HNO) field of a specified geolocation to create this geolocation filter.
House Number Suffix, such as A, 1/2 (HNS)	Check this box to use the House Number Suffix, such as A, 1/2 (HNS) field of a specified geolocation to create this geolocation filter.
Landmark (LMK)	Check this box to use the Landmark (LMK) field of a specified geolocation to create this geolocation filter.
Additional Location Information, such as Room Number (LOC)	Check this box to use the Additional Location Information, such as Room Number (LOC) field of a specified geolocation to create this geolocation filter.
Floor (FLR)	Check this box to use the Floor (FLR) field of a specified geolocation to create this geolocation filter.
Name of Business or Resident (NAM)	Check this box to use the Name of Business or Resident (NAM) field of a specified geolocation to create this geolocation filter.
Zip or Postal Code (PC)	Check this box to use the Zip or Postal Code (PC) field of a specified geolocation to create this geolocation filter.

Location Conveyance Feature

Location conveyance involves configuration to make the following behavior possible:

- Communicate geolocation information across clusters
    - Allow communication of geolocation information from one cluster to another, at call establishment as well as midcall joins and redirects.

Note Enterprise parameters and logical partitioning configuration do not control location conveyance. If a device that communicates through a trunk associates with geolocation information, check the Send Geolocation Information check box when you configure the trunk (either SIP or ICT) to convey the geolocation information across clusters.

Note For the logical partitioning feature in the current release, the Cisco Unified Communications Manager does not send the configured geolocation information to line devices (phones that are running SIP or SCCP).

Geolocation Conveyance Across SIP Trunks and Intercluster Trunks

Geolocation conveyance entails the following characteristics:

- Geolocation gets sent from one cluster to another.
- Geolocation information gets sent both at call establishment and at midcall joins and redirects.

The SIP trunk supports the location conveyance of Presence Information Data Format Location Object (PIDF-LO) as RFC 4119 describes, which specifies an encapsulation of location information within a presence document:

- Location conveyance supports the subset of SIP extension as specified in Location Conveyance draft-ietf-sip-location-conveyance-10.
- For communicating indication of device type, use User Agent Capability Presence Status, as specified in SIP extension draft-ietf-simple-prescaps-ext-08.
- Location conveyance supports the PIDF-LO in the <device> element as specified in SIP extension draft-ietf-geopriv-pdif-lo-profile-11.
- INVITE and UPDATE requests carry the PIDF-LO XML.
- Geolocation fields support ASCII and unicode characters.

Intercluster trunk also supports location conveyance that is using PIDF-LO XML with reduction in some of the XML elements:

- Elements include Setup, Alert, Progress, Connect, and Notify requests.
- Geolocation fields support ASCII characters.

The SIP trunk or intercluster trunk uses the geolocation information and device type that the call control messages send to construct the PIDF-LO XML.

SIP Trunk Error Handling for Geolocation Information

Incoming requests that carry geolocation information for location conveyance get checked for compliance as follows:

1. Geolocation headers indicate inclusion of PIDF-LO, but message body does not carry PIDF-LO.

2. Geolocation header has a CID header that refers to a URI for which no corresponding Content-ID header with the same URI exists.
3. Geolocation header has a URI other than CID header (for example, SIP or SIPS URI for LbyR).

The SIP trunk that receives a noncompliant SIP request responds with a “424 Bad Location Information” response.

The following cases result in ignoring the processing of geolocation info. For information purposes, the SIP trunk sends a Geolocation-Error header in the next outgoing SIP response (for example, 180 or 200).

- PIDF-LO lacks mandatory elements, such as “geopriv,” “location-info,” “civicAddress,” or “usage-rules.”
- If usage-rules show a retention-expiry time that already elapsed when it is compared to the current time in GMT, processing gets ignored.

Because the received geolocation information gets ignored, the SIP trunk continues to use the locally configured geolocation information on the SIP trunk.

Intercluster Trunk Error Handling for Geolocation Information

If an error occurs while the received geolocation information on an intercluster trunk is being processed, locally configured geolocation information for the trunk gets used.

Handle a Received Geolocation

The cluster that receives the PIDF-LO XML parses the received geolocation information and passes the information as colon-separated name value pairs in the GeolocationInfo data structure of the CcNotifyInd signal.

Example: “Country=US:A1=NC:A3=RTP:LOC=BLD9”

The content of the received geolocation information of the PIDF-LO overrides any locally configured geolocation information on a trunk, which gets used for the device across the trunk.

Example: {geolocPkid=, filterPkid=d5bdda76-6a86-56c5-b5fd-6dff82b37493, geolocVal=”Country=US:A1=NC:A3=RTP:LOC=BLD9”, devType=4}

Feature Interactions with Midcall Geolocation Change

Outgoing Geolocation Change

The supplementary service (SS) feature interactions, such as Transfer, Conference, Park retrieval, and others, result in connected party change.

For such scenarios, if the SIP trunk or intercluster trunk device receives valid geolocation information from Call Control that differs from previously sent geolocation information, updated geolocation information gets communicated in an UPDATE (SIP trunk) or Notify (intercluster trunk) message.

Incoming Geolocation Change

For SS feature interactions in a remote cluster, the updated geolocation information gets received over an SIP trunk or intercluster trunk in an UPDATE or Notify message.

When such an update is received, the SIP trunk or intercluster trunk parses the PIDF-LO and passes the PIDF-LO to call control and to the LPSession process.

Example PIDF-LO

The following example shows a PIDF-LO that is sent across a SIP trunk. Be aware that the items that are shown in bold font are relevant for location conveyance.

```
UPDATE sip:4400@10.10.10.2:5060;transport=tcp SIP/2.0Date: Sat, 12 Jul 2008
13:28:42 GMT
Call-Info: <urn:x-cisco-remotecc:callinfo>; security= NotAuthenticated
Geolocation: <cid:4900@10.10.10.1>;inserted-by=”10.10.10.1”
Content-ID: 4900@10.10.10.1
From: <sip:4900@10.10.10.1>;tag=4d1edcb1-f546-4ee7-966c-2973fbc56475-31638661
P-Asserted-Identity: <sip:4900@10.10.10.1>
Content-Length: 1070
User-Agent: Cisco-CUCM7.1
To: <sip:4400@10.10.10.2>;tag=e1258ce2-8620-4005-9aa1-72d99cd54050-31642615
Contact: <sip:4900@10.10.10.1:5060;transport=tcp>
Content-Type: application/pidf+xml
Call-ID: bbb3f900-8781b563-b-47f54c0a@10.10.10.2
Via: SIP/2.0/TCP 10.10.10.1:5060;branch=z9hG4bK179f431e3
CSeq: 101 UPDATE
Max-Forwards: 70
<?xml version=”1.0” encoding=”UTF-8”?>
<presence xmlns=”urn:ietf:params:xml:ns:pidf”
xmlns:gp=”urn:ietf:params:xml:ns:pidf:geopriv10”
xmlns:cl=” urn:ietf:params:xml:ns:pidf:geopriv10:civicLoc”
xmlns:dm=”urn:ietf:params:xml:ns:pidf:data-model”
xmlns:caps=”urn:ietf:params:xml:ns:pidf:caps”
xmlns:cisco=”http://www.cisco.com”
entity=”pres:geotarget@example.com”>
<dm:device id=”sg89ae”>
<caps:devcaps>
<cisco:gateway>false</cisco:gateway>
</caps:devcaps>
<gp:geopriv>
<gp:location-info>
<cl:civicAddress>
<cl:country>IN</cl:country>
<cl:A1>KA</cl:A1>
<cl:A2>a2</cl:A2>
<cl:A3>BLR</cl:A3>
<cl:A4>a4</cl:A4>
<cl:A5>a5</cl:A5>
<cl:A6>a6</cl:A6>
<cl:PRD>prd</cl:PRD>
<cl:POD>pod</cl:POD>
<cl:STS>sts</cl:STS>
<cl:HNO>123</cl:HNO>
<cl:HNS>hns</cl:HNS>
<cl:LMK>lmk</cl:LMK>
<cl:LOC>BLDG1</cl:LOC>
<cl:FLR>flr</cl:FLR>
<cl:NAM>nam</cl:NAM>
<cl:PC>pc</cl:PC>
</cl:civicAddress>
</gp:location-info>
<gp:usage-rules>
<gp:retransmission-allowed>yes</gp:retransmission-allowed>
<gp:retention-expiry>2008-09-03T17:58:19Z</gp:retention-expiry>
</gp:usage-rules>
</gp:geopriv>
<timestamp>2008-09-02T17:58:19Z</timestamp>
</dm:device>
</presence>
```

Location Conveyance Configuration

If geolocation information about devices needs to be communicated across clusters, ensure that location conveyance is configured.

To associate devices with geolocations, see the Configure Geolocations, on page 575.

Tip Before you configure location conveyance, review the Configure Location Conveyance, on page 577.

CHAPTER 26

Global Dial Plan Replication

This chapter provides information about how to configure the Global Dial Plan Replication feature. When Global Dial Plan Replication is enabled, the Intercluster Lookup Service (ILS) replicates local and learned directory URIs, enterprise alternate numbers, +E.164 alternate numbers, and number patterns throughout the ILS network. Global Dial Plan Replication allows you to create a global dial plan that spans the ILS network and which includes intercluster dialing of directory URIs and alternate numbers.

Set Up Global Dial Plan Replication

This procedure describes how to set up Global Dial Plan Replication in the ILS network. See the Related Topics for more detailed information on how to perform some of the high-level steps in this procedure.

Before you begin

Global Dial Plan Replication runs on an ILS network. Follow the procedure to set up an ILS network in the "Intercluster Lookup Service" chapter before you configure Global Dial Plan Replication.

Procedure

Step 1 Enable ILS support for Global Dial Plan Replication in the local cluster:

a) Log in to the Unified Communications Manager publisher node.
b) In Cisco Unified Communications Manager Administration, choose **Advanced Features** > **ILS Configuration**.
c) Check the **Exchange Global Dial Plan Replication Data with Remote Clusters** check box.
d) In the **Advertised Route String** text box, enter a route string for the local cluster.
e) Click **Save**.

Step 2 (Optional) If you want to be able to dial directory URIs across clusters, set up URI dialing in the local cluster. For details, see the "URI dialing" chapter.

Step 3 (Optional) If you want to set up alternate numbers that you can dial between clusters, set up alternate number replication by doing the following:

a) Assign enterprise alternate numbers or +E.164 alternate numbers to the directory numbers in your network.

b) For each alternate number, check the **Advertise Globally via ILS** check box.

Step 4 (Optional) If you want to set up a PSTN failover number for specific directory URIs or alternate numbers, assign an alternate number as the PSTN failover number for all the directory URIs and alternate numbers that are associated to a specific directory number.

Step 5 (Optional) If you want to summarize your alternate numbers with a pattern, set up an advertised pattern, and assign a PSTN failover rule for the pattern.

Step 6 In the **Partitions for Learned Numbers and Patterns** configuration window, assign route partitions to the alternate numbers and patterns that the local cluster learns through ILS.

Step 7 Set up SIP route patterns to route calls to the remote clusters in your ILS network by doing the following:

a) Create SIP route patterns that match the route strings for the remote clusters in the ILS network.

b) Point those SIP route patterns to SIP trunks or route lists that route calls to the next-hop clusters in the ILS network.

Step 8 If your network includes a Cisco Unified Border Element, do the following for the SIP profiles in your network:

a) In Cisco Unified CM Administration, choose **Device** > **Device Settings** > **SIP Profile**.

b) Check the **Send ILS Learned Destination Route String** check box and click **Save**.

Step 9 Set an upper limit for the number of learned objects that ILS can write to the local database by setting a value for the ILS Max Number of Learned Objects service parameter. The default value is 100,000.

Step 10 Repeat the previous steps for each cluster in your ILS network.

Step 11 (Optional) If you want your ILS network to interoperate with a Cisco TelePresence Video Communication Server or third-party call control system, import directory URI catalogs from a CSV file for the other system into any hub cluster in the ILS network.

Note If the hub cluster fail, all the spokes connected to it will not have synced-up data until the hub is up. But, existing learn patterns will work.

Related Topics

Set Up Alternate Number, on page 600

Set Up an Advertised Pattern for Alternate Numbers, on page 603

Set Up PSTN Failover for Directory URIs and Alternate Numbers, on page 605

Global Dial Plan Data

When Global Dial Plan Replication is enabled, each cluster in an ILS network advertises its global dial plan data, including global dial plan data that was configured locally and any data that was learned from other clusters, to the ILS network. Global dial plan data includes the following:

Directory URIs

ILS advertises the full catalog of locally configured directory URIs where the Advertise Globally via ILS option is selected. The URI dialing chapter in the *Cisco Unified Communications Manager Features* *and Services Guide* contains details on how to set up URI dialing. See URI Dialing, on page 1081 for more information.

Alternate Numbers

ILS advertises locally configured enterprise alternate numbers and +E.164 alternate numbers to the ILS network where the Advertise globally via ILS option has been selected.

Advertised Patterns

ILS advertises locally configured alternate number patterns to the ILS network.

PSTN Failover

ILS advertises locally configured PSTN failover information for alternate numbers, directory URIs, and advertised patterns.

Route String

ILS advertises the local route string to the ILS network. Each global dial plan data element associates to a route string that identifies the home cluster for that element. Remote clusters use the route string in combination with a SIP route pattern in order to route to the various clusters in an ILS network.

Learned Global Dial Plan Data

In addition to locally configured global dial plan data, ILS advertises all global dial plan data that the local cluster has learned from other clusters in the ILS network. This ensures that all advertised data reaches each cluster in the ILS network. Learned global dial plan data includes learned directory URIs, learned alternate numbers, learned patterns, learned PSTN failover rules, and learned route strings.

Imported Global Dial Plan Data

ILS advertises imported global dial plan data throughout the ILS network. Imported global dial plan data includes directory URIs, +E.164 patterns, and PSTN failover rules that were imported manually from a CSV file for a Cisco TelePresence Video Communication Server or a third-party call control system.

Related Topics

Alternate Numbers, on page 599
Advertised Patterns, on page 601
PSTN Failover, on page 604
Route Strings, on page 605
Learned Global Dial Plan Data, on page 606
Imported Global Dial Plan Catalog Settings, on page 611

Alternate Numbers

Alternate numbers can be configured as aliases of directory numbers. Alternate numbers allow you to configure globally routable numbers that can be dialed from anywhere within an ILS network. Cisco Unified Communications Manager allows you to create two types of alternate numbers:

- Enterprise alternate numbers
- +E.164 alternate numbers

In Cisco Unified Communications Manager Administration, you can create an enterprise alternate number or +E.164 alternate number and associate the alternate number to a directory number. When you associate an alternate number to a directory number, the alternate number can act as an alias of that directory number so that when you dial the alternate number, the phone that is registered to the associated directory number rings.

Each alternate number that you set up must associate to a single directory number. However, that directory number can associate to both an enterprise alternate number and a +E.164 alternate number at the same time. You can also choose one of the alternate numbers as the PSTN failover number for all alternate numbers and directory URIs that are associated to that directory number. See PSTN Failover, on page 604 for more information.

Local Routing with Alternate Numbers

To configure local routing for alternate numbers, you must assign the alternate number to a local route partition that is configured in a calling search space. In Directory Number Configuration, under the alternate number, check the Assign to a local route partition check box and choose a route partition that is in a local calling search space.

Intercluster Routing with Alternate Numbers

For intercluster routing of alternate numbers, Cisco Unified Communications Manager uses ILS to advertise alternate numbers and patterns to the ILS network. For each alternate number that you assign to a directory number, you have the option to include that alternate number in the advertised global dial plan data. If this option is chosen, ILS includes the alternate number along with the local route string and advertises that data to the ILS network. Remote clusters use the route string, in combination with a SIP route pattern, to route calls to that alternate number.

As an alternative, you can configure a pattern that summarizes a range of alternate numbers, and advertise that pattern to the ILS network. The advertised pattern saves you from having to configure replication for each alternate number on an individual basis. For details on advertised patterns, see Advertised Patterns, on page 601.

Related Topics

Set Up Alternate Number, on page 600
Advertised Patterns, on page 601
PSTN Failover, on page 604

Set Up Alternate Number

This procedure describes how to assign an enterprise alternate number or +E.164 alternate number to an existing directory number and configure that alternate number for local or intercluster calls.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Call Routing** > **Directory Number**.

Step 2 Find and select the directory number to which you want to associate the alternate number.

Step 3 Click either **Add Enterprise Alternate Number** or **Add +E.164 Alternate Number** depending on which type of alternate number you want to assign.

Step 4 In the **Number Mask** field, enter the number mask that you want to apply to the directory number. The **Alternate Number** field displays how the alternate number appears after Cisco Unified Communications Manager applies the number mask.

Step 5 (Optional) If you want to enable local routing for the alternate number, do the following:

a) Check the **Add to Local Route Partition** check box.
b) From the **Route Partition** drop-down list box, choose a route partition that is assigned to a local calling search space.

Step 6 (Optional) If you want to use a number pattern to set up intercluster routing for this alternate number, click **Save** and end the procedure. See the Related Topics section for a procedure on how to advertise an alternate number pattern to the ILS network.

Step 7 (Optional) If you want to set up intercluster routing for this alternate number, check the **Advertise Globally via ILS** check box for this alternate number.

Step 8 (Optional) If you want to assign a PSTN failover number to this alternate number, from the **PSTN failover** drop-down list box, assign a number as the PSTN failover.

Step 9 Click **Save**.

What to do next

If you want to enable intercluster routing for the alternate number you must also set up Global Dial Plan Replication within your ILS network. ILS will not advertise the alternate number unless Global Dial Plan Replication is enabled.

Related Topics

Set Up an Advertised Pattern for Alternate Numbers, on page 603

Advertised Patterns

Advertised patterns allow you to create summarized routing instructions for a range of enterprise alternate numbers or +E.164 alternate numbers and replicate that pattern throughout an ILS network such that all clusters within the ILS network know the pattern. Advertised patterns prevent you from having to configure routing information for each alternate number on an individual basis. Advertised patterns are never used by the local cluster on which they are configured—they are only used by remote clusters that learn the pattern through ILS.

For example, if Cluster A has a range of enterprise alternate numbers between 80001 and 89999 and you want to replicate those alternate numbers throughout the ILS network, you can create a pattern of 8XXXX and advertise that pattern to the ILS network. When a remote cluster receives an outgoing call for which the dial string matches the learned pattern (for example, 82211), the remote cluster uses the route string that is associated with the pattern to route the call.

You can also configure PSTN failover information for patterns that are advertised by ILS. See PSTN Failover, on page 604 for more information.

Related Topics

Advertised Patterns Settings, on page 602
Set Up an Advertised Pattern for Alternate Numbers, on page 603
PSTN Failover, on page 604

Advertised Patterns Settings

In Cisco Unified CM Administration, use the **Call Routing** > **Global Dial Plan Replication** > **Advertised Patterns** menu path to create alternate number patterns that ILS advertises to remote clusters in the ILS network.

In the **Advertised Patterns Configuration** window, you can create a number pattern that summarizes a range of alternate enterprise or +E.164 numbers. If Global Dial Plan Replication is enabled, ILS advertises the number pattern to remote clusters in the ILS network.

The following table describes the field settings for the Advertised Patterns Configuration window.

Field	Field Description
Description	
Description	In the text box, enter a description of the number pattern.
Advertised Pattern	
Pattern	In the text box, enter the number pattern that you want Cisco Unified Communications Manager to match against incoming calls. The number pattern must consist of an optional + followed by one or more dialable digits (0-9, A-D, *, #), digit ranges in regular expression format (example: [6-9] or [^6-9]), or single-digit wildcards (X). The pattern may end with an optional % or !. If Global Dial Plan Replication is configured, ILS advertises this pattern to remote clusters in the ILS network. When a remote cluster receives an incoming call that matches this pattern, the remote cluster applies this pattern to the incoming call and tries to route the call to this cluster.
Pattern Type	Choose the type of pattern that applies to this number pattern. When an outgoing call arrives for which the destination dial string matches this number pattern, Cisco Unified Communications Manager assigns the route partition that applies for this pattern type. Click one of the following radio buttons: • Enterprise Number Pattern—choose this option if the number pattern is used for enterprise alternate numbers. • +E.164 Number Pattern—choose this option if the number pattern is used for +E.164 alternate numbers.
Don't use PSTN Failover	Click this radio button if you do not want to configure a PSTN failover for calls that match this pattern. If Cisco Unified Communications Manager is unable to route a call to this pattern over a SIP trunk, the call will not be rerouted to the PSTN.
Use Pattern as PSTN Failover	Click this radio button if you want to use the dial string as the PSTN failover for calls that match this pattern. If Cisco Unified Communications Manager is unable to route the call over a SIP trunk, Cisco Unified Communications Manager uses the calling party AAR CSS to reroute the call to a PSTN gateway.

Field	Field Description
Apply Strip Digits and Prepend Digits to Pattern and Use for PSTN Failover	Click this radio button to use the PSTN Failover Strip Digits and PSTN Failover Prepend Digits fields as the PSTN failover for calls that match this pattern. If Cisco Unified Communications Manager is unable to route the call over a SIP trunk, Cisco Unified Communications Manager applies the PSTN Failover Strip Digits and PSTN Failover Prepend Digits fields to the dial string and uses the calling party AAR CSS to reroute the call to a PSTN gateway.
PSTN Failover Strip Digits	In the text box, enter the number of digits that you want Cisco Unified Communications Manager to strip from the beginning of the dial string for incoming dial strings that match this pattern. You can enter up to 16 digits.
PSTN Failover Prepend Digits	In the text box, enter the digits that you want Cisco Unified Communications Manager to attach to the beginning of the dial string for incoming calls that match this pattern. The allowed characters are 0-9 with an optional leading +.

Set Up an Advertised Pattern for Alternate Numbers

Follow this procedure to create a pattern that summarizes a range of alternate numbers and advertise the pattern to the ILS network.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Call Routing** > **Global Dial Plan Replication** > **Advertised Patterns**.

Step 2 In the **Description** field, enter a description for the pattern.

Step 3 In the **Pattern** field, enter the pattern that you want to advertise to the ILS network.

Step 4 Use the **Pattern Type** radio buttons to choose whether you want to apply the pattern to a range of enterprise alternate numbers or +E.164 alternate numbers.

Step 5 Complete the remaining fields in the **Advertised Patterns Configuration** window to configure a PSTN failover rule for the pattern.

Step 6 Click **Save.**

If Global Dial Plan Replication is enabled, ILS advertises the pattern to remote clusters in the ILS network.

What to do next

For remote clusters to be able to route calls to the PSTN failover number, in the remote cluster you must set up AAR and create route patterns that route the PSTN failover digits to a PSTN gateway.

PSTN Failover

When Global Dial Plan Replication is enabled, ILS can be configured to replicate a PSTN failover rule for learned directory URIs, learned numbers, and learned patterns. If the dial string for an outgoing call matches a learned pattern, learned alternate number, or learned directory URI, and Cisco Unified Communications Manager is unable to route the call over a SIP trunk, Cisco Unified Communications Manager uses the calling party's AAR CSS to reroute the call to the associated PSTN failover number.

Cisco Unified Communications Manager uses the PSTN failover to reroute calls only for calls placed to patterns, alternate numbers, or directory URIs that were learned through ILS. Cisco Unified Communications Manager does not reroute calls to the PSTN failover number for calls that are placed to locally configured patterns, alternate numbers, and directory URIs.

You can use two different methods to assign a PSTN failover rule:

- In the **Advertised Pattern Configuration** window, you can assign PSTN failover Strip Digits and Prepend Digits instructions for an ILA-advertised pattern that summarizes a range of alternate numbers. ILS advertises the pattern and PSTN failover instructions to remote clusters in the ILS network.
- In the **Directory Number Configuration** window, you can configure an alternate number as the PSTN failover for all ILS-advertised alternate numbers and directory URIs that associate to that directory number.

PSTN Failover for Advertised Pattern Example

Company ABC has clusters in New York and Los Angeles in an ILS network and advertises an enterprise alternate number pattern of 8XXXX to represent the range of New York extensions. The pattern includes PSTN failover instructions to strip the first digit and prepend +1718555 to the dial string.

If a Los Angeles employee dials 86301 to reach a New York employee and Cisco Unified Communications Manager is unable to route the call over a SIP trunk, the call is rerouted to a PSTN gateway with +17185556301 as the dial string.

PSTN Failover for Directory URI Example

At Company ABC, Alice’s Los Angeles extension is 2100. Alice also has an enterprise alternate number of 72100, a +E.164 alternate number of +13105552100, and a directory URI of alice@abc.com, all of which are associated to her extension. Alice’s +E.164 alternate number is configured as the PSTN failover.

If a New York employee dials alice@abc.com and Cisco Unified Communications Manager is unable to route the call over a SIP trunk, Cisco Unified Communications Manager reroutes the call to the PSTN failover of +131055521000 and sends the call to a PSTN gateway.

Note For the PSTN failover to be used by remote clusters, you must set up Automated Alternate Routing in your remote clusters and create route patterns that route the PSTN failover number to a PSTN gateway.

Set Up PSTN Failover for Directory URIs and Alternate Numbers

This procedure describes how to assign a PSTN failover number for directory URIs or alternate numbers and advertise that PSTN failover number to the ILS network. Remote clusters can use the PSTN failover number for calls to learned directory URIs or learned alternate numbers.

Note For alternate numbers, you can also assign a PSTN failover rule to an advertised pattern that summarizes a range of alternate numbers. To assign a PSTN failover rule to an advertised pattern, see Set Up an Advertised Pattern for Alternate Numbers, on page 603.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Call Routing** > **Directory Number**.

Step 2 Find and select the directory number that is associated to the directory URI or alternate number for which you want to assign a PSTN failover number.

Step 3 If the alternate number that you want to use as the PSTN failover does not exist, create either an enterprise alternate number or a +E.164 alternate number for the directory number.

Step 4 In the PSTN Failover drop-down list box, choose the alternate number that you want to use as the PSTN failover.

Step 5 Click **Save**.

Cisco Unified Communications Manager associates that PSTN failover number to that directory number. Global Dial Plan Replication advertises that number to the ILS network as the PSTN failover number for all the directory URIs and alternate numbers that are associated to that directory number.

What to do next

In order for a remote cluster to route calls to the PSTN failover number, you must set up the AAR CSS and configure route patterns in the remote cluster that route the PSTN failover number to a PSTN gateway.

Route Strings

To configure Global Dial Plan Replication, you must assign a distinct route string for each cluster in the ILS network. Route String must contain only alphanumeric characters (A-Z,a-z,0-9), dots (.) or dashes (-), not more than 64 characters in length. Although route strings are used with domain-based routing, route strings do not have to match a specific domain—you can assign whatever route strings you want.

When you assign a route string to a cluster, ILS associates that route string to all the global dial plan data that is local to that cluster (including locally configured directory URIs, alternate numbers, advertised patterns, and PSTN failover information). If Global Dial Plan Replication is enabled, ILS advertises the local route string and the rest of the global dial plan data to the ILS network.

To configure remote Cisco Unified Communications Manager clusters to route to the route string, for each cluster in the ILS network, you must configure SIP route patterns that match the route strings in the ILS network and route calls that are destined for those route strings to SIP trunks that lead to the next-hop clusters in your ILS network.

When a user in a remote cluster dials a directory URI or alternate number that was learned through ILS, Cisco Unified Communications Manager matches the associated route string to a SIP route pattern, and routes the call to the trunk that is specified by the SIP route pattern.

You can assign a route string to the local cluster in the ILS Configuration window.

Route String Example

Company ABC has an ILS network with clusters in San Jose and Paris. ABC assigns *ABC.SanJose.USA* and *ABC.Paris.France* as route strings. In the San Jose cluster, ABC configures a domain-based SIP route pattern that routes calls that are destined for *ABC.Paris.France* to an outbound trunk that leads to the Paris cluster. When a user in San Jose dials an alternate number or directory that was configured in Paris, Cisco Unified Communications Manager matches the alternate number to the Paris route string and sends the call to the outbound trunk that is specified by the SIP route pattern.

Learned Global Dial Plan Data

Global dial plan data that Cisco Unified Communications Manager learns through ILS is stored in the local database. In addition to replicating locally configured data, ILS also replicates learned global dial plan data to the rest of the ILS network so that all data that is learned by one cluster is learned by all clusters in the ILS network.

Note Cisco Unified Communications Manager pauses the recording of learned ILS patterns until replication of the cluster is successfully established.

In Cisco Unified CM Administration, you can view the following types of learned global dial plan data:

Learned Alternate Numbers

To display a list of all the alternate enterprise and +E.164 numbers that Cisco Unified Communications Manager learned through ILS, in Cisco Unified CM Administration, choose **Call Routing** > **Global Dial Plan Replication** > **Learned Numbers** and click **Find**.

Learned Enterprise and +E.164 Patterns

To display a list of all the enterprise and +E.164 number patterns that Cisco Unified Communications Manager learned through ILS, in Cisco Unified CM Administration, choose **Call Routing** > **Global Dial Plan Replication** > **Learned Patterns** and click **Find**.

Learned Directory URIs

To display a list of all the directory URIs that Cisco Unified Communications Manager learned through ILS, in Cisco Unified CM Administration, choose **Call Routing** > **Global Dial Plan Replication** > **Learned Directory URIs** and click **Find**.

For any learned alternate number, learned pattern, or learned directory URI, you can click the number, pattern, or directory URI to open that item in the Learned Object window, where you can view additional details, such as the PSTN failover number.

Partitions for Learned Patterns Settings

In Cisco Unified CM Administration, use the **Call Routing** > **Global Dial Plan Replication** > **Partitions for Learned Patterns** menu path to assign route partitions to the alternate numbers and patterns that Cisco Unified Communications Manager learns through the Global Dial Plan Replication feature with ILS.

You must assign learned numbers and learned patterns to a partition. You cannot assign a learned number or learned pattern to a NULL partition. You can define your own partitions or use the predefined default partitions. Cisco Unified Communications Manager comes installed with the following predefined partitions for learned alternate numbers and number patterns:

- Global Learned Enterprise Numbers
- Global Learned E.164 Numbers
- Global Learned Enterprise Patterns
- Global Learned E.164 Patterns

The following table describes the field settings for the **Partitions for Learned Alternate Numbers and Patterns Configuration** window.

Table 68: Partitions for Learned Patterns Settings

Field	Description
Associated Partitions for Learned Alternate Numbers and Patterns	
Partition for Enterprise Alternate Numbers	From the drop-down list box, choose a partition on which to apply enterprise alternate numbers that Cisco Unified Communications Manager learns from remote clusters in the ILS network. If the dial plan contains overlapping route patterns, by default, Cisco Unified Communications Manager does not route the call until the interdigit timer expires (even if a possible route exists for the dialed digits). This setting guards against learned numbers that overlap with statically configured directory numbers and number patterns by allowing Cisco Unified Communications Manager to choose the best match of all available routes for the dial string. Check the **Mark Learned Number as Urgent Priority** check box to configure Cisco Unified Communications Manager to route the call after it finds a match between the dialed digits and an available route, without waiting for the interdigit timer to expire (for example, the T302 Timer service parameter).

Field	Description
Partition for +E.164 Alternate Numbers	From the drop-down list box, choose a partition on which to apply +E.164 alternate numbers that Cisco Unified Communications Manager learns from remote clusters in the ILS network. If the dial plan contains overlapping route patterns, by default, Cisco Unified Communications Manager does not route the call until the interdigit timer expires (even if a possible route exists for the dialed digits). This setting guards against learned numbers that overlap with statically configured directory numbers and number patterns by allowing Cisco Unified Communications Manager to choose the best match of all available routes for the dial string. Check the **Mark Learned Number as Urgent Priority** check box to configure Cisco Unified Communications Manager to route the call after it finds a match between the dialed digits and an available route, without waiting for the interdigit timer to expire (for example, the T302 Timer service parameter).
Partition for Enterprise Patterns	From the drop-down list box, choose a partition on which to apply enterprise alternate number patterns that are learned from remote clusters in the ILS network. If the dial plan contains overlapping route patterns, by default, Cisco Unified Communications Manager waits for the interdigit timeout (for example, the T302 Timer service parameter) to expire before attempting to route calls (even if a match exists). This setting guards against learned patterns that overlap with statically configured directory numbers and patterns by allowing Cisco Unified Communications Manager to choose the best match of all available routes for the dial string. To configure Cisco Unified Communications Manager to ignore the interdigit timeout and route the call after it finds a possible route, check either or both of the following check boxes: • **Mark Fixed Length Patterns as Urgent**—When this check box is checked, Cisco Unified Communications Manager immediately routes calls as soon it receives a match with an advertised pattern of fixed length. • **Mark Variable Length Patterns as Urgent**—When this check box is checked, Cisco Unified Communications Manager immediately routes calls as soon as it receives a match with an advertised pattern of variable length.

Field	Description
Partition for +E.164 Patterns	From the drop-down list box, choose a partition on which to apply +E.164 alternate number patterns that are learned from remote clusters in the ILS network. If the dial plan contains overlapping route patterns, by default, Cisco Unified Communications Manager waits for the interdigit timeout (for example, the T302 Timer service parameter) to expire before attempting to route calls (even if a match exists). This setting guards against learned patterns that overlap with statically configured directory numbers and patterns by allowing Cisco Unified Communications Manager to choose the best match of all available routes for the dial string. To configure Cisco Unified Communications Manager to ignore the interdigit timeout and route the call after it finds a possible route, check either or both of the following check boxes: • **Mark Fixed Length Patterns as Urgent**—When this check box is checked, Cisco Unified Communications Manager immediately routes calls as soon as it receives a match with an advertised pattern of fixed length. • **Mark Variable Length Patterns as Urgent**—When this check box is checked, Cisco Unified Communications Manager immediately routes calls as soon as it receives a match with an advertised pattern of variable length.

Block a Learned Pattern

If you want to prevent a local Cisco Unified Communications Manager cluster from routing calls to a learned alternate number or learned alternate number pattern, you can configure a local blocking rule on that cluster. Before routing a call to a learned number or learned pattern, ILS checks to see if a local blocking rule matches the dial string. If the blocking rule matches, Cisco Unified Communications Manager does not route the call.

Some additional characteristics of blocking rules:

- Blocking rules are applied only on the local cluster on which you configure them—ILS does not advertise blocking rules.
- Blocking rules are applied only to learned alternate numbers and learned patterns—Cisco Unified Communications Manager does not apply blocking rules to locally configured numbers or route patterns.

To set up a blocking rule for a learned alternate number or learned alternate number pattern, perform the following steps:

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Call Routing** > **Global Dial Plan Replication** > **Block Learned Numbers and Patterns**.

Step 2 Enter a description for the blocking rule.

Step 3 In the Blocked Pattern section, complete the fields that you want to use as conditions for the blocking rule. If you do not want to use a specific field as a blocking condition, you can leave that field blank. For example:

- If you want to block all calls to ABC_cluster1 regardless of the other call parameters, enter ABC_cluster1 in the **Cluster ID** field, click the **Any** radio button, and leave the remaining fields empty.

- If you want to block all +E.164 calls to Cluster_3 that use a prefix of 683, enter “Cluster_3” in the Cluster ID field, enter “683” in the Prefix field, click the **+E.164 Pattern** radio button, and leave the remaining fields empty.
- If you want to block a specific enterprise pattern, enter the pattern in the Pattern field and click the **Enterprise Pattern** radio button.

Step 4 In the Pattern type field, choose whether you want to apply the blocking rule to Enterprise patterns, +E.164 patterns, or both.

Step 5 Click **Save**.

Blocked Learned Patterns Settings

In Cisco Unified CM Administration, use the **Call Routing** > **Global Dial Plan Replication** > **Block Learned Numbers and Patterns** menu path to create blocking rules that prevent the local cluster from routing calls to specific enterprise and +E.164 alternate numbers or number patterns that were learned through the Intercluster Lookup Service (ILS).

The following table describes the field settings for the **Blocked Learned Pattern** window. In the Blocked Pattern section, complete only the fields that you want to use that are relevant as blocking conditions.

Field	Field Description
Description	
Description	In the text box, enter a description of the number or pattern that you want to block.
Blocked Pattern	
Pattern	If you want to use a number pattern to identify the calls that you want to block, in this text box, enter the number pattern, including numbers and wildcards (do not use spaces). For example, a number pattern of 206XXXXXXX could be used to block calls that are placed to either 2065551212 or 2063331234. If you do not want to use a number pattern as part of your blocking rule, leave this field empty. If your blocking number pattern has a fewer matching digits than the ILS-learned number pattern, Cisco Unified Communications Manager will still route the call. For example, if you have a call placed to 2065551212 for which there is an ILS-advertised matching number pattern of 206555XXXX as well as a blocked pattern of 206XXXXXXX, the call will still be routed, because the matching pattern has more matching digits than the blocking pattern.
Prefix	If you want to block patterns based on the dial string prefix, enter the prefix digits for which you want Cisco Unified Communications Manager to block calls. If you do not want to use a prefix as part of your blocking rule, leave this field empty.

Field	Field Description
Cluster ID	If you want to block all calls from being sent to a specific cluster, enter the cluster ID for the remote cluster that you want to block calls from reaching. Otherwise, leave this field empty.
Pattern Type	Choose one of the following three options depending on the number pattern type to which you want to apply the blocking rule: • Any—Choose this option if the blocking rule applies to both enterprise number patterns and +E.164 patterns. • Enterprise Pattern—Choose this option if the blocking rule applies to enterprise number patterns only. • +E.164 Pattern—Choose this option if the blocking rule applies to +E.164 number patterns only.

About Imported Global Dial Plan Data

Cisco Unified Communications Manager allows you to import global dial plan data from a CSV file into any hub cluster in an ILS network and ILS replicates the imported global dial plan data throughout the ILS network allowing you to interoperate Cisco Unified Communications Manager with a Cisco TelePresence Video Communications Server or a third-party call control system.

You can import directory URIs, +E.164 patterns, and associated PSTN failover rules into Cisco Unified Communications Manager. You can view the global dial plan data that has been imported into the local cluster by doing the following:

- Imported Directory URIs—To view a list of directory URIs and associated PSTN failover numbers that have been imported into the local cluster, choose **Call Routing** > **Global Dial Plan Replication** > **Imported Directory URIs** and click the **Find** button.
- Imported Patterns—To view a list of +E.164 patterns and PSTN failover rules that have been imported into the local cluster, choose **Call Routing** > **Global Dial Plan Replication** > **Imported Patterns** and click the **Find** button.

Note Imported data includes only global dial plan data that is imported manually into Cisco Unified Communications Manager. Imported global dial plan data does not include data that was learned through ILS.

Imported Global Dial Plan Catalog Settings

In Cisco Unified CM Administration, use the **Call Routing** > **Global Dial Plan Replication** > **Imported Global Dial Plan Catalog** path to import manually directory URIs, +E.164 patterns and PSTN failover rules from a CSV file for a call control system that is not running ILS, such as a Cisco TelePresence Video Communication Server or a third-party call control system.

Configure the settings on the **Imported Global Dial Plan Catalog** window to create an empty catalog with a route string for the remote call control system. After you configure the settings, you must use Bulk Administration to insert directory URIs and patterns from the CSV file into the newly created catalog.

Note The local cluster must be part of an existing ILS network. For more information about ILS networks, see the "Intercluster Lookup Service" chapter of the *Cisco Unified Communications Manager Features and Services Guide.*

The following table contains field descriptions for the Imported Global Dial Plan Catalog window.

Field	Description
Name	Enter a unique name to identify the catalog that you want to import.
Description	Enter a description for the catalog that you want to import.
Route String	Enter a route string for the remote call control system. Route strings can be up to 250 alphanumeric characters long and can include dots and dashes. Cisco Unified Communications Manager uses route strings in conjunction with SIP route patterns to route calls to directory URIs that are configured in remote clusters. When a call from the local cluster is placed to a directory URI in this remote catalog, Cisco Unified Communications Manager matches the directory URI with the route string and then uses a SIP route pattern to match that route string to an outbound trunk that routes to that directory URI. **Note** After you create the route string, create a SIP route pattern that routes this route string to an outbound trunk. See the SIP route pattern setup chapter of the *Cisco Unified Communications Manager Administration Guide* for more information about SIP route patterns.

Import Directory URIs and Patterns From a Non-ILS System

Follow this procedure if you are running the Intercluster Lookup Service (ILS) on your local cluster and you want to import a global dial plan catalog, including directory URIs, +E.164 number patterns, or PSTN failover rules from a CSV file for a call control system that is not running ILS, such as a Cisco TelePresence Video Communication Server (VCS) or a third-party call control system.

To perform this procedure, the Cisco Bulk Provisioning Service must be running on the local cluster, which must be configured as a hub cluster in an ILS network. After you import the catalog into Cisco Unified Communications Manager, ILS replicates the imported catalog to the other clusters in the ILS network.

Note Make sure that the CSV file that you use for the import is compatible with your version of Cisco Unified Communications Manager. For example, a CSV file that is compatible to import into Version 9.0(1) is not compatible with Version 10.0(1). To view a sample CSV file for your release, in Cisco Unified CM Administration, choose **Bulk Administration** > **Directory URIs and Patterns** > **Insert Directory URIs and Patterns** and click **View Sample File**.

Note Within Cisco Unified CM Administration, you can enter directory URIs with embedded double quotation marks or commas. However, when you use Bulk Administration to import a CSV file that contains directory URIs with embedded double quotation marks and commas, you must enclose the entire directory URI in double quotation marks and escape the embedded double quotation marks with a double quotation mark. For example, a directory URI of Jared, “Jerry”,Smith@test.com must be input as “Jared”, ““Jerry””, “Smith@test.com” in the CSV file.

Procedure

Step 1 In Cisco Unified CM Administration, choose **Call Routing** > **Global Dial Plan Replication** > **Imported Global Dial Plan Catalogs**.

Step 2 In the **Name** field, enter a name for the catalog.

Step 3 In the **Description** field, enter a description of the catalog.

Step 4 In the **Route String** field, create a route string for the system from which you are importing the catalog.

Step 5 Click **Save**.

Step 6 In Cisco Unified CM Administration, choose **Bulk Administration** > **Upload/Download Files**.

Step 7 Click **Add New**.

Step 8 Click **Browse** and select the CSV file for the catalog that you want to import.

Step 9 In the **Select the Target** drop-down list box, choose **Imported Directory URIs and Patterns**.

Step 10 In the **Select Transaction Type** drop-down list box, choose **Insert Imported Directory URIs and Patterns**.

Step 11 Click **Save**.

Step 12 In Cisco Unified CM Administration, choose **Bulk Administration** > **Directory URIs and Patterns** > **Insert Imported Directory URIs and Patterns**.

Step 13 In the **File Name** drop-down list box, choose the CSV file that contains the catalog that you want to import.

Step 14 In the **Imported Directory URI Catalog** drop-down list box, choose the catalog that you named in the Imported Global Dial Plan Catalog window.

Step 15 In the **Job Description** text box, enter a name for the job that you are about to run.

Step 16 Select when you want to run the job.

- If you want to run the job now, click the **Run Immediately** radio button, and click **Submit.**
- If you want to schedule the job to run at a specified time, check the **Run Later** radio button and click **Submit**. If you choose this option, you must use the Bulk Administration Job Scheduler to schedule when the job runs.

Note Cisco Unified Communications Manager saves all imported +E.164 patterns to the Global Learned +E.164 Patterns partition.

CHAPTER 27

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.

Configure Hold Reversion

The Hold Reversion feature alerts a phone user when a held call exceeds a configured time limit. When the held call duration exceeds the limit, Cisco Unified Communications Manager generates alerts, such as a ring or beep, at the phone to remind the user to handle the call. The held call becomes a reverted call when the hold duration exceeds the configured time limit.

Perform the following steps to configure the hold reversion feature. This procedure assumes that you have configured DNs for phones or are using auto-registration.

Procedure

Step 1 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 installed the locale installer.

Step 2 (Optional) Configure the Reverted Call Focus Priority setting in the Device Pool Configuration window for a new or existing device pool.

Step 3 In the Service Parameter Configuration window for the Cisco CallManager service, configure the hold reversion timer settings.

Step 4 In the Phone Configuration window, verify that the correct device pool is configured for the Cisco Unified IP Phone(s). If not, apply the correct device pool.

Step 5 In the Phone Configuration window, verify that the correct user locale is configured for the Cisco Unified IP Phone(s).

Step 6 Verify that the Cisco CallManager service is activated in Cisco Unified Serviceability.

Related Topics

Configure Call Focus Priority, on page 625
Configuration Tips for Cisco Hold Reversion, on page 625
Configure Hold Reversion Timer Settings, on page 626

Cisco Hold Reversion Feature

The Hold Reversion feature alerts a phone user when a held call exceeds a configured time limit. When the held call duration exceeds the limit, Cisco Unified Communications Manager generates alerts, such as a ring or beep, at the phone to remind the user to handle the call. The held call becomes a reverted call when the hold duration exceeds the configured time limit.

Note Throughout this chapter, references to reverted calls apply only to reverted calls that are invoked by the hold reversion feature; these references do not apply to other reverted call types, such as park reverted calls.

As administrator, you can configure hold reversion for any DN that is associated with a phone that is on the same Cisco Unified Communications Manager server. The phone device that is associated with the line must support this feature, or hold reversion does not activate. When multiple phone devices share a line, only those devices that support hold reversion can use this feature.

Note Cisco Hold Reversion applies specifically to calls that an end user puts on hold. You cannot activate this feature on calls that the system or network puts on hold; for example, during conference or transfer operations.

The types of alerts that are generated at the phone for reverted calls depend on the capabilities of the phone device. Cisco Unified Communications Manager provides the following alerts when the hold reversion feature activates, depending on the capabilities of the phone and the firmware release that is installed.

- The phone rings once or beeps once.
- The status line briefly displays “Hold Reversion” for the reverted call at the user phone.
- The LED next to the line button flashes continuously on the phone handset, like other alerting operations.
- A “wobbling” handset icon displays for a reverted call.

See the Cisco Unified IP Phone administration guides for Cisco Unified IP Phone models that support hold reversion and this version of Cisco Unified Communications Manager for more information about your phone capabilities.

Cisco Hold Reversion Description

To enable hold reversion, you configure timer settings for your system or for specific phone lines.

- When hold reversion is enabled for the system, the hold reversion feature gets invoked when a call that a user at your site puts on hold exceeds the configured time limit, unless the feature is disabled for that line or the phone does not support the hold reversion feature.
- When hold reversion is enabled for a line but not for the system, only calls that are received on that line can invoke the hold reversion feature.
- When hold reversion is enabled for both the line and the system, the timer settings for the line override the timer settings for the system.

Hold Reversion Alerting Operations

The following table provides a summary of hold reversion alerting operations for different call scenarios when hold reversion is invoked for a line or system. These operations apply to incoming calls and outgoing calls that a phone user puts on hold.

Hold reversion ring uses the ring settings that are defined in Cisco Unified Communications Manager Administration for that user, except that flash gets converted to flash once and ring gets converted to ring once. If the ring setting specifies disabled, the phone will not ring, flash, or beep.

If the user has another active call, the user also receives call waiting tone once on the reverted call.

Table 69: Hold Reversion Alerting Operations

Scenario	Alerting Operations
Incoming call alerting before hold reversion activates	No hold reversion alerts get sent to the holding phone until the incoming call is answered (except for the hold reversion icon).
Incoming call alerting after hold reversion activates	No additional alerts get sent to the holding phone until the incoming call is answered.
Shared line	Only the device that initiates the held call receives alerts. Other instances of the shared line do not receive alerts.
Multiple reverted calls on the same phone device or on the same phone line with no incoming call	All reverted calls receive alerts. You can configure different alert intervals for different lines.
Mutual hold	Both parties can receive hold reversion alerts.
Holding party represents one-sided call; for example, another feature splits the call or redirects the call	Hold reversion alerts get delayed until the holding party reassociates with another party.

Note 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.

Call Focus Operations

A reverted call must have focus, meaning be highlighted on the phone, before it can be retrieved.

The call focus priority specifies which call type, incoming calls or reverted calls, has priority for user actions, such as going off hook. At Cisco Unified Communications Manager installation, incoming calls have priority.

You can configure which call type has priority. For example, when incoming calls are configured with a higher priority, if a held call is in the reverted state and the phone goes off hook, Cisco Unified Communications Manager resumes the reverted call only when no incoming call is present.

If the user puts multiple calls on hold for the same line or on the same phone and more than one call is in the reverted state, the oldest call keeps focus, and Cisco Unified Communications Manager resumes the oldest reverted call first, unless an incoming call exists (when incoming calls have priority) or the user chooses to resume another reverted call. Users can choose to retrieve another reverted call by highlighting the call and pressing the Select softkey.

If the phone device of the user has a remote-in-use call and a reverted call, Cisco Unified Communications Manager retrieves the reverted call on off hook.

See the Call Focus Priority, on page 624 for more information about call focus configuration settings for this feature.

Retrieve Reverted Calls

When the reverted call has focus, users can retrieve the reverted call by

- Picking up the handset
- Pressing the speaker button on the phone
- Pressing the headset button
- Selecting the line that is associated with the reverted call
- Pressing the Resume softkey

These actions assume that the handset is idle and the speaker is not already on.

Note See the Cisco Unified IP Phone user guides for Cisco Unified IP Phone models that support hold reversion and this version of Cisco Unified Communications Manager for more information.

Timer Deactivation

The hold reversion alerting timers for the hold reversion feature stop when

- The user retrieves a held call.
- The user invokes another feature on the same call.
- The held call gets released.

If the call is not resumed before the clusterwide Maximum Hold Duration Timer system setting expires, Cisco Unified Communications Manager stops the reminder alerts and clears the call. If the Maximum Hold Duration Timer specifies 0, the call remains on hold until the clusterwide Maximum Call Duration Timer setting expires and Cisco Unified Communications Manager clears the call.

See the Interactions, on page 622 section for more information about how hold reversion works with Cisco Unified Communications Manager applications and call-processing features.

Examples

The following examples describe how hold reversion works in Cisco Unified Communications Manager.

In these examples, the hold reversion duration timer, which defines when to activate hold reversion, is set to 30, and the hold reversion interval timer, which defines when to send reminder alerts, is set to 20.

Example: Hold Reversion Feature Disabled

User A calls user B, who exists on the same system as user A. User B answers the call and puts the call on hold. If MOH is configured for held calls, user A receives music.

Because hold reversion is not enabled for the DN, user B does not receive alerts to indicate that the call remains on hold. The clusterwide Maximum Hold Duration Timer system setting expires, and Cisco Unified Communications Manager clears the call.

Example: Reverted Call and New Outgoing Call

User A calls user B, who exists in the same Cisco Unified Communications Manager system as user A. User B answers the call and puts the call on hold. If MOH is configured for held calls, user A receives music.

Cisco Unified Communications Manager notifies user B when the held call assumes the reverted state - after 30 seconds, Cisco Unified Communications Manager sends the message “Hold Reversion” to the phone and rings the phone once (or beeps or flashes once) on the holding DN. (Your phone may support additional alerting mechanisms.)

User B goes off hook to make an outgoing call when the held call is in the reverted state. Cisco Unified Communications Manager resumes the held call. User B cannot make a new outgoing call.

Example: Shared Line

User A and user B exist in the same system. User A calls a shared line on user B phone. User B puts the call on hold. If MOH is configured for held calls, user A receives music.

Cisco Unified Communications Manager notifies user B when hold reversion activates for the call - after 30 seconds, Cisco Unified Communications Manager sends the message “Hold Reversion” to the phone and rings the phone once (or beeps or flashes once) on the holding DN. (Your phone may support additional alerting mechanisms.) Other users on the shared line do not receive reverted call alert.

Until user B retrieves the reverted call, Cisco Unified Communications Manager sends periodic reminder alerts every 20 seconds to the holding phone for the DN - Cisco Unified Communications Manager sends the message “Hold Reversion” to the phone and rings the phone once (or beeps or flashes once) on the holding

DN at the configured intervals. (Your phone may support additional alerting mechanisms.) No other users on the shared line receive reminder alerts.

User B receives no other calls on the phone. The reverted call has focus, and user B goes off hook. User B retrieves the reverted call.

Note When the held party is a shared line, other line appearances show normal indicators for a remote-in-use call. When the holding party is a shared line, the remote-in-use indicator does not display on other line appearances after the user puts the call on hold; the remote-in-use indicator redisplays on the other line appearances when the user reconnects with the call. If another user on the shared line picks up the reverted call, the phone of the holding party displays the remote-in-use indicator and no longer displays hold reversion alerts. If the holding party drops off the call, for example, gets released by an application, the Hold Reversion timers deactivate.

Example: Multiple Reverted Calls on the Same Line

User A and user C call user B on the same DN; user B has Hold Reversion enabled, and call A is a reverted call.

User B answers the call from User C and puts the call on hold. If MOH is configured for held calls, user C receives music.

Cisco Unified Communications Manager notifies user B when call C assumes the reverted state - after 30 seconds, Cisco Unified Communications Manager sends the message “Hold Reversion” to the phone and rings the phone once (or beeps or flashes once) on the holding DN. (Your phone may support additional alerting mechanisms.) User B gets reminder alerts for both calls every 20 seconds.

Call A has focus, and user B retrieves the reverted call from user A.

Example: Multiple Reverted Calls on Different Lines with Incoming Call

User A calls on line B1 for user B, who has hold reversion configured on both B1 and B2. User B puts user A on hold. If MOH is configured for held calls, user A receives music.

User C calls on line B2 for user B. User B puts user C on hold. If MOH is configured for held calls, user C receives music.

Both held calls enter the reverted state when they exceed the preconfigured time limit of 30 seconds. User B gets hold reversion alerts for both held calls.

An incoming call comes in on line B3. Incoming calls have focus priority. User B goes off hook and answers the incoming call. User B ends the B3 call.

User B goes off hook and resumes the B1 call. User B still receives reminder alerts every 20 seconds for call B2. User B presses the **Resume** softkey. Call B1 gets put on hold, and call B2 gets connected.

Cisco Unified Communications Manager restarts the timer for activating the hold reversion feature on call B1.

System Requirements

Hold reversion requires the following software components:

- Cisco Unified Communications Manager 6.0 or later

- Cisco CallManager service that is running on at least one node in the cluster

  Cisco CallManager service that is running on the node

- Cisco CTIManager service that is running on at least one node in the cluster

  Cisco CTIManager service that is running on the node

- Cisco Database Layer Monitor service that is running on the same node as the Cisco CallManager service
- Cisco RIS Data Collector service that is running on the same node as the Cisco CallManager service
- Cisco Tftp service that is running on at least one node in the cluster

  Cisco Tftp service that is running on the node

- Cisco Unified Communications Manager Locale Installer; that is, if you want to use non-English phone locales or country-specific tones (see the Cisco Unified Communications Operating System Administration Guide for information on locale installers)

Determine Device Support for Hold Reversion

Use the Cisco Unified Reporting application to generate a complete list of devices that support hold reversion. To do so, follow these steps:

For additional information about the Cisco Unified Reporting application, see the *Cisco Unified Reporting Administration Guide*.

Procedure

Step 1 Start Cisco Unified Reporting by using any of the methods that follow. The system uses the Cisco Tomcat service to authenticate users before allowing access to the web application. You can access the application by,

- choosing **Cisco Unified Reporting** in the Navigation menu in Cisco Unified Communications Manager Administration and clicking **Go.**
- choosing **File** > **Cisco Unified Reporting** at the Cisco Unified Real Time Monitoring Tool (RTMT) menu.
- entering https://<server name or IP address>:8443/cucreports/ and then entering your authorized username and password.

Step 2 Click **System Reports** in the navigation bar.

Step 3 In the list of reports that displays in the left column, click the **Unified CM Phone Feature List** option.

Step 4 Click the Generate a new report link to generate a new report, or click the Unified CM Phone Feature List link if a report already exists.

Step 5 To generate a report of all devices that support hold reversion, choose these settings from the respective drop-down list boxes and click the **Submit** button:

Product: All

Feature: Hold Reversion

The List Features pane displays a list of all devices that support the hold reversion feature. You can click on the Up and Down arrows next to the column headers (Product or Protocol) to sort the list.

Interactions and Restrictions

This section describes the interactions and restrictions for hold reversion.

Interactions

This section describes how hold reversion interacts with Cisco Unified Communications Manager applications and call processing.

Music On Hold

Cisco Unified Communications Manager supports MOH 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, Cisco Unified Communications Manager 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, Cisco Unified Communications Manager alerts the user with one ring. Cisco Unified Communications Manager does not play a preemption ring. If a high precedence call becomes a reverted call, Cisco Unified Communications Manager 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 Manager JTAPI Developer Guide
- Cisco Unified Communications Manager TAPI Developer Guide

Hold Reversion Notification Interval for SCCP and 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.

Restrictions

The following restrictions apply to the hold reversion feature:

- Cisco Extension Mobility and Cisco Web Dialer features do not support the hold reversion feature.
- 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.
- When hold reversion is enabled for the system, the phone must have the ability to support the hold reversion feature, or the feature does not activate.
- Shared line devices cannot configure different hold reversion timers.
- 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.

- The maximum number of reverted calls that are allowed on a line equals the maximum number of calls setting for your system.
- See the 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.
- To enable this feature with CTI applications, ensure that the CTI application is certified to work with this feature and this Cisco Unified Communications Manager 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:
  - Unified Communications Manager JTAPI Developer Guide.
  - Unified Communications Manager TAPI Developer Guide.

Install and Activate Cisco Hold Reversion

Hold reversion automatically installs when you install Cisco Unified Communications Manager. After you install Cisco Unified Communications Manager, you must configure hold reversion feature settings in Cisco Unified Communications Manager Administration to enable the feature.

Hold reversion relies on the Cisco CallManager service, so make sure that you activate the Cisco CallManager service in Cisco Unified Serviceability.

Cisco Hold Reversion Configuration

This section provides information to configure Hold Revision.

Tip Before you configure hold reversion, review the summary task to configure Hold Reversion.

Related Topics

Configure Hold Reversion, on page 615

Hold Reversion Timers in the Service Parameter Window

The following timers in Cisco Unified Communications Manager specify the alert operations for hold reversion:

- The Hold Reversion Duration timer specifies the wait time before a reverted call alert gets issued to the phone of the holding party.
- The Hold Reversion Notification Interval timer specifies the frequency of the periodic reminder alerts to the holding party phone.

For example, a duration timer setting of 20 and an interval setting of 30 means that Cisco Unified Communications Manager will issue the first alert after 20 seconds and a reminder alert every 30 seconds thereafter. The hold reversion feature activates when the hold reversion duration timer times out (after 20 seconds).

See the Configure Hold Reversion Timer Settings, on page 626 for the hold reversion timer configuration procedure.

At installation, the value of the hold reversion duration timer settings specifies 0, which means that the feature is disabled. The hold reversion duration line settings remain empty.

Call Focus Priority

When a phone has a reverted call and an incoming call alerting, the call focus priority specifies which call type has focus, meaning which call type has priority for user actions, such as going off hook. At Cisco Unified Communications Manager installation, incoming calls have priority.

As administrator, you configure the Reverted Call Focus Priority setting for a device pool, which you then assign to a phone device in Cisco Unified Communications Manager Administration. The focus priority for the device pool that is associated with the phone applies to reverted and incoming calls that appear on the same line or on different lines on the phone device.

See Configure Call Focus Priority, on page 625 for the call focus priority configuration procedure.

Configuration Tips for Cisco Hold Reversion

Consider the following information when you configure the hold reversion feature in Cisco Unified Communications Manager Administration:

- You must set the Hold Reversion Duration timer and Hold Reversion Notification Interval timer settings for the system for Cisco CallManager service updates.
- At installation, the Hold Reversion Duration timer specifies 0, which disables the feature.
- You cannot configure hold reversion settings for DNs that are associated with phones that do not support this feature.
- Configure the Maximum Hold Duration Timer system setting to a value greater than 0; otherwise, a reverted call can remain on hold until the Maximum Call Duration Timer expires.
- If you configure the Maximum Hold Duration Timer to a value less than the Hold Reversion Duration timer, the hold reversion feature does not activate.
- If you leave either the Hold Reversion Ring Duration (seconds) timer setting or Hold Reversion Notification Interval (seconds) timer setting blank in the Directory Number Configuration window, Cisco Unified Communications Manager uses the hold reversion timer settings for the system. If you configure a value for either timer in the Directory Number Configuration window, Cisco Unified Communications Manager uses the timer settings for the line.
- If you configure the Hold Reversion Duration timer for either the system or a line to a value greater than 0 but do not configure the Hold Reversion Notification Interval timer, Cisco Unified Communications Manager sends just one alert, when the call assumes the reverted state. If you configure the Hold Reversion Notification Interval timer for either the cluster or the line but do not configure Hold Reversion Duration timer to a value greater than 0, the hold reversion feature does not activate.
- Only Cisco Unified IP Phones that support the hold reversion feature display the hold reversion timer settings in the Directory Number Configuration window. 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 that line.
- If the ring settings that are configured for the phone specify Disabled, the phone will not ring, flash, or beep for the hold reversion feature.
- Changing the hold reversion duration timer requires a reset of the device; changing the reverted call priority field requires reset of devices in that device pool.
- To fully disable the hold reversion feature after it is enabled, be sure to disable the Hold Reversion Duration timer on every line in addition to disabling the clusterwide settings.

Configure Call Focus Priority

Perform the following procedure to configure the call focus priority setting for the hold reversion feature. You can configure this setting in the Default device pool or in another device pool in the list, or you can create a new device pool for hold reversion feature users.

Note The Not Selected setting specifies the reverted call focus priority setting for the default device pool at installation. At installation, incoming calls have priority. You cannot choose this setting in Cisco Unified Communications Manager Administration.

If you are configuring a new device pool, see the *Cisco Unified Communications Manager Administration Guide* for more information.

Procedure

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

The Find and List Device Pools window displays.

Step 2 To display the device pools list, click **Find**, or use the search results from an active query. Choose a device pool in the Find and List Device Pool window.

Step 3 In the Reverted Call Focus Priority field, choose one of the following settings:

a) Choose Default to assign highest priority to incoming calls.
b) Choose Highest to assign highest priority to reverted calls.

Step 4 Click the **Save** button.

Step 5 Reset any devices in the device pool to incorporate the change.

Note Call focus priority gets sent to the phone that is running SIP by its TFTP configuration file.

Configure Hold Reversion Timer Settings

Perform the following procedure to enable the hold reversion feature and to configure the hold reversion timer settings. This procedure assumes that DNs are configured for a phone or that the phones are using auto-registration.

Consider the following information when you are configuring hold reversion timer settings:

- To enable hold reversion, change the Hold Reversion Duration timer in the Service Parameters window to a value greater than 0.
- If you do not want to use the default system setting for reminder alerts, configure the Hold Reversion Notification Interval timer in the Service Parameters window. The default value specifies 30 seconds.
- To disable hold reversion for a line when the system setting is enabled, enter a value of 0 for the Hold Reversion Duration timer in the Directory Number Configuration window. If you leave the field empty, Cisco Unified Communications Manager uses the timer setting.
- To enable hold reversion for a line when the system setting is disabled, set the Hold Reversion Ring Duration (seconds) timer in the Directory Number Configuration window to a value greater than 0. To enable reminder alerts, configure the Hold Reversion Notification Interval timer to a value greater than 0 in the same window or leave it blank to use the default setting.
- To configure hold reversion timer settings that differ from the default settings when hold reversion is enabled, enter different values for the hold reversion timers in the Directory Number Configuration window.

Procedure

Step 1 Find the hold reversion timers for a line or the default:

a) To enable hold reversion and configure timer settings, choose **System** > **Service Parameters** in Cisco Unified Communications Manager Administration.

  - From the Server drop-down list box, choose the server that is running the Cisco CallManager service.
  - From the Service drop-down list box, select the Cisco CallManager service.

  The Service Parameters Configuration window displays. Go to the next step.

b) To enable or disable hold reversion and configure hold reversion timer settings for a line, choose **Device** > **Phone** in Cisco Unified Communications Manager Administration. Click Find to display the device pools list, or use the search results from an active query.

  - Choose a device from the phone list that displays in the Find and List Phones window. The Phone Configuration window displays.
  - In the phone configuration window, choose a Directory Number from the list at the left.

  The Directory Number Configuration window displays. Go to the next step.

Step 2 Configure the hold reversion timers:

a) In the Hold Reversion Ring Duration (seconds) field, enter a value greater than 0 to enable the hold reversion feature. To disable the hold reversion feature, enter a 0. You can enter a value from 0 to 1200 seconds (inclusive). This timer notifies a user when a held call enters the reverted state.

b) If you do not want to use the existing setting for reminder alerts, enter a value between 0 to 1200 seconds (inclusive) in the Hold Reversion Notification Interval (sec) field. Cisco Unified Communications Manager uses this timer to schedule periodic reminder alerts to the phone of the holding party for reverted calls. If you enter a 0, no reminder alerts get sent.

Step 3 Click the **Save** button.

Step 4 Reset any devices to incorporate changes in the Directory Number Configuration window.

Step 5 Repeat this procedure to configure additional timers.

What to do next

Additional Steps

In the Phone Configuration window, verify that the correct device pool is configured for the Cisco Unified IP Phone(s). If not, apply the correct device pool.

Provide Cisco Hold Reversion Information to Users

The Cisco Unified IP Phone user guides provide procedures for how to use the hold reversion feature. Some Cisco Unified IP Phones have a ? button, which displays help for more information.

Troubleshooting Cisco Hold Reversion

Use the Cisco Unified Serviceability Trace Configuration and Real Time Monitoring Tool to help troubleshoot hold reversion problems. See the *Cisco Unified Serviceability Administration Guide*.

CHAPTER 28

Hotline

This chapter provides information about the hotline feature which 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 hotline feature adds the additional restriction that hotline devices that receive calls will only receive calls from other hotline devices, and will reject non-hotline callers.

Hotline phones typically have a restricted feature set. You can restrict the features on a hotline phone by applying a softkey template to the phone. You can configure a hotline phone to originate calls only, terminate calls only, or originate and terminate calls.

Hotline uses route class signalling to allow hotline phones to receive calls only from other hotline phones. Hotline also provides configurable call screening based on caller ID, which allows a receiving hotline phone to screen calls and allow only callers in the screening list to connect.

Configure Hotline

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 hotline feature adds the additional restriction that hotline devices that receive calls will only receive calls from other hotline devices, and will reject non-hotline callers.

Hotline phones typically have a restricted feature set. You can restrict the features on a hotline phone by applying a softkey template to the phone. You can configure a hotline phone to originate calls only, terminate calls only, or originate and terminate calls.

Hotline uses route class signalling to allow hotline phones to receive calls only from other hotline phones. Hotline also provides configurable call screening based on caller ID, which allows a receiving hotline phone to screen calls and allow only callers in the screening list to connect.

Perform the following steps to configure hotline in your network.

Procedure

Step 1 Configure hotline service parameters.

Step 2 Configure PLAR, which makes a phone dial a preset number when it goes offhook.

Step 3 Check the Hotline Device check box in the Phone Configuration window.

Step 4 Configure translation patterns or route patterns to assign a route class to inbound T1 CAS calls and strip off the corresponding prefix digit.

Step 5 Configure the call and receive settings for the phone. This is only necessary if you want to restrict a hotline phone to only originating calls or only terminating calls.

Step 6 Create a softkey template that blocks unwanted features and apply it to the phone.

Step 7 Configure SIP trunks to support hotline by checking the Route Class Signaling Enabled check box.

Step 8 Configure MGCP PRI gateways to support hotline by checking the Route Class Signaling Enabled check box.

Step 9 Configure MGCP T1/CAS gateways to support hotline by checking the Route Class Signaling Enabled check box, and optionally, configure the Encode Voice Route Class parameter.

Step 10 Configure call screening based on caller ID.

Related Topics

Configure Service Parameters for Hotline, on page 634
Access Hotline Configuration in CUCM Administration, on page 637
Configure Phone Call and Receive Settings, on page 631
Configure Call Screening, on page 631

Hotline for CUCM Feature

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 gets 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 only receive calls 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 Signalling

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 with the same route class from a hotline phone.

You set the route class of a call by configuring route patterns or translation patterns.

Configurable Call Screening

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.

You configure the call screen setting on translation patterns.

Configure Phone Call and Receive Settings

You can configure a hotline phone to call only, receive only, or both call and receive. You configure this by using Calling Search Spaces (CSS) and partitions, as described in this example:

Procedure

Step 1 Create a CSS named NoRouteCSS, and two partitions named EmptyPartition and IsolatedPartition.

Step 2 Do not assign the EmptyPartition partition to any line.

Step 3 Configure the NoRouteCSS CSS to select only the EmptyPartition partition.

Step 4 Do not select the IsolatedPartition partition on any CSS window.

Step 5 To receive only, assign the NoRouteCSS CSS to the phone.

Step 6 To call only, assign the IsolatedPartition partition to the phone.

Configure Call Screening

This section describes the two methods to implement caller screening: using CCS and partitions, or using calling party number routing. You can screen calls to a terminating hotline phone such that only callers in a screening list are allowed to connect. You typically use this feature to allow a terminating hotline to receive calls from more than one originator (pair-protected) but less than every originator in the same class (non-pair protected).

Configure Call Screening with Calling Search Spaces and Partitions

For all intraswitched (line to line) hotline calls, you can configure call screening by managing the Calling Search Space (CSS) and partition configuration, as described in the following example:

Procedure

Step 1 Assign the terminating line to a partition to protect it.

Step 2 Create the screening list by including the terminating partition in only the CSSs of originating hotline phones that you want to allow to connect to the terminating hotline.

Configure Call Screening with Calling Party Number Routing

Because trunks are associated with more than one inbound/outbound phone, the CSS and partition method of call screening described in the Configure Call Screening with Calling Search Spaces and Partitions, on page

631 cannot be used to build per-DN screens. Cisco Unified Communications Manager can use the Calling Party Number to make routing decisions.

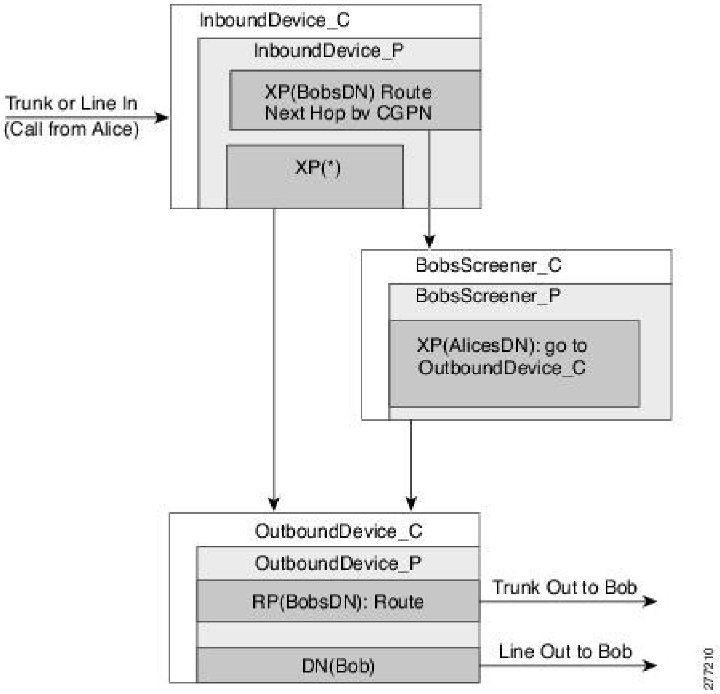
This call screening method can also be used for lines, but it is particularly useful for connection paths involving trunks such as the following:

Phone - PBX - Gateway - Cisco Unified Communications Manager - Gateway - PBX - Phone

If you cannot screen at the PBX, then this method allows you to screen for the PBX by using Cisco Unified Communications Manager.

The following figure and the description that follows illustrate this method.

Figure 54: Call Screening with Calling Party Number Routing



- InboundDevice_C is the inbound CSS for the trunk or line on which the call came in.
- InboundDevice_P is a partition that is a member of InboundDevice_C.
- XP(BobsDN) is a translation pattern that is a member of InboundDevice_P, which directs all calls to Bob's DN to go through Bob's screener. The check box Route Next Hop By Calling Party is checked in the translation pattern window. The CSS for the next hop is set to BobsScreener_C.

  For inbound PLAR lines, this pattern would match on blank and transform the blank called party to Bob's DN.
- XP(*) is a wildcard translation pattern for all inbound calls whose destination has no associated screen.
- BobsScreener_C and BobsScreener_P are the CSS and Partition, respectively, to hold calling party number screening patterns for Bob.
- XP(AlicesDN) is a translation pattern belonging to BobsScreener_P, representing a calling party (Alice) that needs to be allowed to connect. For these patterns, the CSS should be set to OutboundDevice_C.

- OutboundDevice_C, OutboundDevice_P, and DN(cdpnXxxx) or RP(cdpnXxxx) are all normal dial plan configurations to go out lines and trunks.

  Either the DN or the route pattern are part of the partition, but not both.

To build a screening list, create one translation pattern for each pattern that you want to allow through.

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.

Determine Device Support for Hotline

Use the Cisco Unified Reporting application to generate a complete list of devices that support hotline. To do so, follow these steps:

Procedure

Step 1 Start Cisco Unified Reporting by using any of the methods that follow. The system uses the Cisco Tomcat service to authenticate users before allowing access to the web application. You can access the application

- by choosing **Cisco Unified Reporting** in the Navigation menu in Cisco Unified Communications Manager Administration and clicking **Go.**
- by choosing **File** > **Cisco Unified Reporting** at the Cisco Unified Real Time Monitoring Tool (RTMT) menu.
- by entering `https://<server name or IP address>:8443/cucreports/` and then entering your authorized username and password.

Step 2 Click **System Reports** in the navigation bar.

Step 3 In the list of reports that displays in the left column, click the **Unified CM Phone Feature List** option.

Step 4 Click the Generate a new report link to generate a new report, or click the **Unified CM Phone Feature List** link if a report already exists.

Step 5 To generate a report of all devices that support hotline, choose these settings from the respective drop-down list boxes and click the **Submit** button:

Product: All

Feature: Hotline

The List Features pane displays a list of all devices that support the hotline feature. You can click on the Up and Down arrows next to the column headers (Product or Protocol) to sort the list.

What to do next

For additional information about the Cisco Unified Reporting application, see the *Cisco Unified Reporting Administration Guide*.

Install and Activate Hotline

After you install Cisco Unified Communications Manager, your network can support hotline if you perform the necessary configuration tasks. For information on configuration tasks that you must perform, see the Configure Hotline, on page 629.

Hotline Configuration

This section contains information to configure Hotline.

Tip Before you configure Hotline, review the summary task to configure this feature.

Related Topics

Configure Hotline, on page 629

Configure Service Parameters for Hotline

The following table describes the service parameters that you can configure for hotline. To configure service parameters in Cisco Unified Communications Manager Administration, choose **System** > **Service Parameters**.

All of these service parameters support the Cisco Unified Communications Manager service.

Tip For a step-by-step procedure on how to configure enterprise parameters, see the Cisco Unified Communications Manager Administration Guide. For a step-by-step procedure on how to configure service parameters, see the Cisco Unified Communications Manager Administration Guide.

Table 70: Enterprise and Service Parameters for Hotline

Parameter	Description
Route Class Trunk Signaling Enabled	This parameter determines whether Cisco Unified Communications Manager processes (inbound) and sends (outbound) route class signaling on trunks that support it. Route class trunk signaling enables interworking between IP and TDM switches that use route class. Set it to True to enable route class trunk signaling, or to False to disable it. This field is required. The default equals True.
SIP Satellite Avoidance Route Class Label	This parameter specifies a label representing the Satellite Avoidance route class in SIP signaling, as defined by the owner of the domain name specified in the SIP Route Class Naming Authority service parameter. Cisco Unified Communications Manager combines the value in this parameter with the value in the SIP Route Class Naming Authority parameter to create the complete signaling syntax for the SIP satellite avoidance route class value. This label proves useful when interworking with TDM networks that make routing decisions based on satellite avoidance route class. You can change this parameter based on your own vendor- specific or deployment-specific requirements. Make certain that the far-end switch expects to receive the same value that you configure in this parameter. See the help text for the service parameter SIP Route Class Naming Authority for additional information pertinent to this parameter. The following rules apply to values that you specify for this parameter: • Maximum of 64 characters. • Only alphanumeric (A-Z, a-z,0-9) or dash (-) characters are allowed. • Dashes are only allowed between alphanumeric characters. This field is required and hidden. The default equals nosat. The hotline feature does not use this parameter. It supports other route class features.

Parameter	Description
SIP Hotline Voice Route Class Label	This parameter specifies a label representing the Hotline Voice route class in SIP signaling, as defined by the owner of the domain name specified in the SIP Route Class Naming Authority service parameter. Cisco Unified Communications Manager combines the value in this parameter with the value in the SIP Route Class Naming Authority parameter to create the complete signaling syntax for the SIP Hotline Voice route class value. This label proves useful when interworking with TDM networks that make routing decisions based on Hotline Voice route class. You can change this parameter based on your own vendor-specific or deployment-specific requirements. Make certain that the far-end switch expects to receive the same value that you configure in this parameter. See the help text for the service parameter SIP Route Class Naming Authority for additional information pertinent to this parameter. The following rules apply to values that you specify for this parameter: • Maximum of 64 characters. • Only alphanumeric (A-Z, a-z,0-9) or dash (-) characters are allowed. • Dashes are only allowed between alphanumeric characters. This field is required. The default equals hotline.

Parameter	Description
SIP Hotline Data Route Class Label	This parameter specifies a label representing the Hotline Data route class in SIP signaling, as defined by the owner of the domain name specified in the SIP Route Class Naming Authority service parameter. Cisco Unified Communications Manager combines the value in this parameter with the value in the SIP Route Class Naming Authority parameter to create the complete signaling syntax for the SIP Hotline Data route class value. This label proves useful when interworking with TDM networks that make routing decisions based on Hotline Data route class. You can change this parameter based on your own vendor-specific or deployment-specific requirements. Make certain that the far-end switch expects to receive the same value that you configure in this parameter. See the help text for the service parameter SIP Route Class Naming Authority for additional information pertinent to this parameter. • The following rules apply to values that you specify for this parameter: • Maximum of 64 characters. • Only alphanumeric (A-Z, a-z,0-9) or dash (-) characters are allowed. • Dashes are only allowed between alphanumeric characters. This field is required. The default equals hotline-ccdata.

Access Hotline Configuration in CUCM Administration

The following table describes the hotline configuration settings in Cisco Unified Communications Manager Administration, except for hotline service parameters, which are described in Configure Service Parameters for Hotline, on page 634. For additional information, see topics related to configuring a trunk in the *Cisco Unified Communications Manager Administration Guide*.

Configuration Setting	Description
Device > Phone	

Configuration Setting	Description
Hotline Device	Check this check box to make this device a hotline device. Hotline devices that receive calls will only receive calls from other hotline devices, and will reject non-hotline callers. This feature is an extension of PLAR, which configures a phone to automatically dial one directory number when it goes off-hook. Hotline provides additional restrictions that you can apply to devices that use PLAR. To implement hotline, you must also create a softkey template without supplementary service softkeys, and apply it to the hotline device.
Device > **Trunk**	
Route Class Signaling Enabled	From the drop-down list, enable or disable route class signaling for the port. Choose one of the following values: • Default - If you choose this value, the device uses the setting from the Route Class Signaling service parameter. • Off - Choose this value to enable route class signaling. This setting overrides the Route Class Signaling service parameter. • On - Choose this value to disable route class signaling. This setting overrides the Route Class Signaling service parameter. Route class signaling communicates special routing or termination requirements to receiving devices. It must be enabled for the port to support the hotline feature. This parameter is available on SIP trunks.
Device > **Gateway**	

Configuration Setting	Description
Route Class Signaling Enabled	From the drop-down list, enable or disable route class signaling for the port. Choose one of the following values: • Default - If you choose this value, the device uses the setting from the Route Class Signaling service parameter. • Off - Choose this value to enable route class signaling. This setting overrides the Route Class Signaling service parameter. • On - Choose this value to disable route class signaling. This setting overrides the Route Class Signaling service parameter. Route class signaling communicates special routing or termination requirements to receiving devices. It must be enabled for the port to support the hotline feature. This parameter is available on MGCP PRI and T1/CAS gateway ports.
Encode Voice Route Class	Check this check box to encode voice route class for voice calls. Because voice is the default route class, it typically does not need explicit encoding. If this is disabled (the default setting), the port will not explicitly encode the voice route class. The voice route class (explicitly encoded or not) can get used by downstream devices to identify a call as voice. This parameter is available on MGCP T1/CAS gateway ports
Call Routing > **Route/Hunt** > **Route Pattern**	

Configuration Setting	Description
Route Class	Choose a route class setting for this route pattern from the drop-down list box: • Default • Voice • Data • Satellite Avoidance • Hotline voice • Hotline data The 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. The Default setting uses the existing route class of the incoming call. You should only use non-default route class settings to translate an inbound T1 CAS route class digit into a Cisco Unified Communications Manager route class value (and strip off the digit). You should not need to assign a non-default route class setting to any other inbound calls that use pattern configuration.
Call Routing > Translation Pattern	
Route Class	Choose a route class setting for this translation pattern from the drop-down list box: • Default • Voice • Data • Satellite Avoidance • Hotline voice • Hotline data The 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. The Default setting uses the existing route class of the incoming call. You can use non-default route class settings to translate an inbound T1 CAS route class digit into a Cisco Unified Communications Manager route class value (and strip off the digit). You should not need to assign a non-default route class setting to any other inbound calls that use pattern configuration. If the route pattern points to a SIP trunk supporting G.Clear, then specify Data or Hotline as the Route Class.

Configuration Setting	Description
Route Next Hop By Calling Party Number	Check this box to enable routing based on the calling party number, which is required for call screening based on caller ID information to work between clusters.
Device > **Device Settings** > **Softkey Template**	
	To configure SoftKey Templates that remove supplementary service softkeys from hotline phones.

Troubleshooting Hotline

For hotline troubleshooting information, see the Troubleshooting Guide for Cisco Unified Communications Manager.

CHAPTER 29

IM and Presence Service

You enableIM and Presence Service on Unified Communications Manager to give users instant messaging and availability capabilities. This feature allows administrators to:

- Easily enable end users for IM and availability from Unified Communications Manager via a single checkbox
- Set up unified communications (UC) services, such as voicemail, mailstore, conferencing, and CTI
- Set up service profiles for UC services
- Assign users to service profiles with specified UC services
- Select line appearances for users and enable them for presence
- Associate directory numbers and devices to a user from the **End User** setup window.

IM and Presence Installation Considerations

To add the IM and Presence service to your deployment, you must install and configure one or more IM and Presence servers when you install a Unified Communications Manager cluster.

To install an IM and Presence server, see the IM and Presence installation section in *Installing Cisco Unified Communications Manager*.

Upgrade

This section contains the steps to upgrade Unified Communications Manager and IM and Presence properly. Depending on your server setup, you can perform a standard or refresh upgrade.

Software version restrictions

Unified Communications Manager and IM and Presence Service software versions must have the same major and minor release number. Major and minor release numbers are defined as follows:

```
9.x.y
```

where `9` = major release number, `x` = minor release number and `y` = maintenance release number.

For example, IM and Presence Release 9.0.2.10000-4 is compatible with Unified Communications Manager Release 9.0.12.30000-2, but it is not compatible with Unified Communications Manager Release 9.1.1.10000-3. Similarly, Unified Communications Manager Release 8.6.2.10000-6 is not compatible with IM and Presence Release 9.0.1.10000-9.

The software version of subsequent IM and Presence nodes that you upgrade must match all five version numbers of the first IM and Presence node that you upgraded.

Note You cannot upgrade IM and Presence unless the upgraded release of Unified Communications Manager is already installed on the active or inactive partition. You must upgrade Unified Communications Manager before you can upgrade IM and Presence to the matching version.

Caution If you use Platform Administrative Web Services (PAWS) Management to upgrade IM and Presence, do not attempt to upgrade and reboot to the current IM and Presence release if the active partition on Unified CM is running an incompatible software version. If you do, the upgrade will fail, as expected, but the failure will not be reported until near the end of the upgrade process. You will also experience system downtime when the system reboots.

The delayed upgrade failure notification applies only to upgrades that are performed with PAWS Management. If you perform the upgrade through Cisco Unified IM and Presence Operating System Administration or through the CLI, the upgrade failure notification is displayed at the beginning of the upgrade.

Upgrade Order

Note The order in which you upgrade Unified Communications Manager and IM and Presence is very important.

Standard Upgrade Order

The following upgrade paths are standard upgrades:

- Unified Communications Manager Release 8.6.x to Unified Communications Manager Release 9.0(1)
- Cisco Unified Presence Release 8.6(4) to IM and Presence Service Release 9.0(1)

For standard upgrades, you must perform the upgrades in the following order:

1. Upgrade the Unified Communications Manager database publisher node.
2. Upgrade the IM and Presence database publisher node and the Unified CM subscriber nodes.

3. Upgrade the IM and Presence subscriber nodes.
4. Switch versions on the Unified Communications Manager database publisher node.
5. Switch versions on the IM and Presence database publisher node and Unified Communications Manager subscriber nodes.
6. Switch versions on the IM and Presence subscriber nodes.

Refresh Upgrade Order

The following upgrade paths are refresh upgrades:

- Unified Communications Manager Release 8.5 and earlier to Unified Communications Manager Release 9.0(1)
- Cisco Unified Presence Release 8.6(3) and earlier to IM and Presence Service Release 9.0(1)

For refresh upgrades, you must perform the upgrades in the following order:

1. Upgrade the Unified Communications Manager database publisher node
2. Switch versions on the Unified Communications Manager database publisher node.
3. Upgrade the IM and Presence database publisher node and the Unified Communications Manager subscriber nodes.
4. Switch versions on the IM and Presence database publisher node and Unified Communications Manager subscriber nodes.
5. Upgrade the IM and Presence subscriber nodes.
6. Switch versions on the IM and Presence subscriber nodes.

Note Refresh upgrades for Unified Communications Manager are described in the topic “Software upgrade process overview” in the *Upgrade Guide for Cisco Unified Communications Manager*.

IM and Presence for End Users

When you set up IM and Presence in Cisco Unified Communications Manager Administration, you enable presence capability for an end user, which includes presence licensing, the provisioning of UC services and service profiles that are assigned to the end user.

After you set up the servers, you must complete the following tasks:

1. Enable the IM and Presence service for end users in Cisco Unified Communications Manager:
    - For a pre-existing user, from the end user configuration window: **User Management** > **End User**
    - From the Bulk Administration Tool (BAT):
        - For a set of pre-existing users from **Bulk Administration** > **Users** > **Update Users**

  - For new users inserted via BAT from **Bulk Administration** > **Users** > **User Template**, then **Bulk Administration** > **Users** > **Insert Users**

- The Bulk Administration Tool, for administering multiple users: **Bulk Administration** > **Users** > **User Template**
- A feature group template: **User Management** > **User/Phone Add** > **Feature Group Templates**

Note You assign an IM and Presence configured feature group template to a user via the quick user/phone add window: **User Management** > **User/Phone Add** > **Quick User/Phone Add**

2. Create a UC service for IM and Presence, and include that UC service in either the system-wide default service profile you created, or in other service profiles that are individually associated to end users.

For more information about how to configure end users for IM and Presence, see the UC Services and Service Profiles sections in *Cisco Unified Communications Manager Administration Guide*.

Presence Viewer for End Users

Use the Presence Viewer to view the availability status of a user in IM and Presence Service, and to view the list of contacts and watchers that are configured for that user.

Access the Presence Viewer from an end-user configuration record using Cisco Unified Communications Manager Administration when IM and Presence Service is enabled for that user. For more information, see topics related to enablingIM and Presence Service for a user.

The user must be assigned to an IM and Presence Service node for valid presence information to be available. The AXL, Presence Engine, and Proxy Service must all be running on the IM and Presence Service node for this feature to be functional.

The following table lists the fields that are displayed on the Presence Viewer for the selected end user in Cisco Unified Communications Manager Administration

Table 71: End User Presence Viewer Fields

Presence Setting	Description
User Status	Identifies the availability state of the user, including: • Available • Away • Do Not Disturb • Unavailable • Custom
User ID	Identifies the selected user ID. A user photo is displayed if one is available for that user. You can click **Submit** to choose a different User ID.

Presence Setting	Description
View From Perspective of	Specifies a user to see the availability status from the perspective of the user. This allows you to determine how the availability status of a specified user appears to another user, known as a watcher. This functionality is useful in debugging scenarios, for example, where a user has configured privacy policies. A maximum of 128 characters is allowed.
Contacts	Displays the number of contacts in the contact list for this user. Click the arrow beside the Contacts heading in the Contacts and Watchers list area to view the availability status of a specific user contact. Click the arrow beside the group name to expand the list of contacts within that group. Contacts that are not part of a group (groupless contacts) display below the contact group list. A contact may belong to multiple groups, but will only count once against the contact list size for that user. A warning message appears if the maximum number of contacts configured for end users is exceeded. For more information about IM and Presence Service configuration and the maximum contacts setting, see the *IM and Presence Administration Online Help*.
Watchers	Displays a list of users, known as watchers, who have subscribed to see the availability status of this user in their contact list. Click the arrow beside the Watchers heading in the Contacts and Watchers list area to view the availability status of a specific watcher. Click the arrow beside the group name to expand the list of watchers within that group. A watcher may belong to multiple groups but will only count once against the watcher list size for that user. A warning message appears if the maximum number of watchers configured for end users is exceeded. For more information about IM and Presence Service configuration and the maximum watchers setting, see the *IM and Presence Administration Online Help*.
Presence Server Assignment	Identifies the IM and Presence Service server to which the user is assigned. Hyperlinks allow you to go directly to the server configuration page for details.
Enable accessible presence icons	Select this check box to enable presence accessibility icons for this end user.
Submit	Select to run the Presence Viewer. The user must be assigned to an IM and Presence node for valid presence information to be available. The AXL, Presence Engine and Proxy Service must all be running on the IM and Presence server for this action to be functional.

Display Presence Viewer for End Users

Use Cisco Unified Communications Manager Administration to display the Presence Viewer for an end user.

Before you begin

The end user must be on the home cluster and have IM and Presence enabled.

Ensure that an Exchange Presence Gateway is configured on the Cisco Unified Communications Manager IM and Presence Service server.

Procedure

Step 1 Select **User Management** > **End User** to find the end user.

The End User Configuration window displays.

Step 2 Click the **Presence Viewer for User** link in the Service Settings area.

Note The Presence Viewer for User link will display only if the Home Cluster and Enable User for Unified CM IM and Presence check boxes are checked.

The Presence Viewer displays.

Directory UC Services for Presence

Cisco Unified Communications Manager allows you to set up the directory UC service and service profile. You use this feature for directory search presence and contact add functionality from the IM and Presence-enabled clients.

There are three directory options:

User data service (UDS)

User data service is a service that provide access to user informatin stored in the Cisco Unified Communications Manager back-end storage. You can access this directory option from the **User Management** > **User Settings** > **Service Profile** menu path.

Enhanced Directory UC service

Enhanced Directory is a product type for the Directory UC service that is used when a client is able to determine directory setup and mappings from the desktop device by default.

Note If the defaults need to be changed, then a customer TFTP file must be loaded on Cisco Unified Communications Manager. See more information in the Cisco Jabber for Windows documentation.

Basic Directory UC service

Basic Directory is a product type for the Directory UC service where all of the Lightway Directory Access Protocol (LDAP) attribute mappings settings must be specified on the server for the client to download and use.

Note These mappings are specified on the IM and Presence Administration GUI under **Application** > **Legacy Clients** > **Settings**.

Tip Because Cisco clients support various directory UC services, Cisco recommends that you set up all three of the directory services in a single service profile.

Note Cisco Jabber for Windows clients can use UDS or another LDAP directory such as Enhanced Directory. Enhanced Directory is the default, and in most cases is the best option for directory integration. For more information, see the Cisco Jabber for Windows documentation.

Note UDS is not currently recommended in multi-cluster deployments that do not have the full enterprise list of users in the database of each cluster.

Presence Redundancy Groups and High Availability

A presence redundancy group is comprised of two IM and Presence Service nodes from the same cluster and provides both redundancy and recovery for IM and Presence Service clients and applications. Use **Cisco Unified CM Administration** to assign nodes to a presence redundancy group and to enable high availability.

- Failover - Occurs in a presence redundancy group when one or more critical services fails on an IM and Presence Service node in the group or a node in the group fails. Clients automatically connect to the other IM and Presence Service node in that group.
- Fallback - Occurs when a fallback command is issued from the Command Line Interface (CLI) or Cisco Unified Communications Manager during either of these conditions:
  - The failed IM and Presence Service node comes back into service and all critical services are running. The failed over clients in that group reconnect with the recovered node when it becomes available.
  - The backup activated IM and Presence Service node fails due to a critical service failure, and the peer node is in the Failed Over state and supports the automatic recovery fallback.

Automatic FallbackIM and Presence Service supports automatic fallback to the primary node after a failover. Automatic fallback is the process of moving users back to the primary node after a failover without manual intervention. You can enable automatic fallback with the Enable Automatic Fallback service parameter on the Cisco Unified CM IM and Presence Administration interface. Automatic fallback occurs in the following scenarios:

- A critical service on Node A fails—A critical service (for example, the Presence Engine) fails on Node A. Automatic failover occurs and all users are moved to Node B. Node A is in a state called “Failed Over with Critical Services Not Running”. When the critical service recovers, the node state changes to "Failed

Over." When this occurs Node B tracks the health of Node A for 30 minutes. If no heartbeat is missed in this timeframe and the state of each node remains unchanged, automatic fallback occurs.

- Node A is rebooted—Automatic failover occurs and all users are moved to Node B. When Node A returns to a healthy state and remains in that state for 30 minutes automatic fallback will occur.
- Node A loses communications with Node B—Automatic failover occurs and all users are moved to Node B. When communications are re-established and remain unchanged for 30 minutes automatic fallback will occur.

If failover occurs for a reason other than one of the three scenarios listed here, you must recover the node manually. If you do not want to wait 30 minutes before the automatic fallback, you can perform a manual fallback to the primary node. For example: Using presence redundancy groups, Cisco Jabber clients will fail over to a backup IM and Presence Service node if the services or hardware fail on the local IM and Presence Service node. When the failed node comes online again, the clients automatically reconnect to the local IM and Presence Service node. When the failed node comes online, a manual fallback operation is required unless the automatic fallback option is set.

You can manually initiate a node failover, fallback, and recovery of IM and Presence Service nodes in the presence redundancy group. A manual fallback operation is required unless the automatic fallback option is set.

For instructions to set up presence redundancy groups and high availability, see *Cisco Unified Communications Manager Administration Guide*.

Cisco Server Recovery Manager

The Cisco Server Recovery Manager (SRM) on IM and Presence Service manages the failover between nodes in a presence redundancy group. The Cisco Server Recovery Manager manages all state changes in a node; state changes are either automatic or initiated by the administrator (manual).

When you enable high availability for a presence redundancy group, the IM and Presence node restarts the Cisco Service Recovery Manager (SRM), which establishes heartbeat connections with the peer node, and begins to monitor critical processes. To verify that this service is running, select **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Network Services**

The SRM does not allow the critical services to be started on an “Idle” node. This only applies to a manual failover. If you attempt to start one of the critical services, the service state transitions from “Starting” to “Started” to “Stopped”. You can (re)start services to fix the failure in an automatic failover.

The SRM is responsible for monitoring conditions that can cause a failover and for setting the failover state of each node. Failover can occur due to the following events:

- An administrator initiates a manual failover.
- A node in the presence redundancy group fails and an automatic failover occurs.
- A critical service on one node in the presence redundancy group stops and fails to recover, and an automatic failover occurs.

The SRM on the peer node performs the user failover operation, not the SRM on the failed node. For example, if node A fails, the SRM on node B updates the node status and automatic failover initiates. If the SRM is not turned on, it does not monitor any critical processes, nor does it monitor the heartbeat connections with the peer node.

Before you enable high availability in a presence redundancy group, you must configure the SRM service parameters to properly reflect your deployment. See the *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.

Presence Redundancy Group Interactions and Limitations

Consider the following when configuring presence redundancy groups using **Cisco Unified CM Administration**:

- Each presence redundancy group requires at least one IM and Presence Service node assigned to it, and each can support up to two IM and Presence Service nodes.
- An IM and Presence Service node can be assigned to only one presence redundancy group.
- Both nodes in the presence redundancy group must be running the same version of IM and Presence Service software.
- Both nodes in the presence redundancy group must be on the same cluster and have the same IM and Presence Service database publisher node.
- The IM and Presence node does not need to be collocated with the Cisco Unified Communications Manager publisher node.
- For WAN deployments, a minimum of 10 megabits per second of dedicated bandwidth is required for each IM and Presence cluster, with no more than an 80 millisecond round-trip latency. Any bandwidth less than this recommendation can adversely impact performance.
- The Cisco Jabber client can be either local or remote to the IM and Presence Service node.

Balanced High Availability and Presence Redundancy Groups

Balanced high availability is achieved when you evenly distribute users across all nodes in the cluster and only use up to 35% of the CPU of each IM and Presence Service server. A balanced high-availability deployment supports up to 15,000 users per redundancy group and up to three redundancy groups per cluster for a total maximum of 45,000 users in a cluster with high-availability. For example, if you have six IM and Presence Service nodes in your cluster and 45,000 users, you assign 7.5 thousand users to each node. Using Cisco Unified Communications Manager Administration, you can either manually assign users to different nodes or initiate automatic rebalancing of user assignments across all nodes in the cluster for optimum load balancing.

For presence redundancy groups in a balanced high-availability deployment, it is recommended that you assign only half the number of users to each node in the presence redundancy group. If one node fails, the other node can handle the full load of the additional 50% of users, even at peak traffic.

High availability is provided at the system level. As such, the Cisco Sync Agent for IM and Presence Service may still have a single point of failure.

Failover Impacts

The IM and Presence Service supports high availability for Cisco Unified Personal Communicator Release 8.5(x) and later. Prior to Release 10.0(x), the Cisco Unified IM and Presence Administration GUI was used to configure high availability on IM and Presence Service. As of Release 10.0(x), the Cisco Unified Communications Manager Administration is used to configure high availability for IM and Presence Service.

During failover to the backup node, availability and instant messaging services are temporarily unavailable on client applications. After failover is complete, the availability and instant messaging services become available on the client again when the client signs back in. Similarly, if fallback occurs, availability and instant messaging services are temporarily unavailable on client applications until fallback completes and the client signs back in. IM and Presence Service clients are signed back in automatically.

The impact of failover on temporary adhoc chat messages depends on the particular client application. On Cisco Unified Personal Communicator, any ad hoc chat windows that were open before failover should display again after the failover is complete. However, if all of the users in a chat room automatically exit the chat room as part of a failover or fallback process, or if the ad hoc chat room is hosted on a failed node, the ad hoc chat windows will not display again after failover and a message is displayed explaining that the chat room was deleted. On all clients, any persistent chat rooms that users create on the failed node cannot be accessed again until recovery.

If the IM and Presence Service client is operating in softphone mode (the user is on a voice call) during failover, the voice call is not disconnected.

When failover occurs, the Intercluster Sync Agent is responsible for communicating the user move information to other clusters. The Intercluster Sync Agent runs on the IM and Presence Service database publisher node and on the IM and Presence Service subscriber nodes in the cluster. For more information about high-availability deployment models for IM and Presence Service, see the *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.

Node State Definitions

Table 72: Presence Redundancy Group Node State Definitions

State	Description
Initializing	This is the initial (transition) state when the Cisco Server Recovery Manager service starts; it is a temporary state.
Idle	IM and Presence Service is in Idle state when failover occurs and services are stopped. In Idle state, the IM and Presence Service node does not provide any availability or Instant Messaging services. In Idle state, you can manually initiate a fallback to this node using the **Cisco Unified CM Administration** user interface.
Normal	This is a stable state. The IM and Presence Service node is operating normally. In this state, you can manually initiate a failover to this node using the **Cisco Unified CM Administration** user interface.
Running in Backup Mode	This is a stable state. The IM and Presence Service node is acting as the backup for its peer node. Users have moved to this (backup) node.
Taking Over	This is a transition state. The IM and Presence Service node is taking over for its peer node.
Failing Over	This is a transition state. The IM and Presence Service node is being taken over by its peer node.
Failed Over	This is a steady state. The IM and Presence Service node has failed over, but no critical services are down. In this state, you can manually initiate a fallback to this node using the **Cisco Unified CM Administration** user interface.

State	Description
Failed Over with Critical Services Not Running	This is a steady state. Some of the critical services on the IM and Presence Service node have either stopped or failed.
Falling Back	This is a transition state. The system is falling back to this IM and Presence Service node from the node that is running in backup mode.
Taking Back	This is a transition state. The failed IM and Presence Service node is taking back over from its peer.
Running in Failed Mode	An error occurs during the transition states or Running in Backup Mode state.
Unknown	Node state is unknown. A possible cause is that high availability was not enabled properly on the IM and Presence Service node. Restart the Server Recovery Manager service on both nodes in the presence redundancy group.

Node States, Causes, and Recommended Actions

You can view the status of nodes in a presence redundancy group on the **Presence Redundancy Group Configuration** window when you choose a group using the **Cisco Unified CM Administration** user interface.

Table 73: Presence Redundancy Group Node High-Availability States, Causes, and Recommended Actions

Node 1		Node 2		
State	**Reason**	**State**	**Reason**	**Cause/Recommended Actions**
Normal	Normal	Normal	Normal	Normal
Failing Over	On Admin Request	Taking Over	On Admin Request	The administrator initiated a manual failover from node 1 to node 2. The manual failover is in progress.
Idle	On Admin Request	Running in Backup Mode	On Admin Request	The manual failover from node 1 to node 2 that the administrator initiated is complete.
Taking Back	On Admin Request	Falling Back	On Admin Request	The administrator initiated a manual fallback from node 2 to node 1. The manual fallback is in progress.
Idle	Initialization	Running in Backup Mode	On Admin Request	The administrator restarts the SRM service on node 1 while node 1 is in “Idle” state.
Idle	Initialization	Running in Backup Mode	Initialization	The administrator either restarts both nodes in the presence redundancy group, or restarts the SRM service on both nodes while the presence redundancy group was in manual failover mode.

Node 1		Node 2		
State	**Reason**	**State**	**Reason**	**Cause/Recommended Actions**
Idle	On Admin Request	Running in Backup Mode	Initialization	The administrator restarts the SRM service on node 2 while node 2 is running in backup mode, but before the heartbeat on node 1 times out.
Failing Over	On Admin Request	Taking Over	Initialization	The administrator restarts the SRM service on node 2 while node 2 is taking over, but before the heartbeat on node1 times out.
Taking Back	Initialization	Falling Back	On Admin Request	The administrator restarts the SRM service on node 1 while taking back, but before the heartbeat on node 2 times out. After the taking back process is complete, both nodes are in Normal state.
Taking Back	Automatic Fallback	Falling Back	Automatic Fallback	Automatic Fallback has been initiated from node 2 to node 1 and is currently in progress.
Failed Over	Initialization or Critical Services Down	Running in Backup Mode	Critical Service Down	Node 1 transitions to Failed Over state when either of the following conditions occur: • Critical services come back up due to a reboot of node 1. • The administrator starts critical services on node 1 while node 1 is in Failed Over with Critical Services Not Running state. When node 1 transitions to Failed Over state the node is ready for the administrator to perform a manual fallback to restore the nodes in the presence redundancy group to Normal state.
Failed Over with Critical Services not Running	Critical Service Down	Running in Backup Mode	Critical Service Down	A critical service is down on node 1. IM and Presence Service performs an automatic failover to node 2. **Recommended Actions:** **1.** Check node 1 for any critical services that are down and try to manually start those services. **2.** If the critical services on node 1 do not start, then reboot node 1. **3.** When all the critical services are up and running after the reboot, perform a manual fallback to restore the nodes in the presence redundancy group to the Normal state.

Node 1		Node 2		
State	**Reason**	**State**	**Reason**	**Cause/Recommended Actions**
Failed Over with Critical Services not Running	Database Failure	Running in Backup Mode	Database Failure	A database service is down on node 1. IM and Presence Service performs an automatic failover to node 2. **Recommended Actions:** **1.** Reboot node 1. **2.** When all the critical services are up and running after the reboot, perform a manual fallback to restore the nodes in the presence redundancy group to the Normal state.
Running in Failed Mode	Start of Critical Services Failed	Running in Failed Mode	Start of Critical Services Failed	Critical services fail to start while a node in the presence redundancy group is taking back from the other node. **Recommended Actions.** On the node that is taking back, perform the following actions: **1.** Check the node for critical services that are down. To manually start these services, click **Recovery** in the **Presence Redundancy Group Configuration** window. **2.** If the critical services do not start, reboot the node. **3.** When all the critical services are up and running after the reboot, perform a manual fallback to restore the nodes in the presence redundancy group to the Normal state.
Running in Failed Mode	Critical Service Down	Running in Failed Mode	Critical Service Down	Critical services go down on the backup node. Both nodes enter the failed state. **Recommended Actions:** **1.** Check the backup node for critical services that are down. To start these services manually, click **Recovery** in the **Presence Redundancy Group Configuration** window. **2.** If the critical services do not start, reboot the node.

Node 1		Node 2		
State	**Reason**	**State**	**Reason**	**Cause/Recommended Actions**
Node 1 is down due to loss of network connectivity or the SRM service is not running.		Running in Backup Mode	Peer Down	Node 2 has lost the heartbeat from node 1. IM and Presence Service performs an automatic failover to node 2. **Recommended Action.** If node 1 is up, perform the following actions: **1.** Check and repair the network connectivity between nodes in the presence redundancy group. When you reestablish the network connection between the nodes, the node may go into a failed state. Click **Recovery** in the **Presence Redundancy Group Configuration** window to restore the nodes to the Normal state. **2.** Start the SRM service and perform a manual fallback to restore the nodes in the presence redundancy group to the Normal state. **3.** (If the node is down) Repair and power up node 1. **4.** When the node is up and all critical services are running, perform a manual fallback to restore the nodes in the presence redundancy group to the Normal state.
Node 1 is down (due to possible power down, hardware failure, shutdown, reboot)		Running in Backup Mode	Peer Reboot	IM and Presence Service performs an automatic failover to node 2 due to the following possible conditions on node 1: • hardware failure • power down • restart • shutdown **Recommended Actions:** **1.** Repair and power up node 1. **2.** When the node is up and all critical services are running, perform a manual fallback to restore the nodes in the presence redundancy group to the Normal state.

Node 1		Node 2		
State	**Reason**	**State**	**Reason**	**Cause/Recommended Actions**
Failed Over with Critical Services not Running OR Failed Over	Initialization	Backup Mode	Peer Down During Initialization	Node 2 does not see node 1 during startup. **Recommended Action:** When node1 is up and all critical services are running, perform a manual fallback to restore the nodes in the presence redundancy group to the Normal state.
Running in Failed Mode	Cisco Server Recovery Manager Take Over Users Failed	Running in Failed Mode	Cisco Server Recovery Manager Take Over Users Failed	User move fails during the taking over process. **Recommended Action:** Possible database error. Click **Recovery** in the **Presence Redundancy Group Configuration** window. If the problem persists, then reboot the nodes.
Running in Failed Mode	Cisco Server Recovery Manager Take Back Users Failed	Running in Failed Mode	Cisco Server Recovery Manager Take Back Users Failed	User move fails during falling back process. **Recommended Action:** Possible database error. Click **Recovery** in the **Presence Redundancy Group Configuration** window. If the problem persists, then reboot the nodes.
Running in Failed Mode	Unknown	Running in Failed Mode	Unknown	The SRM on a node restarts while the SRM on the other node is in a failed state, or an internal system error occurs. **Recommended Action:** Click **Recovery** in the **Presence Redundancy Group Configuration** window. If the problem persists, then reboot the nodes.
Backup Activated	Auto Recover Database Failure	Failover Affected Services	Auto Recovery Database Failure.	The database goes down on the backup node. The peer node is in failover mode and can take over for all users in the presence redundancy group. Auto-recovery operation automatically occurs and all users are moved over to the primary node.
Backup Activated	Auto Recover Database Failure	Failover Affected Services	Auto Recover Critical Service Down	A critical service goes down on the backup node. The peer node is in failover mode and can take over for all users in the presence redundancy group. Auto-recovery operation automatically occurs and all users are moved over to the peer node.

Node 1		Node 2		
State	Reason	State	Reason	Cause/Recommended Actions
Unknown		Unknown		Node state is unknown. A possible cause is that high availability was not enabled properly on the IM and Presence Service node. **Recommended Action:** Restart the Server Recovery Manager service on both nodes in the presence redundancy group.

IM and Presence Service High-Availability Setup

Use Cisco Unified Communications Manager Administration to set up a presence redundancy group consisting of two IM and Presence Service nodes and enable high availability. Nodes within the presence redundancy group that have high availability enabled perform an automatic failover and fallback procedure if one of the nodes fail.

You can also perform a manual failover, fallback, and recovery of nodes within a presence redundancy group using Cisco Unified Communications Manager Administration. As well, you can view the current node status and assigned users for each of the nodes within the group.

Enable or Disable High Availability

Use the **Cisco Unified CM Administration** user interface to enable or disable high availability for a presence redundancy group that has two IM and Presence Service nodes assigned. You must manually enable high availability for the presence redundancy group to operate in a high availability capacity.

⚠

Caution Disabling high availability for a presence redundancy group removes failover protection for users on those IM and Presence Service nodes.

Before you begin

- Enable high availability for a presence redundancy group only if replication is setup in the IM and Presence Service cluster and all critical services are running.
- Make sure critical services are running on at least one node in the presence redundancy group before you turn on high availability in a presence redundancy group. If critical services are not running on either node, the presence redundancy group will go into a Failed state when you turn on high availability. If critical services are only down on one node, then that node fails over to the other node when you turn on high availability. For more information about the critical services for specific deployments, see the *Cisco Unified Communications Manager Administration Guide* (on Cisco.com).
- You can turn off high availability in a presence redundancy group so that the two nodes in the presence redundancy group act as standalone nodes. If you turn off high availability in a presence redundancy group when either node is in a failed over scenario (Failed Over, Failed), users on the failed node are

homed to the backup node. IM and Presence Service does not move these users to the primary node; they remain on the backup node.

- See the *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager* for more information about setting up IM and Presence Service nodes and stopping or starting critical services.

Caution Failure to set up replication in the IM and Presence Service cluster and ensure that all critical services are running may result in an immediate failover when high availability is enabled for the presence redundancy group.

Procedure

Step 1 Choose **System** > **Presence Redundancy Groups**.

The **Find and List Presence Redundancy Groups** window displays.

Step 2 Choose the presence redundancy group search parameters, and then click **Find**.

Matching records appear.

Step 3 Choose the presence redundancy group that is listed in the **Find and List Presence Redundancy Group** window.

The **Presence Redundancy Group Configuration** window appears.

Step 4 Perform one of the following actions:

a) To enable high availability, check the **Enable High Availability** check box.
b) To disable high availability, uncheck the **Enable High Availability** check box.

Step 5 Click **Save**.

Manual Failover, Fallback, and Recovery

Use Cisco Unified Communications Manager Administration to initiate a manual failover, fallback, and recovery for IM and Presence Service nodes in a presence redundancy group. You can also initiate these actions from Cisco Unified Communications Manager or IM and Presence Service using the CLI. See the *Command Line Interface Guide for Cisco Unified Communications Solutions* for details.

- Manual failover: When you initiate a manual failover, the Cisco Server Recovery Manager stops the critical services on the failed node. All users from the failed node are disconnected and must re-login to the backup node.

  Note After a manual failover occurs, critical services will not be started unless we invoke manual fallback.

- Manual fallback: When you initiate a manual fallback, the Cisco Server Recovery Manager restarts critical services on the primary node and disconnects all users that had been failed over. Those users must then re-login to their assigned node.
- Manual recovery: When both nodes in the presence redundancy group are in a failed state and you initiate a manual recovery, the IM and Presence Service restarts the Cisco Server Recovery Manager service on both nodes in the presence redundancy group.

Initiate Manual Failover

You can manually initiate a failover of IM and Presence Service nodes in a presence redundancy group using Cisco Unified Communications Manager Administration.

Procedure

Step 1 Select **System** > **Presence Redundancy Groups**.

The **Find and List Presence Redundancy Groups** window displays.

Step 2 Select the presence redundancy group search parameters, and then click **Find**.

Matching records appear.

Step 3 Select the presence redundancy group that is listed in the **Find and List Presence Redundancy Group** window.

The **Presence Redundancy Group Configuration** window appears.

Step 4 Click **Failover** in the ServerAction field.

Note This button appears only when the server and presence redundancy group are in the correct states.

Initiate Manual Fallback

Use Cisco Unified Communications Manager Administration to manually initiate the fallback of an IM and Presence Service node in a presence redundancy group that has failed over. For more information about presence redundancy group node status, see topics related to node state, state change causes, and recommended actions.

Procedure

Step 1 Select **System** > **Presence Redundancy Groups**.

The **Find and List Presence Redundancy Groups** window displays.

Step 2 Select the presence redundancy group search parameters, and then click **Find**.

Matching records appear.

Step 3 Select the presence redundancy group that is listed in the **Find and List Presence Redundancy Group** window.

The **Presence Redundancy Group Configuration** window appears.

Step 4 Click **Fallback** in the ServerAction field.

Note This button appears only when the server and presence redundancy group are in the correct states.

Initiate Manual Recovery

A manual recovery is necessary when both nodes in the presence redundancy group are in the failed state. Use Cisco Unified Communications Manager Administration to manually initiate the recovery of IM and Presence Service nodes in a presence redundancy group that is in the failed state.

For more information about presence redundancy group node status, see topics related to node state, state change causes, and recommended actions.

Before you begin

A manual recovery is necessary when both nodes in the presence redundancy group are in the failed state. Use Cisco Unified Communications Manager Administration to manually initiate the recovery of IM and Presence Service nodes in a presence redundancy group that is in the failed state.

Procedure

Step 1 Select **System** > **Presence Redundancy Groups**.

The **Find and List Presence Redundancy Groups** window displays.

Step 2 Select the presence redundancy group search parameters, and then click **Find**.

Matching records appear.

Step 3 Select the presence redundancy group that is listed in the **Find and List Presence Redundancy Group** window.

The **Presence Redundancy Group Configuration** window appears.

Step 4 Click **Recover**.

Note This button appears only when the server and presence redundancy group are in the correct states.

Other IM And Presence Features

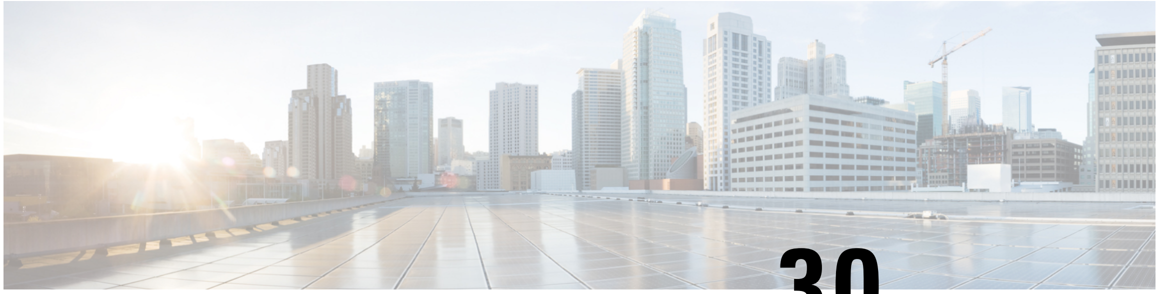
After IM and Presence Service is installed alongside Cisco Unified Communications Manager and end users are configured, end users with IM and availability-capable clients can sign in, create contact lists to see availability, get availability for users through directory search, and get integrated availability through Microsoft Outlook (depending on the client support).

Perform these actions to configure other IM and Presence Service features:

Table 74: Other IM And Presence Service Features

Action	Where to find more information
To enable the network-based phone availability for all devices to be reported for the user, you need to associate each line appearance with the user.	You can accomplish these tasks from the **End User** configuration window, under “Device Settings.” See “End user setup” in *Cisco Unified Communications Manager Administration Guide*
You must configure an IM and Presence Service publish trunk.	See "Cisco Unified Communications Manager configuration for integration with IM and Presence" in the *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*
For high availability of phone presence, you must also configure a Cisco Unified Communications Manager presence gateway in the IM and Presence Service node.	See “Cisco Unified Communications Manager configuration for integration with IM and Presence” in the *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*

For more information about other IM and Presence Service features, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager, Release 9.0(1)*.



CHAPTER 30

Immediate Divert

This chapter provides information about the Immediate Divert (iDivert) feature which allows you to immediately divert a call to a voice-messaging system. When the call gets diverted, the line becomes available to make or receive new calls.

Immediate Divert

This chapter provides information about the Immediate Divert (iDivert) feature which allows you to immediately divert a call to a voice-messaging system. When the call gets diverted, the line becomes available to make or receive new calls.

Configure Immediate Divert

The Immediate Divert (iDivert) feature allows you to immediately divert a call to a voice-messaging system. When the call gets diverted, the line becomes available to make or receive new calls.

Perform the following steps to configure immediate divert.

Procedure

Step 1 Change the Call Park Display Timer clusterwide service parameter if the default is not appropriate.

Step 2 Change the Use Legacy Immediate Divert clusterwide service parameter if the default is not appropriate.

Step 3 Change the Allow QSIG During iDivert clusterwide service parameter if the default is not appropriate.

Step 4 Change the iDivert User Response Timer service parameter if the default is not appropriate.

Step 5 In the Directory Number Configuration window, associate a voice-mail profile to each user who will have access to immediate divert.

Note This step assumes that voice-mail profiles and pilots are configured.

Step 6 Assign the iDivert softkey to the Standard User or Standard Feature softkey template. Assign the softkey in the On Hook, Connected, On Hold, and Ring In states. Cisco Unified IP Phones 8900 and 9900 series have the Divert softkey assigned by default.

Note The administrator assigns the iDivert softkey for the Cisco Unified IP Phone 6921, 6941, and 6961; however, the user sees Divert on the phone screen.

Step 7 In the Phone Configuration window, assign the Standard User or Standard Feature softkey template, to which you added the iDivert softkey, to each device that has immediate divert access.

Tip To make the iDivert softkey available to many users, configure a softkey template with the iDivert softkey; then, assign that softkey template to a device pool and, finally, assign that device pool to all users who need iDivert.

Step 8 Notify users that the immediate divert feature is available.

Related Topics

Set the Service Parameters for Immediate Divert, on page 672

Immediate Divert Feature

The Immediate Divert (iDivert or Divert softkeys) feature allows you to immediately divert a call to a voice-messaging system. When the call gets diverted, the line becomes available to make or receive new calls.

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.

Access the Immediate Divert feature by using the iDivert or Divert softkey. Configure this softkey by using the Softkey Template Configuration window of Cisco Unified Communications Manager Administration. The softkey template gets assigned to phones that are in the Cisco Unified Communications Manager system.

Consider immediate divert, a Cisco Unified Communications Manager supplementary service, as available for general use within the system. Immediate divert does not require the user to log in to make the iDivert or Divert softkey available on the phone.

You can divert inbound calls that are in the call offering, call on hold, or call active states. You can divert outbound calls in the call active or call hold states. The diverted party receives the greeting of the voice-messaging system of the party to whom the call gets diverted.

Legacy iDivert allows diversion of a call to the voice mailbox of the party that invokes the iDivert feature. Enhanced iDivert allows diversion of a call to either the voice mailbox of the party that invokes the iDivert feature or to the voice mailbox of the original called party.

When enhanced iDivert mode is active for incoming calls, the user to whom a call is presented can invoke immediate divert to divert the call either to the voice mailbox of the user or to the voice mailbox of the original called party. After the invoking user presses the iDivert softkey, a screen on the invoking user phone identifies both the original called party and the invoking user. The user selects one of the two names, and the call gets redirected to the voice mailbox of the selected party.

Note When users invoke the Immediate Divert feature to divert an incoming call, they receive the choice of the original called party only if the Use Legacy Immediate Divert clusterwide service parameter is set to False. See the Set the Service Parameters for Immediate Divert, on page 672.

System Requirements for Immediate Divert

Immediate divert requires the following software component to operate:

- Cisco Unified Communications Manager 6.0 or later
- The following table lists the phones that use the Divert or iDivert softkey

Table 75: Cisco Unified IP Phones That Use iDivert or 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

To find more information about Cisco Unified IP Phones and the Immediate Divert feature, see the user documentation for your phone model.

The following voice-messaging systems support immediate divert:

- Voice-messaging systems such as Unity that use the skinny protocol
- Voice-messaging systems such as Octel that use SMDI

Call-Processing Requirements for Immediate Divert

This section describes call-processing requirements for immediate divert.

Softkey Requirements

Because the iDivert softkey does not automatically get configured in a softkey template, use the Softkey Template Configuration window in Cisco Unified Communications Manager Administration to configure the iDivert softkey in any available softkey template. You can configure the iDivert softkey in the following call states:

- Connected
- On hold
- Ring in

Note The ring-in state in the softkey template represents the call-offering state in the phone call state.

Use the Phone Configuration window in Cisco Unified Communications Manager Administration to assign the softkey template that contains the iDivert softkey to a phone.

For information about softkey template configuration, see the Cisco Unified Communications Manager Administration Guide. For information about assigning softkey templates to phones, see the Cisco Unified Communications Manager Administration Guide.

Requirements for Incoming Calls

The following list gives called party types in the call-forwarding chain that immediate divert supports:

- Party A calls party B.
- Party B forwards to party C.
- Party C forwards to party D.

Party B represents the original called party. Party C represents the last redirecting party. Party D represents the last called party.

Immediate divert supports the following incoming call states:

- Call offering
- Call on hold
- Call active

When the called party presses the iDivert softkey and the Use Legacy Immediate Divert clusterwide service parameter is set to True, immediate divert redirects the incoming call to the voice-messaging mailbox that is associated with the called party. You can administer a voice-messaging mailbox for the called party through the voice-messaging profile that is assigned to the directory number of the called party.

When the called party presses the iDivert softkey and the Use Legacy Immediate Divert clusterwide service parameter is set to False, immediate divert may allow the called party to select the destination voice mailbox. A screen gets presented to the called party if the call had previously diverted (see the Interactions, on page 670). The called party can choose to divert the call to the voice-messaging mailbox of the original called party or to the voice-messaging mailbox that is associated with the called party, or the called party can cancel the divert that is in the iDivert menu. You may administer a voice-messaging mailbox for the original called party or for the called party through the voice-messaging profile that is assigned to the associated directory numbers.

For information about voice messaging, see the Cisco Unified Communications Manager Integration Guide for Cisco Unity Connection, Cisco Unified Communications Manager Administration Guide, and the Cisco Unified Communications Manager System Guide.

Requirements for Outgoing Calls

Immediate divert supports the following outgoing call states:

- Call on hold
- Call active

When the calling party presses the iDivert softkey, immediate divert redirects an outgoing call to the voice-messaging mailbox that is associated with the calling party. You may administer a voice-messaging mailbox for the calling party through the voice-messaging profile that is assigned to the directory number of the calling party.

For information about voice messaging, see the Cisco Unified Communications Manager Integration Guide for Cisco Unity Connection, Cisco Unified Communications Manager Administration Guide, and the Cisco Unified Communications Manager System Guide.

Immediate Divert Phone Display Messages

Immediate divert displays the following messages on the IP phone to indicate the status of an immediate divert action:

- Key is not active - The voice-messaging profile of the user who pressed iDivert does not have a voice-messaging pilot.
- Temporary failure - The voice-messaging system does not work, or a network problem exists.
- Busy - This message indicates that a voice-messaging system is busy.

Use Immediate Divert

The following scenarios provide examples of using the Immediate Divert feature.

Immediate Divert Scenarios with Use Legacy Immediate Divert Service Parameter Set to True

Scenario 1: Called Party Presses iDivert Softkey

1. Party A calls Manager A.
2. Manager A presses the iDivert softkey (call-offering state).
3. Immediate divert diverts the call to Manager A voice-messaging mailbox.
4. Party A receives the voice-messaging mailbox greeting of Manager A.

Scenario 2: Voice-Messaging Profile of an Original Called Party Does Not Have Voice-Messaging Pilot

1. Party A calls Party B.
2. The call gets forwarded to the personal line of Assistant B.
3. Assistant B presses the iDivert softkey (call-offering state).

4. Immediate divert diverts the call to Assistant B voice-messaging mailbox. Party B does not have a voice-messaging pilot number that is configured, but Assistant B does.
5. Party A receives the voice-messaging mailbox greeting of Assistant B.

Scenario 3: Manager A Forwards a Call to Manager B

1. Party A calls Manager A.
2. Manager A has line forwarded to Manager B.
3. Manager B presses the iDivert softkey (call-offering state).
4. Immediate divert diverts the call to Manager B voice-messaging mailbox.
5. Party A receives the voice-messaging mailbox greeting of Manager B.

Scenario 4: Voice-Messaging Port That Is Defined in a Voice-Messaging Profile is Busy

1. Party A calls Party B.
2. Party B presses the iDivert softkey (call offering state).
3. Immediate divert cannot divert the call to the voice-messaging mailbox because the voice-messaging port is busy.
4. Party B sees the message Busy on the IP phone.
5. The original call remains in the call-offering state.

Scenario 5: Calling Party Calls a Call Center That Uses a Hunt Pilot Number

1. Party A calls Hunt List A.
2. Hunt List A member presses the iDivert softkey (call offering state), which is greyed out.
3. Immediate divert cannot divert the call to the voice-messaging mailbox because Hunt List A does not have a voice-messaging profile.
4. Hunt List A member sees the Key is Not Active message on the IP phone.

Scenario 6: Calling Party B Transfers a Call to Party C on Different Cisco Unified Communications Manager Cluster

1. Party A calls Party B.
2. Party B transfers the call to Party C on a different Cisco Unified Communications Manager cluster.
3. Party C answers the incoming call.
4. Party C presses the iDivert softkey.
5. Party A receives the voice-messaging mailbox greeting of Party C.

Immediate Divert Scenarios with Use Legacy Immediate Divert Service Parameter Set to False

Scenario 7: Calling Party A Calls Party B, and Party B Forwards the Call to Party C

1. Party A calls Party B.
2. Party B phone forwards the call to Party C.
3. Party C gets presented with the incoming call and presses the iDivert softkey.
4. Party C presses the iDivert softkey.
5. Party C receives a screen that offers the choice of diverting to Party B voice-messaging mailbox or Party C voice-messaging mailbox.
6. Party C chooses the voice-messaging mailbox of Party B.
7. Party A receives the voice-messaging mailbox greeting of Party B.

Scenario 8: Calling Party Calls a Call Center That Uses a Hunt Pilot Number

1. Party A calls Hunt List A.
2. Hunt List A member presses the iDivert softkey (call offering state).
3. Immediate divert diverts the call to the voice-messaging mailbox of the hunt list A member that invokes the iDivert feature.
4. Party A receives the voice-messaging mailbox greeting of Hunt List A member.

Scenario 9: Auto Call Pickup Enabled Clusterwide Service Parameter is Set to False, and a User is in a Call Pickup Group

1. Party B, Party C, and Party D exist in the same call pickup group.
2. Party A calls Party B.
3. Party B IP phone rings but Party B does not answer the call.
4. Party C uses call pickup to answer the call.
5. If Party C presses the iDivert softkey during alerting state, connected state, or on hold state, the IP phone display gets presented to Party C. Party C can choose between two options: iDivert the call to the original called party voice-messaging mailbox (Party B) or iDivert the call to the last called party voice-messaging mailbox (Party C).

Note 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 a 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.

Interactions and Restrictions

This section describes the interactions and restrictions for immediate divert.

Interactions

This section describes how immediate divert interacts with Cisco Unified Communications Manager applications and call processing features.

Multilevel Precedence and Preemption (MLPP)

The following interactions occur between immediate divert and 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 solve this situation, set the CFNA timer service parameter to enough time (for example, 60 seconds). If the iDivert screen has been presented to the iDivert invoker and the CFNA timer expires, the call forwards onward.

Call Detail Records (CDR)

Immediate divert uses the immediate divert code number in the Onbehalf of fields (for example, joinOnbehalfOf and lastRedirectRediectOnBehalfOf) in CDR.

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

Immediate divert works as follows for DNs that are members of a line group:

- Ensure the iDivert softkey is enabled
- For calls that reach the phone directly through a hunt list pilot (as part of the hunting algorithms), the iDivert softkey will appear grayed out if the Use Legacy Immediate Divert clusterwide service parameter is set to True; otherwise, it does not appear grayed out.
- 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 grayed when the Use Legacy Immediate Divert clusterwide service

parameter is set to True or False. (This includes scenarios where a call was made to a hunt list pilot, the hunt list was exhausted, and the call followed the forwarding disposition to the DN that also happens to be a member of a hunt group. This would represent a case where a call reaches a member of a hunt group indirectly through a hunt list pilot.)

Restrictions

The following restrictions apply to immediate divert:

- Immediate divert supports 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. See the Set the Service Parameters for Immediate Divert, on page 672 for details. When iDivert is allowed over QSIG trunks, follow these guidelines: when you use QSIG integration with your voice-messaging system, a voice-mail profile that includes either a voice mail pilot or a voice mail 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.
- 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).
- When it reaches a voice-messaging system over a local/SCCP connection, iDivert can detect a busy condition on the voice-messaging ports. (The call cannot divert to a busy voice-messaging system, but the original call gets maintained. Busy will display on the phone on which iDivert was invoked to indicate that the call was not diverted.) When a voice-messaging 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 voice-messaging systems that can be reached over QSIG/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 voice-messaging systems over QSIG or SIP trunks. Immediate divert cannot divert a call to a busy voice-messaging port; however, voice-messaging ports can exist as members of a route/hunt list, thus reducing the busy port scenario.
- If the Use Legacy Immediate Divert clusterwide service parameter is set to True, members of a hunt list can invoke iDivert if the call is direct. They cannot invoke iDivert if they are reached as a member of a line group. The message, Key is Not Active, displays on the IP phone.
- When Cisco Unified Communications Manager goes down, users cannot leave voice messages unless a media path was established between a redirected party and the voice-messaging system before the Cisco Unified Communications Manager went down.
- System does not support using Malicious Caller ID and Immediate Divert features together.
- CTI applications do not have immediate divert available (applications use Transfer to Voicemail).
- Use the Call Park Display Timer service parameter to control the timer for the immediate divert text display on the IP phones. When the service parameter gets changed, the text display timer for immediate divert also gets changed.
- See the Multilevel Precedence and Preemption (MLPP), on page 670 for restrictions about using MLPP.
- A race condition in connection with the Forward No Answer Timeout exists when the iDivert softkey gets pressed. 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.

- The calling and called parties can divert the call to their voice-messaging mailboxes if both simultaneously press the iDivert softkey. The voice-messaging mailbox of the calling party would contain a portion of the outgoing greeting of the called party. Similarly, the voice-messaging mailbox of the called party would contain a portion of the outgoing greeting of the calling party.
- 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.
- 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-messaging mailbox. Instead, enhanced iDivert immediately diverts the call to the voice-messaging mailbox that is associated with the called party.
- When iDivert is allowed over QSIG trunks, follow these guidelines: when you use QSIG integration with your voice-messaging system, a voice mail profile that includes either a voice mail pilot or a voice mail 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 always gets set to No Voice Mail.

Install and Activate Immediate Divert

Immediate Divert, a system feature, comes standard with Cisco Unified Communications Manager software. Immediate divert does not require special installation.

Immediate Divert Configuration

This section contains information to configure immediate divert.

Tip Before you configure immediate divert, review the configuration summary task for this feature.

Related Topics

Configure Immediate Divert, on page 663

Set the Service Parameters for Immediate Divert

The behavior of the Immediate Divert feature depends on the setting for various service parameters. Descriptions of the service parameters that affect the Immediate Divert feature follow.

Call Park Display Timer Clusterwide Service Parameter

Immediate divert uses the Cisco Unified Communications Manager clusterwide service parameter Call Park Display Timer. The default for this service parameter specifies 10 seconds. Use the Call Park Display Timer service parameter to control the timer for the immediate divert text display on the IP phones. When the service parameter gets changed, the text display timer for immediate divert also changes. Set this timer for the server or for each server in a cluster that has the Cisco CallManager service and immediate divert configured.

For information about text displays, see the Immediate Divert Phone Display Messages, on page 667.

Use Legacy Immediate Divert Clusterwide Service Parameter

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 only if the Use Legacy Immediate Divert clusterwide service parameter is set to False. If the Use Legacy Immediate Divert service parameter is set to True, the user that invokes the iDivert feature can divert an incoming call only to his own voice mailbox.

Setting the Use Legacy Immediate Divert clusterwide service parameter to False allows access to voice-messaging systems that are reached over QSIG.

Allow QSIG During iDivert Clusterwide Service Parameter

Immediate divert diverts calls to voice-messaging systems that can be reached over QSIG, SIP, and QSIG-enabled H.323 devices if the Allow QSIG During iDivert clusterwide service parameter is set to True.

Immediate Divert User Response Timer Service Parameter

The value of the Immediate Divert User Response Timer service parameter determines the time that the invoker of the iDivert softkey is given to choose the party to whom to divert a call. If the invoker does not choose a party, the call remains connected.

CHAPTER 31

Intercluster Lookup Service

When the Intercluster Lookup Service (ILS) is configured on multiple clusters, ILS updates Cisco Unified Communications Manager with the current status of remote clusters in the ILS network.

The ILS cluster discovery service allows Cisco Unified Communications Manager to learn about remote clusters without the need for an administrator to manually configure connections between each cluster.

ILS supports the Global Dial Plan Replication feature. This feature allows you to quickly configure a global dial plan, including directory URIs, alternate numbers, number patterns, PSTN failover numbers, and route strings, that spans across the entire ILS network.

The ILS service runs only on the Unified Communications Manager publisher node.

Intercluster Lookup Service

When the Intercluster Lookup Service (ILS) is configured on multiple clusters, ILS updates Cisco Unified Communications Manager with the current status of remote clusters in the ILS network.

The ILS cluster discovery service allows Cisco Unified Communications Manager to learn about remote clusters without the need for an administrator to manually configure connections between each cluster.

ILS supports the Global Dial Plan Replication feature. This feature allows you to quickly configure a global dial plan, including directory URIs, alternate numbers, number patterns, PSTN failover numbers, and route strings, that spans across the entire ILS network.

The ILS service runs only on the Unified Communications Manager publisher node.

Set Up ILS Network

The following procedure describes the steps required to set up an ILS network.

Procedure

Step 1 Study your network and design an ILS topology.

Step 2 Assign unique cluster IDs for each cluster in your network.

Step 3 If you want to use TLS authentication between clusters, you must exchange Tomcat certificates between the publisher node of each cluster in the ILS topology. From Cisco Unified Operating System Administration, use the Bulk Certificate Management feature to:

a) For each cluster in your network, export certificates from the publisher node to a central location.
b) From any publisher node server in your ILS network, consolidate exported certificates.
c) For each cluster in your network, import certificates into the publisher node for that cluster.

Step 4 If you want to use password authentication between remote clusters, assign a password for all communications between clusters in your ILS network.

Step 5 Activate ILS on the first hub cluster in your ILS network by doing the following:

a) Login to the Unified Communications Manager publisher node.
b) In Cisco Unified CM Administration, choose **Advanced Features** > **ILS Configuration**.
c) Change the Role to **Hub Cluster** and click **Save**.
d) In the ILS Configuration Registration popup window, leave the Registration Server text box empty and click **OK**.

Step 6 Activate ILS on the remaining hub and spoke clusters in your ILS network. When prompted for a registration server, enter the IP address or fully qualified domain name of the publisher node for an existing hub cluster in your ILS network.

Step 7 Confirm that your ILS network is configured by viewing the network in the ILS Clusters and Directory URI Imported Catalogs view in the ILS Configuration window. When the full network appears, your ILS network is configured for cluster discovery.

Step 8 Optional. If you want ILS to support Global Dial Plan Replication, for each cluster in the ILS network, open the ILS Configuration window and do the following:

a) Check the **Exchange Global Dial Plan Replication Data with Remote Clusters** check box.
b) In the Advertised Route String text box, assign a route string for this cluster.
c) Click **Save**.

ILS Network Components

In Cisco Unified CM Administration, you can configure ILS on a pair of clusters and then join those clusters to form an ILS network. ILS allows you to join additional clusters to the network without having to configure the connections between each cluster.

An ILS network comprises the following components:

- Hub clusters
- Spoke clusters
- Global dial plan imported catalogs

You must configure each cluster in your ILS network as either a hub cluster or a spoke cluster. Each ILS network must have at least one hub cluster.

You can view the current structure and status of the ILS network from the ILS Clusters and Directory URI Imported Catalogs view in the ILS Configuration window of Cisco Unified CM Administration.

Hub Clusters

Each ILS network must have at least one hub cluster. Hub clusters form the backbone of an ILS network. Hub clusters exchange ILS updates with the other hub clusters in the ILS network, and then relay that information to and from their spoke clusters.

ILS uses automesh functionality to create a full mesh connection between all hub clusters within an ILS network. When a new hub cluster registers to another hub cluster in an existing ILS network, ILS automatically creates a full mesh connection between the new hub cluster and all the existing hub clusters in the ILS network.

You can connect a hub cluster to multiple other hub clusters, or you might configure a hub cluster as the only hub cluster in the network. In addition, you can connect a hub cluster to multiple spoke clusters, or you might configure the hub cluster with no spokes clusters.

Spoke Clusters

A spoke cluster in an ILS network relies on the hub cluster that it is connected to in order to relay ILS updates to and from the rest of the ILS network. Although a hub cluster can have many spokes, a spoke cluster can have only one hub cluster. Spoke clusters contact only their local hub cluster and never directly contact other hub clusters or other spoke clusters.

Global Dial Plan Imported Catalogs

You cannot connect a third party call control system into an ILS network. However, in order to provide URI dialing compatibility with third party systems, you can manually import a third party directory URI or +E.164 number catalog from a CSV file into any hub cluster in the ILS network. ILS maintains the imported catalog and replicates that catalog out to the other clusters in the network so that you can dial one of the third party directory URIs or +E.164 numbers from any server in the ILS network. The imported catalog appears as its own item in the ILS Clusters and Global Dial Plan Imported Catalogs view in the ILS Configuration window.

You can import a third party catalog into a hub cluster only. You cannot import a third party catalog into a spoke cluster.

Synchronization Updates

For cluster synchronization updates, ILS uses a pull-based model in which an ILS cluster sends out an update request to a remote cluster and the remote cluster responds with the requested information. The time interval between update requests depends on the synchronization interval that is configured in the ILS Configuration window in Cisco Unified CM Administration.

For detailed information on setting up an ILS network topology, see the Cisco Unified Communications System SRND.

ILS Network Capacities

ILS networking can scale up to 100 total clusters with at most 10 hubs and 10 spokes per hub. Hub and spoke combination topology is used to avoid too many TCP connections created within each cluster.

ILS Cluster Discovery

Cluster discovery is the base service that ILS provides. ILS cluster discovery allows Cisco Unified Communications Manager clusters to learn dynamically about remote clusters without the need for an administrator to manually configure connections between those clusters.

For example, if you have an existing ILS network of four Cisco Unified Communications Manager clusters and you want to add an additional cluster, you can configure ILS on the new cluster and then register that cluster to any hub cluster in the existing ILS network. ILS automatically informs the new cluster of all clusters in the existing network.

Each cluster in an ILS network exchanges update messages, called peer info vectors, that are designed to inform remote clusters of the status of each cluster in the network. The update messages contain information about the known clusters in the network, including:

- Cluster IDs
- Cluster descriptions and versions
- Fully qualified domain name of the host
- IP addresses and hostnames for the cluster nodes that have ILS activated

The ILS cluster discovery feature automatically populates the list of remote clusters that can be viewed in Cisco Unified CM Administration by choosing **Advanced Features > Cluster View**. From this window, you can configure services such as Extension Mobility Cross Cluster, TFTP, and RSVP Agent for remote clusters.

If Global Dial Plan Replication is also enabled in the network, ILS sends separate messages containing global dial plan data.

Global Dial Plan Replication with ILS

Cisco Unified Communications Manager uses the Intercluster Lookup Service (ILS) to support the Global Dial Plan Replication feature. When Global Dial Plan Replication is enabled across an ILS network, remote clusters in an ILS network share global dial plan data, including the following:

- Directory URIs
- Alternate numbers
- Alternate number patterns
- Route strings
- PSTN failover numbers

Global Dial Plan Replication allows you to create a global dial plan including intercluster dialing of directory URIs and alternate numbers that spans across an ILS network. Global Dial Plan Replication allows you to quickly configure the global dial plan across the ILS network without the need to configure each dial plan component on each cluster separately. After you enable Global Dial Plan Replication across the network, you can simply configure the dial plan component on one cluster, and ILS replicates that information throughout the ILS network.

For detailed information on how to set up Global Dial Plan Replication, see the "Global Dial Plan Replication" chapter.

Related Topics

Global Dial Plan Replication, on page 597

ILS Configuration Settings

In Cisco Unified Communications Manager Administration, use the **Advanced Features** > **ILS Configuration** menu path to configure the Intercluster Lookup Service (ILS) on Cisco Unified Communications Manager clusters.

Although ILS is activated and runs on the publisher node, the configuration settings are applied on a cluster-wide basis. After ILS is configured on the publisher node, those settings are propagated out to the other cluster nodes.

The following table describes the ILS Configuration field settings.

Table 76: ILS Configuration Settings

Field	Description
Role	From the drop-down list box, choose the ILS role for this cluster from the following options: • **Stand Alone Cluster**—Stand alone clusters cannot join an ILS network. This is the default option. • **Hub Cluster**—Hub clusters act as hubs within the ILS network. Hub clusters may connect to multiple hub and spoke clusters. Hub clusters exchange ILS updates with other hub clusters and then communicate that information to their spoke clusters. If the cluster that you are configuring is a hub cluster, and you want to connect this hub cluster to a remote hub cluster, you can enter a registration server for the remote hub cluster in the ILS Cluster Registration popup window that appears after you click **Save.** If you want to connect this hub cluster to another hub cluster, click the **Register to another hub** button and enter the IP address or fully qualified domain name of the publisher node for the hub cluster to which you want to connect. This button does not appear if the local cluster is enabled as a stand alone cluster or as a spoke cluster. • **Spoke Cluster**—Spoke clusters register to a single hub cluster. Spoke clusters rely on the hub in order to communicate with remote clusters. If you choose a spoke cluster, you must enter a registration server in the text box that appears after you click the **Save** button

Field	Description
Exchange Global Dial Plan Replication Data with Remote Clusters	Check this check box to enable Global Dial Plan Replication for this cluster. When Global Dial Plan Replication is enabled, the local cluster advertises its catalog of local and learned directory URIs, alternate numbers, alternate number patterns, PSTN failover numbers, and route strings, to remote clusters in the ILS network. In addition, the local cluster also receives the same types of replication data from the remote clusters in the ILS network. **Note** You must check this check box if you want to implement intercluster URI dialing. **Note** Even if Global Dial Plan Replication is enabled, you can include or exclude an individual directory URI or alternate number from being replicated. If the**Advertise Globally via ILS** check box in Directory Number Configuration window is not checked for an individual directory URI or alternate number, Cisco Unified Communications Manager does not include that directory URI or alternate number with the Global Dial Plan Replication data.
Advertised Route String	In the text box, enter a route string. Route strings can be up to 64 alphanumeric characters and can include dots(.) and dashes(-). If Global Dial Plan Replication is enabled, ILS associates this route string to all the global dial plan replication data that was configured in this cluster and advertises the route string and global dial plan data to the rest of the ILS network. Global dial plan data includes all the directory URIs, alternate numbers, and alternate number patterns that were configured in this cluster. When a user in a remote cluster dials a number that matches a directory URI, alternate number, or alternate number pattern from this cluster, Cisco Unified Communications Manager matches the called number to this route string, looks for a SIP route pattern that matches the route string, and routes the call to the outbound trunk specified by the SIP route pattern.
Synchronize Clusters Every	Enter the delay, in minutes, between when the local cluster checks with remote clusters for ILS updates. The default value is 10 minutes.
ILS Authentication	
Use TLS Certificates	Click this radio button to configure ILS to use TLS to encrypt communications between remote clusters. If you check this radio button, and you are using certificates that are not signed by a trusted certificate authority, you must exchange Tomcat certificates between the clusters in your network.
Use Password	Click this radio button to configure ILS to use password based authentication for communications between remote clusters. If you check this radio button, you must enter a password. You must configure all clusters in your network with the same password.
Confirm Password	If you checked Use Password, confirm your password here.

Field	Description
Registration Server	The Registration Server text box appears in the ILS Cluster Registration popup window that displays after you change the Role to Spoke Cluster or Hub Cluster and click **Save**. To enter a registration server, enter the IP address or fully qualified domain name of the publisher node in the hub cluster to which you want to connect. You must enter a registration server in the following circumstances: • If you are configuring a spoke cluster, you must enter a registration server for the hub cluster to which you want to connect. • If you are configuring a hub cluster, you only have to enter a registration server if you want to connect this hub cluster to another hub cluster in the ILS network. Otherwise, you can leave the field blank. If ILS is running on both the local and remote clusters, ILS uses the registration server to form a relationship with the remote cluster. Once ILS forms a connection, the registration server is no longer used.
Activate the Intercluster Lookup Service on the publisher in this cluster	This check box appears in the ILS Cluster Registration popup window that displays after you change the Role to Spoke Cluster or Hub Cluster and click **Save**. Check this check box if you want to activate ILS on the publisher node in the cluster.
ILS Clusters and Imported Directory URI Catalogs	

Field	Description
ILS Clusters and Imported Directory URI Catalogs	This section displays a snapshot of the current ILS network, including all hub clusters, spoke clusters, and imported directory URI catalogs. Spoke clusters are displayed under their associated hub cluster. The cluster that you are currently logged into is identified as the local cluster For large networks, you can use the **Find** button to filter the display to just those clusters that meet specific search criteria. The table contains the following columns: • Cluster ID/Name—This column displays the cluster ID for the remote cluster. If the other cluster is from a non-ILS system that was manually imported into Cisco Unified CM, the field displays the imported catalog name and the Role column lists the catalog as a Directory URI Imported Catalog. • Last Contact Time—This column displays the last time the local cluster had direct contact with this cluster. If more than two replication intervals pass without an update from the other cluster, a warning icon appears, alerting you that there may be a connection issue. **Note** Spoke clusters only make direct contact with their local hub cluster. Spoke clusters never contact remote hub clusters, or other spokes. • Role—This column displays whether the remote cluster is a hub cluster, spoke cluster, or an imported directory URI catalog. The cluster that you are currently logged into is identified as the local cluster. • Advertised Route String—This column displays the route string for the remote cluster or imported directory URI catalog. • Last USN Data Received—This column displays the last time the local cluster received an updated USN data from this cluster or imported catalog. • USN Data Synchronization Status—This column displays the USN replication status of the cluster or imported directory URI catalog. • Action—Click **Disconnect** if you want to remove this cluster from the ILS network. **Note** If you disconnect a hub cluster from the network, Cisco Unified Communications Manager also disconnects that hub cluster's spoke clusters.

ILS Troubleshooting

Local Cluster Cannot Connect to the ILS Network

To troubleshoot connection issues within the local cluster, open RTMT and run alarms and diagnostic traces on that publisher node.

If you receive an error message when trying to establish ILS between your clusters, you can try to restart the Cisco Intercluster Lookup service from Cisco Unified Serviceability Administration.

In addition, connection issues may arise if authentication is improperly configured between clusters. Check authentication in the following manner:

- If you are using TLS, make sure that all clusters in the network are using TLS and that Tomcat certificates have been exchanged for all the servers that need to communicate.

  Note Certificates exchanged using bulk certificate export, merge, and import can cause an untrusted ILS hub due to TLS errors.

- If you are using TCP password authentication, make sure that all ILS clusters are using TCP password authentication and that the same TCP password is assigned across the network.

Directory URIs Are Not Being Replicated Across the ILS Network

This error can occur for a variety of reasons. Check the following:

- Verify that all clusters in the network are configured to exchange global dial plan data. If a hub cluster is not configured to exchange global dial plan data, none of that hub's spoke clusters will be able to exchange directory URI catalogs.
- Allow enough time for end-to-end replication based on synchronization intervals (set on the ILS Configuration page) that are configured for all the clusters involved in the path. All clusters in an ILS network are a maximum of three hops from every other cluster in the network.
- Use the **utils ils showpeerinfo** CLI command to monitor replication progress by looking at the USN values for the remote clusters.
- Increase speed of replication by changing the ILS Sync Throttle Service Parameter. Note that a low setting can affect system performance.
- Verify that all clusters in the ILS network have unique cluster IDs and that none of the clusters are configured with Stand Alone Cluster as its cluster ID. You can check Cluster IDs in Cisco Unified CM Administration under **System** > **Enterprise Parameters**.

Global Dial Plan Replication Is Configured, but Unified CM Still Cannot Place a Call to A Learned Directory URI or Learned Number in a Remote ILS Cluster

This condition can occur if ILS and Global Dial Plan Replication are enabled on all clusters in the network, but SIP route patterns that route to the route strings for the remote clusters have not been configured. Do the following:

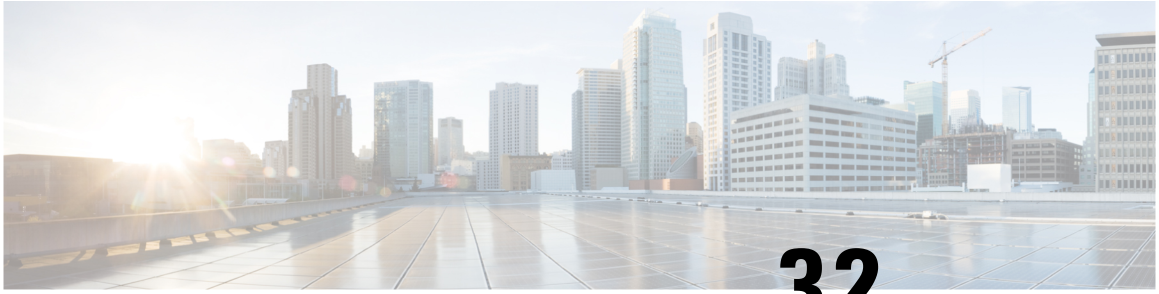
- In the ILS Clusters and Global Dial Plan Imported Catalogs view in the ILS Configuration window, check the route string for the remote cluster.
- In the SIP Route Pattern configuration window, make sure that you have route patterns that map to the route strings for your remote clusters.

Note When advertising URI patterns (`user@domain`), in the **SIP Profile Configuration** window, make sure that the **Dial String Interpretation** field is set to **Always treat all dial strings as URI addresses** to prevent the devices to dial URI learned patterns with only numbers in the user section as Directory Number patterns. Alternatively, you can advertise only URI patterns with text strings in the user section through ILS.

ILS Global Dial Plan Replication Update is Cached Until Cisco Unified Communications Manager Database Replication is Not Corrected

The value of **Last USN Data Received** is Current and USN Data Synchronization Status is **Up to date**. However, the Learned URIs or Learned Patterns are not viewable on local cluster.

This condition occurs when database replication is not corrected. ILS caches the updates with learned URIs or patterns from remote clusters if database replication is not viewable on local cluster across all nodes. Unified Communications Manager can place a call to these learned URIs or patterns after the database replication is corrected.



CHAPTER 32

Intercom

This chapter provides information about Intercom, a type of phone line, which 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 auto-answers to one-way audio whisper. The recipient can then acknowledge the whispered call and initiate a two-way intercom call.

Intercom

This chapter provides information about Intercom, a type of phone line, which 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 auto-answers to one-way audio whisper. The recipient can then acknowledge the whispered call and initiate a two-way intercom call.

Configure Intercom

Intercom, a type of phone line, 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 auto-answers to one-way audio whisper. The recipient can then acknowledge the whispered call and initiate a two-way intercom call.

Users 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.

Note Users can use an intercom line only to dial other intercom lines.

Intercom allows a user to place a call to a predefined target. The called destination auto-answers the call 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, Cisco Unified Communications Manager implements whisper intercom. Whisper intercom means 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.

Note An auto-answer tone indicates the beginning of the whisper state for both the sender and the recipient.

Perform the following steps to configure the Cisco Unified Communications Manager Intercom feature in Cisco Unified Communications Manager.

Procedure

Step 1 Create intercom partition.

Note When you create an intercom partition, the administration user interface will automatically generate a corresponding intercom calling search space with the same name and includes this new intercom partition initially.

Step 2 Create intercom calling search space.

Note Do this if you need to create an intercom calling search space other than the one that is generated automatically when you create the intercom partition.

Step 3 Create intercom translation pattern (optional).

Step 4 Create intercom directory number.

Step 5 Assign intercom directory number to a phone.

Related Topics

Intercom Partition Configuration, on page 692

Intercom Calling Search Space Configuration, on page 698

Intercom Translation Pattern Configuration, on page 702

Intercom Directory Number Configuration, on page 711

Intercom Line and Speed Dial Configuration, on page 722

Intercom Feature

Intercom, a type of phone line, 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 auto-answers to one-way audio whisper. The recipient can then acknowledge the whispered call and initiate a two-way intercom call.

Users 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.

Note Users can use an intercom line only to dial other intercom lines.

Intercom allows a user to place a call to a predefined target. The called destination auto-answers the call 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, Cisco Unified Communications Manager implements whisper intercom. Whisper intercom means 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.

Note An auto-answer tone indicates the beginning of the whisper state for both the sender and the recipient.

Intercom Directory Numbers and Default Devices

Each intercom line needs a default device. The intercom feature requires configuration of the Default Activated Device field in the Intercom Directory Number Configuration window to make an intercom line display as active. The intercom line displays 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 displays when the user logs in.

See the Intercom Directory Number Configuration, on page 711 for configuration details.

Note If an intercom line has been configured and assigned to a phone but fails to display on the phone, check that the Default Activated Device value is set to this device for this intercom line. If that configuration has taken place, check that the phone has been reset.

Intercom Directory Numbers and Cisco Extension Mobility

Be aware that intercom directory numbers (lines) are restricted to one device per intercom line. Because 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.

Because an extension mobility profile can be used on more than one phone simultaneously, use the Default Activated Device field 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.

The Intercom, on page 476 section of the Extension Mobility, on page 463 chapter provides additional details about upgrading from Release 6.0(1) of Cisco Unified Communications Manager to Release 6.1(1) or later.

System Requirements

The system requirements for the intercom feature follow:

- Cisco Unified Communications Manager Release 6.0 or later
- Microsoft Internet Explorer (IE) 7 or Internet Explorer 8 or FireFox 3.x or Safari 4.x
- Cisco Unified IP Phones firmware release 8.3(1) or later

Determine Intercom Support for Cisco Unified IP Phones

The list of devices that support the Intercom feature varies per version and device pack.

Use the Cisco Unified Reporting application to generate a complete list of devices that support the Intercom feature for a particular release and device pack. To do so, follow these steps:

Procedure

Step 1 Start Cisco Unified Reporting by using any of the methods that follow. The system uses the Cisco Tomcat service to authenticate users before allowing access to the web application. You can access the application

- by choosing **Cisco Unified Reporting** in the Navigation menu in Cisco Unified Communications Manager Administration and clicking **Go.**
- by choosing **File** > **Cisco Unified Reporting** at the Cisco Unified Real Time Monitoring Tool (RTMT) menu.
- by entering `https://<server name or IP address>:8443/cucreports/` and then entering your authorized username and password.

Step 2 Click **System Reports** in the navigation bar.

Step 3 In the list of reports that displays in the left column, click the **Unified CM Phone Feature List** option.

Step 4 Click the Generate a new report link to generate a new report, or click the Unified CM Phone Feature List link if a report already exists.

Step 5 To generate a report of all devices that support Intercom, choose these settings from the respective drop-down list boxes and click the **Submit** button:

Product: All

Feature: Intercom

The List Features pane displays a list of all devices that support the Intercom feature. You can click on the Up and Down arrows next to the column headers (Product or Protocol) to sort the list.

For additional information about the Cisco Unified Reporting application, see the *Cisco Unified Reporting Administration Guide*.

Call and Line States

Intercom introduces a new call state for the intercom line, Whisper. Intercom also uses the existing Idle, Connected, Offhook, and Digits After First line states.

Because only one intercom call can occur at a time, the intercom call state maps directly to the line state, and call sort rules will remain unaffected.

The following table lists the intercom call and line states.

Table 77: Intercom Call and Lines States

	Idle	Whisper	Off hook	Digits After First	Connected
Description	Idle intercom state	During whisper, the recipient receives the initiator voice, but the initiator does not receive the recipient voice. Callers on any other active calls with the recipient do not receive the initiator voice.	Only present when a target has not been preconfigured and an intercom target must be dialed.	Only present when a target has not been preconfigured and an intercom target must be dialed.	Connected specifies the connected state for the Intercom feature.
LED Behavior	LED not illuminated	Feature Key: Solid Amber	Feature Key: Solid Amber.	Feature Key: Solid Amber.	Feature Key: Solid Green
Icon	Idle	Whisper	Whisper	Whisper	Connected
Softkey Template	Default Cisco Unified Communications Manager Template	Connected No Feature	Intercom Off hook	Default Unified CM Digits After First template, Connected No Feature.	Connected No Feature
Other		An auto-answer tone precedes whisper.	“Inside” dial tone	No dial tone	

Interactions and Restrictions

This section describes the interactions and restrictions that are associated with intercom.

Interactions

This section describes how intercom interacts with Cisco Unified Communications Manager applications and call processing features.

Bulk Administration Tool

The Cisco Unified Communications Manager administrator can use the Bulk Administration Tool (BAT) to add many intercom users at once instead of adding users individually. See the Cisco Unified Communications Manager Bulk Administration Guide for more information.

Barge

When the intercom destination is a barge target, the Cisco Unified IP Phone can still support whisper intercom.

When the destination caller opts to talk to the intercom caller by pressing the intercom button, the original call has been put on hold, and the barge initiator will get 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 needs to hang up before the phone can reregister with Cisco 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 intercom feature will not be available when the phones are registered with SRST.

Cisco Unified Communications Manager Assistant

See the Cisco Unified Communications Manager Assistant Configuration Wizard chapter in the Cisco Unified Communications Manager Administration Guide.

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 intercom 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.

See the Intercom Directory Number Configuration, on page 711 and to the Extension Mobility, on page 463 for configuration details.

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. For more information on IPv6, see the Internet Protocol Version 6 (IPv6), on page 739.

Restrictions

The following restrictions apply to the Intercom feature:

- Intercom calls do not follow a coverage path.
- 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).
- If sufficient bandwidth does not exist, the intercom call fails.
- 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 conferenced.
- When an active call is being monitored or recorded, the user cannot receive nor place intercom calls
- Video is not supported with intercom.

Install and Activate Intercom

Because intercom comes standard with Cisco Unified Communications Manager Release 6.0 and later, it automatically gets installed and activated.

Configure Intercom

To use the intercom feature, both the caller and called phones require a dedicated intercom line button. This line will have its own Directory Number (DN), which is its intercom code, and partition (intercom group).

The Calling Search Space for this intercom line gets used to restrict the access of intercom destination from this phone.

Note To guarantee that no accidental use of the intercom feature occurs by an unauthorized phone, users cannot access intercom partition and intercom calling search space from other administrative windows, except under the intercom feature.

Note The system does not allow an intercom line to be shared on multiple devices. It should not have any other feature-related configuration, such as forward, pickup, voice mail profile, and so on.

Tip A phone can have more than one intercom button that is assigned.

Tip Before you configure intercom, review the configuration summary task for this feature..

Related Topics

Configure Intercom, on page 685

Intercom Partition Configuration

This section provides information to find, add, update, or delete intercom partitions. An intercom partition contains a list of route patterns [directory number (DN) and route patterns]. Partitions facilitate call routing by dividing the route plan into logical subsets that are based on organization, location, and call type. For more information about partitions, see the *Cisco Unified Communications Manager System Guide*.

Add an Intercom Partition

You can add a new intercom partition by using the following procedure.

Procedure

Step 1 From the Cisco Unified Communications Manager Administration window, click **Call Routing** > **Intercom** > **Intercom Route Partition**.

The Find and List Intercom Partitions window displays.

Step 2 Click the **Add New** button.

An Add New Intercom Partition window displays.

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, Cisco Unified Communications Manager uses the partition name as the description.

The Find and List Intercom Partitions window displays

Step 4 Continue with Find an Intercom Partition, on page 693

Find an Intercom Partition

The Find and List window for intercom partitions allows you to search for an intercom partition, which is a list of route patterns [directory number (DN) and route patterns]. Partitions facilitate call routing by dividing the route plan into logical subsets that are based on organization, location, and call type

Because you might have several intercom partitions in your network, Cisco Unified Communications Manager lets you locate specific intercom partitions based on specific criteria. Use the following procedure to locate intercom partitions.

Note During your work in a browser session, Cisco Unified Communications Manager Administration retains your intercom partition search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your intercom partition search preferences until you modify your search.

Procedure

Step 1 Choose **Call Routing** > **Intercom** > **Intercom Route Partition**.

The Find and List Intercom Directory Numbers window displays. Records from an active (prior) query may also display in the window.

Step 2 To filter or search records

a) From the first drop-down list box, select a search parameter.
b) From the second drop-down list box, select a search pattern.
c) Specify the appropriate search text, if applicable.

Note To add additional search criteria, click the **+** button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the **–** button to remove the last added criterion or click the **Clear Filter** button to remove all added search criteria.

Step 3 To find all records in the database, ensure the dialog box is empty, click **Find.**

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

Note You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking **Delete Selected**. You can delete all configurable records for this selection by clicking **Select All** and then clicking **Delete Selected**.

Step 4 From the list of records that display, click the link for the record that you want to view.

Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Related Topics

Intercom Calling Search Space Configuration, on page 698

Configure an Intercom Partition

Perform the following procedure to configure an intercom partition.

Note When you add a new intercom partition, Cisco Unified Communications Manager automatically adds a new intercom calling search space that contains only the new partition. You can modify the new intercom calling search space later.

Note Be aware that intercom partition and intercom calling search space cannot be mixed with partition and calling search space for regular lines.

Procedure

Step 1 In the menu bar, choose **Call Routing** > **Intercom** > **Intercom Route Partition**.

The Find and List Intercom Partitions window displays.

Locate the partition that you want to configure by using the steps described in Find an Intercom Partition, on page 693.

Step 2 Enter the appropriate settings that are described in Intercom Partition Configuration, on page 695.

Step 3 Click **Save.**

The Intercom Partition Configuration window displays

Step 4 Enter the appropriate settings that are described in Intercom Partition Configuration, on page 695.

If you are updating an intercom partition, click Reset or use the Apply Config button described in the Synchronize an Intercom Partition with Affected Devices, on page 696.

Related Topics

Intercom Calling Search Space Configuration, on page 698

Intercom Partition Configuration

An intercom partition contains a list of route patterns [directory number (DN) and route patterns]. Partitions facilitate call routing by dividing the route plan into logical subsets that are based on organization, location, and call type.

The following table describes the intercom partition configuration settings for adding new intercom partitions.

Table 78: Add New Intercom Partition(s) Configuration Settings

Field	Description
Intercom Partition Information	
Name, Description	Enter a name in the name box. Ensure each intercom partition name is unique to the route plan. Intercom partition names can contain a-z, A-Z and 0-9 characters, as well as spaces, hyphens (-), and underscore characters (_). **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. The table below provides examples of the maximum number of intercom partitions that can be added to an intercom calling search space if intercom partition names are of fixed length. Follow the intercom partition name by a comma (,); then, enter a description on the same line as the Partition Name. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), angle brackets (<>), square bracket ([ ]), ampersand (&), and percentage sign (%). If you do not enter a description, Cisco Unified Communications Manager automatically enters the intercom partition name in this field. Use a new line for each intercom partition and description.

Timesaver Use concise and descriptive names for your intercom partitions. The CompanynameLocationCalltype format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify an intercom partition. For example, CiscoDallasMetroPT identifies a partition for toll-free, inter-local access and transport area (LATA) calls from the Cisco office in Dallas.

Tip You can enter multiple intercom partitions at the same time by entering the intercom partition name and description, if applicable, in the Intercom Partition Information Name text box. Remember to use one line for each intercom partition entry and to separate the intercom partition name and description with a comma.

The following table provides examples of the maximum number of intercom partitions that can be added to an intercom calling search space if partition names are of fixed length.

Table 79: Calling Search Space Partition Limitations

Partition Name Length	Maximum Number of Partitions
2 characters	170
3 characters	128
4 characters	102
5 characters	86

The following table provides descriptions of the information needed to configure an existing intercom partition.

Table 80: Intercom Partition Configuration Settings

Field	Description
Intercom Partition Information	
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 displays 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.

Synchronize an Intercom Partition with Affected Devices

To synchronize devices with an intercom partition that has undergone configuration changes, perform the following procedure, which will apply any outstanding configuration settings in the least-intrusive manner possible. (For example, a reset/restart may not be required on some affected devices.)

Procedure

Step 1 Choose **Call Routing** > **Intercom** > **Intercom Route Partition**.

The Find and List Intercom Partitions window displays.

Step 2 Choose the search criteria to use.

Step 3 Click **Find.**

The window displays a list of intercom partitions that match the search criteria.

Step 4 Click the intercom partition to which you want to synchronize applicable devices. The Intercom Partition Configuration window displays.

Step 5 Make any additional configuration changes.

Step 6 Click **Save.**

Step 7 Click **Apply Config**.

The Apply Configuration Information dialog displays.

Note If devices that are associated with the intercom partition get reset, calls on affected gateways may drop.

Step 8 Click **OK**.

Related Topics

Intercom Calling Search Space Configuration, on page 698

Delete an Intercom Partition

The following procedure describes how to delete an intercom partition.

Before you begin

You cannot delete an intercom partition if it is assigned to an item such as calling search space or to a route pattern. To find out which calling search spaces or other items are using the intercom partition, choose Dependency Records from the Related Links drop-down list box in the Intercom Partition Configuration window and click Go. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the Cisco Unified Communications Manager Administration Guide. If you try to delete a partition that is in use, Cisco Unified Communications Manager displays a message. Before deleting a partition that is currently in use, you must perform either or both of the following tasks:

- Assign a different intercom partition to any intercom calling search spaces, devices, or other items that are using the intercom partition that you want to delete.
- Delete the intercom calling search spaces, devices, or other items that are using the intercom partition that you want to delete.

Procedure

Step 1 In the menu bar, choose **Call Routing** > **Intercom** > **Intercom Route Partition**.

Step 2 Locate the intercom partition that you want to delete.

Step 3 Check the check box of the intercom partition that you want to delete and click **Delete Selected**.

Tip You can delete all the intercom partitions in the list by clicking **Select All** and then clicking **Delete Selected**.

A message displays that states that you cannot undo this action.

Step 4 To delete the intercom partition, click **OK** or to cancel the deletion, click **Cancel**.

Caution Before initiating this action, check carefully to ensure that you are deleting the correct intercom partition. You cannot retrieve deleted intercom partitions. If an intercom partition is accidentally deleted, you must rebuild it.

Tip You can also delete an intercom partition by locating and displaying the partition that you want to delete and clicking **Delete**.

Related Topics

Intercom Calling Search Space Configuration, on page 698

Find an Intercom Partition, on page 693

Intercom Calling Search Space Configuration

This section provides information to find, add, update, copy, or delete a calling search space. An intercom calling search space comprises an ordered list of intercom route partitions that are typically assigned to devices. Intercom calling search spaces determine the partitions that calling devices search when they are attempting to complete a call.

For more detailed information on calling search spaces and partitions, see the *Cisco Unified Communications Manager System Guide*.

Find an Intercom Calling Search Space

The Find and List window for intercom calling search spaces allows you to search for an intercom calling search space, which is an ordered list of intercom route partitions that are typically assigned to devices. Intercom calling search spaces determine the intercom partitions that calling devices search when they are attempting to complete a call.

Because you might have several intercom calling search spaces in your network, Cisco Unified Communications Manager lets you locate specific intercom calling search spaces by using specific criteria as the basis. Use the following procedure to locate intercom calling search spaces.

Note During your work in a browser session, Cisco Unified Communications Manager Administration retains your intercom calling search space search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your intercom calling search space search preferences until you modify your search.

Procedure

Step 1 Choose **Call Routing** > **Intercom** > **Intercom Calling Search Space**.

The Find and List Intercom Calling Search Spaces window displays. Records from an active (prior) query may also display in the window.

Step 2 To filter or search records

a) From the first drop-down list box, select a search parameter.
b) From the second drop-down list box, select a search pattern.
c) Specify the appropriate search text, if applicable.

Note To add additional search criteria, click the **+** button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the **–** button to remove the last added criterion or click the **Clear Filter** button to remove all added search criteria.

Step 3 To find all records in the database, ensure the dialog box is empty, click **Find.**

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

Note You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking **Delete Selected**. You can delete all configurable records for this selection by clicking **Select All** and then clicking **Delete Selected**.

Step 4 From the list of records that display, click the link for the record that you want to view.

Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

What to do next

Additional Topics

See the Intercom Translation Pattern Configuration, on page 702.

Configure an Intercom Calling Search Space

The following procedure describes how to copy, add and update an intercom calling search space.

Procedure

Step 1 In the menu bar, choose **Call Routing** > **Intercom** > **Intercom Calling Search Space**.

Step 2 Perform one of the followings tasks:

a) To copy an existing intercom calling search space, locate the appropriate intercom calling search space as described in Find an Intercom Calling Search Space, on page 698. Click the **Copy** button next to the intercom calling search space that you want to copy. The window displays the copy of the intercom calling search space. Change the Intercom Calling Search Space Name.

b) To add an intercom calling search space, click the **Add New** button.

Note To add more intercom calling search spaces, click Add New and repeat this procedure.

c) To update an existing intercom calling search space, locate the appropriate intercom calling search space as described in Find an Intercom Calling Search Space, on page 698.

Step 3 Enter the appropriate settings as described in Intercom Calling Search Space Configuration, on page 700.

Step 4 Click **Save.**

Related Topics

Intercom Translation Pattern Configuration, on page 702

Intercom Calling Search Space Configuration

An intercom calling search space comprises an ordered list of intercom route partitions that are typically assigned to devices. Intercom calling search spaces determine the partitions that calling devices search when they are attempting to complete a call.

Table 81: Intercom Calling Search Space Configuration Settings

Field	Description
Intercom Calling Search Space Information	
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 (<>).

Field	Description
Intercom Route Partitions for this Calling Search Space	
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.
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 box.

The following figure provides examples of the maximum number of intercom partitions that can be added to a calling search space if intercom partition names are of fixed length.

Table 82: Calling Search Space Partition Limitations

Partition Name Length	Maximum Number of Partitions
2 characters	170
3 characters	128
4 characters	102
5 characters	86
. . .	. . .
10 characters	46
15 characters	32

Delete an Intercom Calling Search Space

The following procedure describes how to delete an intercom calling search space.

Before you begin

You cannot delete intercom calling search spaces that devices, lines (DNs), translation patterns, or other items are using. To find out which devices, lines, translation patterns, or other items are using the intercom calling search space, choose the Dependency Records from the Related Links drop-down list box in the Intercom Calling Search Space Configuration window and click Go. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the Cisco Unified Communications Manager Administration Guide. If you try to delete an intercom calling search space that is in use, Cisco Unified Communications Manager displays a message. Before deleting an intercom calling search space that is currently in use, you must perform either or both of the following tasks:

- Assign a different intercom calling search space to any devices, lines, or translation patterns that are using the intercom calling search space that you want to delete. See the Intercom Directory Number Configuration, on page 711 and the Intercom Translation Pattern Configuration, on page 702.
- Delete the devices, lines, or translation patterns that are using the intercom calling search space that you want to delete. See the Intercom Translation Pattern Configuration, on page 702, and the Delete an Intercom Translation Pattern, on page 710.

Procedure

Step 1 In the menu bar, choose **Call Routing** > **Intercom** > **Intercom Calling Search Space**.

Step 2 Locate the intercom calling search space that you want to delete. See the Find an Intercom Calling Search Space, on page 698.

Step 3 Check the check box of the intercom calling search space that you want to delete and click **Delete Selected**.

A message displays that states that you cannot undo this action.

Step 4 To delete the intercom calling search space, Click **OK** or click **Cancel**.

Caution Before initiating this action, check carefully to ensure that you are deleting the correct intercom calling search space. You cannot retrieve deleted intercom calling search spaces. If an intercom calling search space is accidentally deleted, you must rebuild it.

Tip You can also delete an intercom calling search space by locating and displaying the intercom calling search space that you want to delete and clicking **Delete**.

Related Topics

Intercom Translation Pattern Configuration, on page 702

Intercom Translation Pattern Configuration

This section provides information to add, update, copy, or delete an intercom translation pattern. Cisco Unified Communications Manager uses intercom 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.

Find an Intercom Translation Pattern

The Find and List window for intercom translation patterns allows you to search on intercom translation patterns, which Cisco Unified Communications Manager uses to manipulate dialed digits before it routes a call.

Because you might have several intercom translation patterns in your network, Cisco Unified Communications Manager lets you locate specific intercom translation patterns by using specific criteria as the basis. Use the following procedure to locate intercom translation patterns.

Note During your work in a browser session, Cisco Unified Communications Manager Administration retains your intercom translation pattern search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your intercom translation pattern search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Call Routing** > **Intercom** > **Intercom Translation Pattern**.

The Find and List Intercom Directory Numbers window displays. Records from an active (prior) query may also display in the window.

Step 2 To filter or search records

a) From the first drop-down list box, select a search parameter.
b) From the second drop-down list box, select a search pattern.
c) Specify the appropriate search text, if applicable.

Note To add additional search criteria, click the **+** button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the **–** button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

Step 3 To find all records in the database, ensure the dialog box is empty, click **Find.**

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

Note You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking **Delete Selected**. You can delete all configurable records for this selection by clicking **Select All** and then clicking **Delete Selected**.

Step 4 From the list of records that display, click the link for the record that you want to view.

Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Related Topics

Intercom Directory Number Configuration, on page 711

Configure an Intercom Translation Pattern

This section describes how to configure an intercom translation pattern.

Before you begin

Configure the following Cisco Unified Communications Manager intercom items before configuring an intercom translation pattern:

- Intercom partition
- Intercom route filter
- Intercom calling search space

Procedure

Step 1 Choose **Call Routing** > **Intercom** > **Intercom Translation Pattern**.

The Find and List Intercom Translation Patterns window displays.

Step 2 Perform one of the followings tasks:

a) To copy an existing intercom translation pattern, locate the appropriate intercom translation pattern as described in the Find an Intercom Translation Pattern, on page 703, click the **Copy** button next to the intercom translation pattern that you want to copy.
b) To add a new intercom translation pattern, click the **Add New** button.

Step 3 In the Intercom Translation Pattern Configuration window that displays, enter the appropriate configuration settings as described in Intercom Calling Search Space Configuration, on page 700.

Step 4 Click **Save**.

Note Ensure that the intercom translation pattern, that uses the selected 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 configuration windows if you receive an error that indicates duplicate entries.

The Intercom Translation Pattern Configuration window displays the newly configured intercom translation pattern.

Related Topics

Intercom Directory Number Configuration, on page 711

Intercom Translation Pattern Configuration Settings

Cisco Unified Communications Manager uses intercom 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.

The following table describes the available fields in the Intercom Translation Pattern Configuration window.

Table 83: Translation Pattern Configuration 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.
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 box 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 box. 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 box 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.

Field	Description
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.
Route Filter	Choosing an optional route filter restricts certain number patterns. The route filters that display depend on the numbering plan that you choose from the Numbering Plan drop-down list box. 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 box: • 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.

Field	Description
Calling Search Space	From the drop-down list box, 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 box 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 box. Click the Find button to display the Find and List Calling Search Space window. Find and choose an intercom calling search space name.
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 box: • 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.

Field	Description
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.
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.

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. **Note** The discard digits that display depend on the numbering plan that you choose from the Numbering Plan drop-down list box.
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.

Delete an Intercom Translation Pattern

This section describes how to delete an intercom translation pattern.

Procedure

Step 1 Choose **Call Routing** > **Intercom** > **Intercom Translation Pattern**.

Step 2 Locate the intercom translation pattern that you want to delete. See the Find an Intercom Translation Pattern, on page 703.

Step 3 Check the check box of the intercom translation pattern that you want to delete and click **Delete Selected**.

A message displays that states that you cannot undo this action.

Step 4 To delete the intercom translation pattern, click **OK** or to cancel the deletion, click **Cancel**.

Caution Check carefully to ensure that you are deleting the correct intercom translation pattern before you initiate this action. You cannot retrieve deleted intercom translation patterns. If you accidentally delete an intercom translation pattern, you must rebuild it.

Tip You can also delete an intercom translation pattern by locating and displaying the intercom translation pattern that you want to delete and clicking Delete.

Related Topics

Intercom Directory Number Configuration, on page 711

Intercom Directory Number Configuration

This section provides information about working with and configuring intercom directory numbers (DNs) in Cisco Unified Communications Manager Administration.

Related Topics

Intercom, on page 685

Intercom Directory Number Configuration Overview

Using Cisco Unified Communications Manager Administration, configure and modify intercom directory numbers (DNs) that are assigned to specific phones. These sections provide instructions for working with intercom directory numbers.

Note Be aware that a partition is required for intercom directory numbers.

Note Intercom directory numbers require configuration of the Default Activated Device field in the Intercom Directory Number Configuration window as specified in the Intercom Directory Number Configuration Settings, on page 714 if the intercom directory number is to be active. You can also configure intercom directory numbers for use with Cisco Extension Mobility as specified in the same description.

Related Topics

Intercom, on page 685

Find an Intercom Directory Number

The Find and List window for intercom directory numbers allows you to search for intercom directory numbers, which are directory numbers that are used for the intercom feature and are assigned to specific phones. Use the following procedure to find an intercom directory number (DN).

Procedure

Step 1 Choose **Call Routing** > **Intercom** > **Intercom Directory Number**.

The Find and List Intercom Directory Numbers window displays. Records from an active (prior) query may also display in the window.

Step 2 To filter or search records

a) From the first drop-down list box, select a search parameter.
b) From the second drop-down list box, select a search pattern.
c) Specify the appropriate search text, if applicable.

Note To add additional search criteria, click the **+** button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the **–** button to remove the last added criterion or click the **Clear Filter** button to remove all added search criteria.

Step 3 To find all records in the database, ensure the dialog box is empty, click **Find.**

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

Note You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking **Delete Selected**. You can delete all configurable records for this selection by clicking **Select All** and then clicking **Delete Selected**.

Step 4 From the list of records that display, click the link for the record that you want to view.

Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Related Topics

Intercom, on page 685

Configure an Intercom Directory Number

Follow these instructions to add or update an intercom directory number (DN). You can configure the call forward, call pickup, and MLPP phone features while you are adding the directory number.

Tip 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 the intercom DN configuration fields, Line Text Label, Display (Internal Caller ID), and External Phone Number Mask. (These fields display for an intercom directory number only after you add the intercom directory number and you associate the intercom directory number with a phone.)

Tip For example, add the user name to the line text label and internal caller ID, but add the outside line number to the external number mask, so, when the calling information displays, it says John Chan, not 352XX.

Procedure

Step 1 Choose **Call Routing** > **Intercom** > **Intercom Directory Number**.

The Find and List Intercom Directory Numbers window displays.

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 displays.

Step 3 Perform one of the followings tasks:

a) To add an intercom directory number, click the **Add New** button to add a new intercom directory number. The Intercom Directory Number Configuration window displays.

Note The Phone Configuration window provides an alternate method for adding a directory number. Use the **Device** > **Phone** menu option and create a new phone or search for an existing phone. After you create the new phone or display the existing phone, click either the **Line [1] - Add a new DN** or **Line [2] - Add a new DN** link in the Association Information area on the left side of the Phone Configuration window. The Directory Number Configuration window displays.

b) To update an intercom directory number, click the intercom directory number that you want to update. The Intercom Directory Number Configuration window displays.

Step 4 Update the appropriate settings as described in Intercom Directory Number Configuration Settings, on page 714.

Step 5 Click **Save.**

Note See the Synchronize an Intercom Directory Number with Affected Devices, on page 721 before deciding whether to continue to the next step below.

Step 6 Click **Reset Phone**. For more information, see the Cisco Unified Communications Manager Administration Guide.

Tip If you need more than two lines, you can increase the lines by modifying the phone button template for the phone type. Some phone types, however, only support one or two lines (such as Cisco Unified IP Phone 7906).

Note Restart devices as soon as possible. During this process, the system may drop calls on gateways.

Related Topics

Intercom, on page 685

Intercom Directory Number Configuration Settings

For intercom, you must configure an intercom directory number.

Tip 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 the intercom DN configuration fields, Line Text Label, Display (Internal Caller ID), and External Phone Number Mask. (These fields display for a intercom directory number only after you add the intercom directory number and you associate the intercom directory number with a phone.)

Tip For example, add the user name to the line text label and internal caller ID, but add the outside line number to the external number mask, so, when the calling information displays, it says John Chan, not 352XX.

Note Be aware that a partition is required for intercom directory numbers.

Note Intercom directory numbers require configuration of the Default Activated Device field in the Intercom Directory Number Configuration window as specified in the following table if the intercom directory number is to be active. You can also configure intercom directory numbers for use with Cisco Extension Mobility as specified in the same description.

The following table describes the fields that are available in the Intercom Directory Number Configuration window.

Table 84: Intercom Directory Number Configuration Settings

Field	Description
Intercom Directory Number Information	

Field	Description
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.
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 box 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 box. 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 Parameters and choose CCMAdmin 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 box, 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 box. 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 box, 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 box 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.

Calling Search Space

You can configure the number of intercom calling search spaces that display in this drop-down list box 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 box. Click the Find button to display the Find and List Calling Search Spaces window. Enter a partial intercom calling search space name in the List items where Name contains field. Click the desired intercom calling search space name in the list of intercom calling search spaces 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.

Synchronize an Intercom Directory Number with Affected Devices

To synchronize devices with an intercom directory number that has undergone configuration changes, perform the following procedure, which will apply any outstanding configuration settings in the least-intrusive manner possible. (For example, a reset/restart may not be required on some affected devices.)

Procedure

Step 1 Choose **Call Routing** > **Intercom** > **Intercom Directory Number**.

The Find and List Intercom Directory Numbers window displays.

Step 2 Choose the search criteria to use.

Step 3 Click **Find.**

The window displays a list of intercom directory numbers that match the search criteria.

Step 4 Click the intercom directory number to which you want to synchronize applicable devices. The Intercom Directory Number Configuration window displays.

Step 5 Make any additional configuration changes.

Step 6 Click **Save.**

Step 7 Click **Apply Config**.

The Apply Configuration Information dialog displays.

Step 8 Click **OK**.

Intercom Line and Speed Dial Configuration

To configure the intercom line, perform the following procedure:

Procedure

Step 1 If you have not already done so, create the intercom partition.

Step 2 If you have not already done so, create the intercom directory number.

Step 3 Click **Device** > **Device Settings** > **Phone Button Template** and add the intercom line to an existing phone button template or create a new template.

Note Be aware that the intercom line cannot be configured as the primary line.

Step 4 Choose **DevicePhone** and assign an intercom directory number to the intercom line.

Step 5 Configure the intercom directory number and set up intercom speed dial, if desired.

Note You can configure the intercom line with a predefined destination (speed dial) to allow fast access.

Related Topics

Intercom Partition Configuration, on page 692

Intercom Directory Number Configuration, on page 711

Intercom Operation

This section provides information about how to use intercom.

Case Studies

The following information explains how intercom works when it is initiated to an idle phone and to a busy phone.

Intercom to an Idle Phone

When Alice intercoms Bob, Bob will receive an intercom tone first, followed by the voice of Alice. Alice, however, will not hear Bob.

If Bob has his headset on, he will use it to hear Alice; otherwise, the speaker will get used.

Intercom to a Busy Phone

Bob and Carol are speaking when Alice places an intercom call to Bob. The voice of Alice voice will get mixed with the voice of Carol voice to be played to Bob; however, Alice cannot hear Bob, while Carol will continue to hear Bob.

For most cases, Carol will only hear Bob, but not Alice; however, if Bob is using speakerphone when conversing with Carol, the voices of Alice and Bob might be mixed when they are sent to Carol.

The busy phone means that an active call exists on the phone of Bob, or it represents an outgoing call that has not connected yet.

For intercom terminating caller to end the intercom call without talking to the originator, the caller needs to press I-help button followed by intercom button to bring the softkey set for intercom into focus. User then can press ‘EndCall’ softkey to end the call.

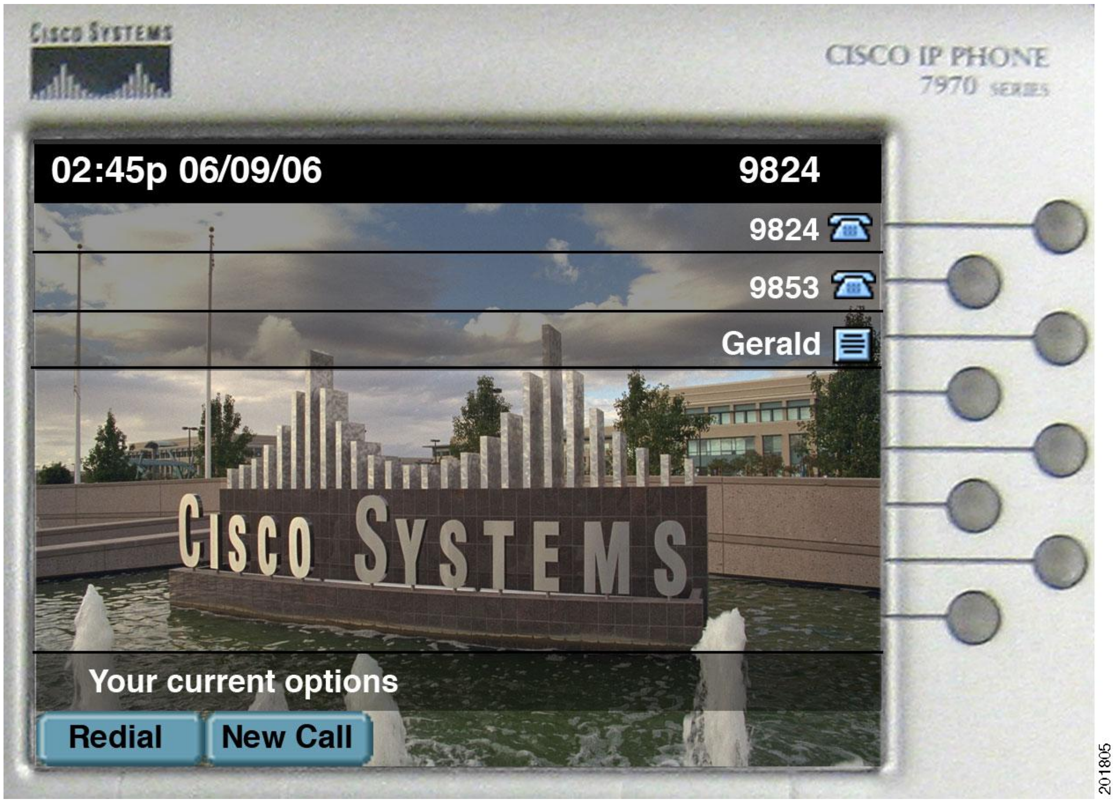
Illustrated Explanation of Intercom

This section describes how intercom works in several different scenarios.

Scenario 1

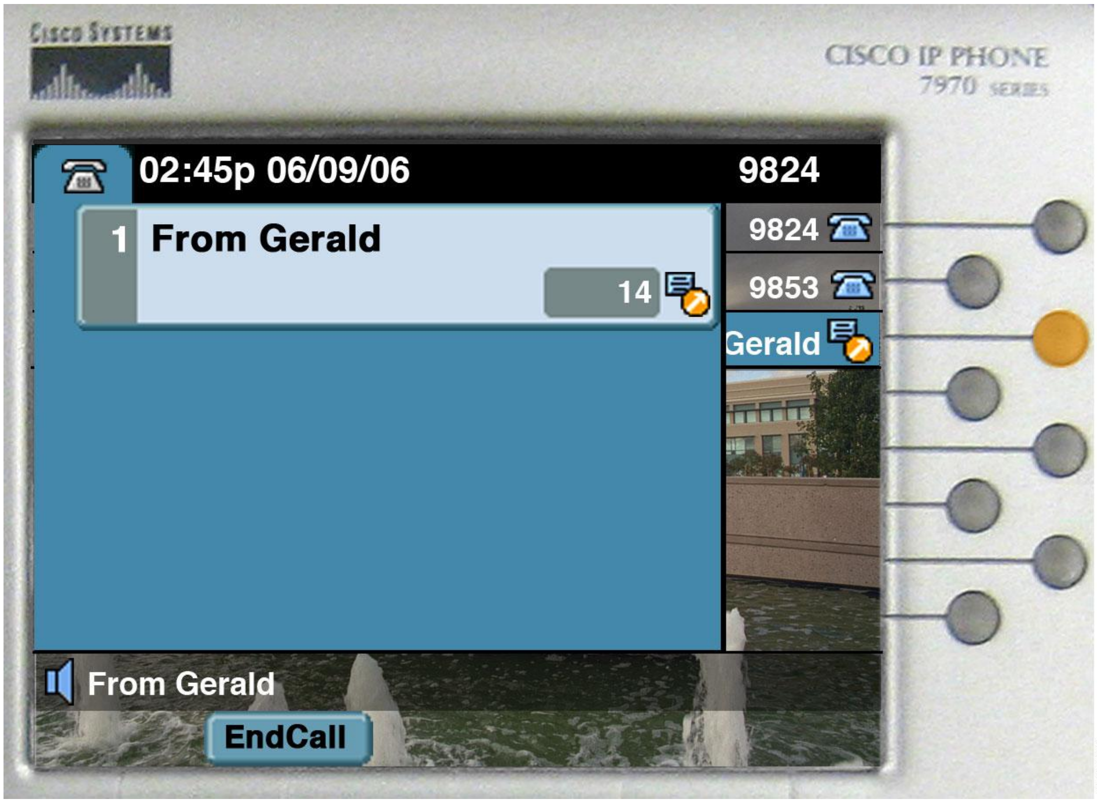
The phone that belongs to Anna, while idle, receives an intercom call from Gerald who is the preconfigured intercom target.

Figure 55: Idle



- Before Gerald places the intercom call to Anna, her phone is idle.
  - The line key and the intercom key appear dark.

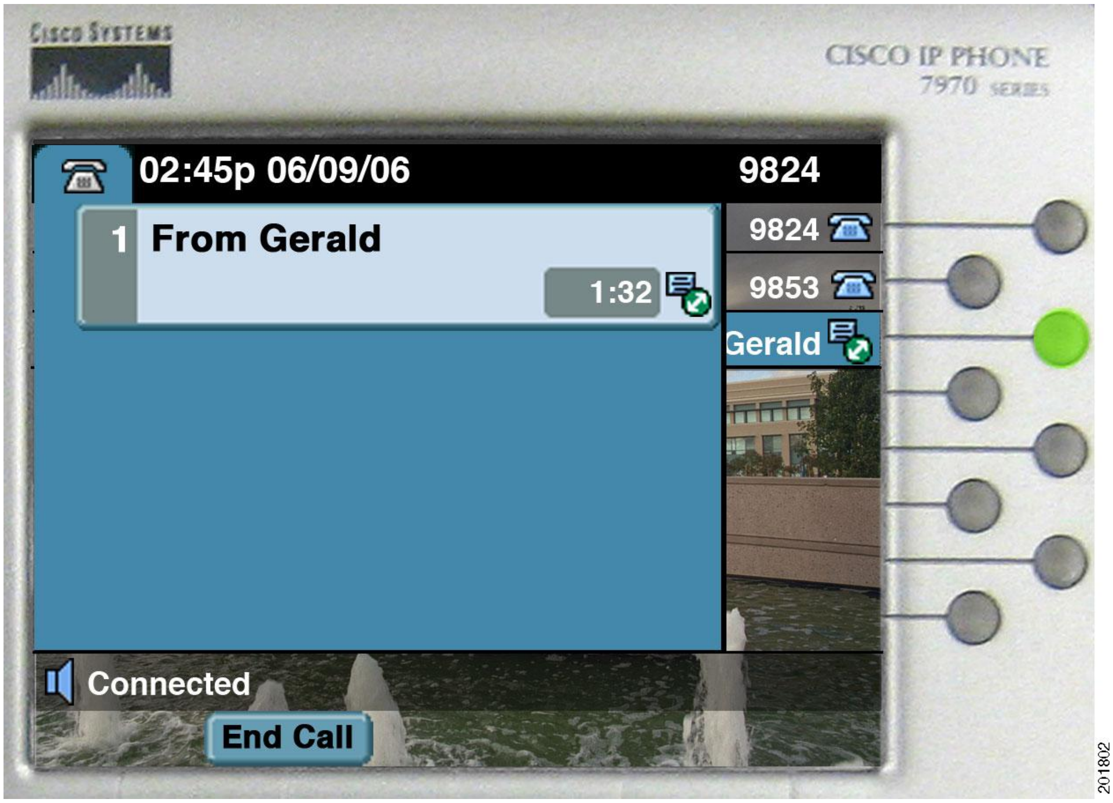
Figure 56: Whisper



- The intercom line becomes active, and a call from Gerald appears.
  - The intercom key displays solid amber.
- Both phones receive auto-answer alert tones.
- Anna hears Gerald speaking, but Gerald cannot hear Anna until she addresses the intercom call.

Note Pressing the Mute key will not address the intercom call; it will only cause the status line to display “That key is not active here.”

Figure 57: Connected



- Anna addresses the intercom call by pressing the intercom line key.
  - The intercom key displays solid green.

Note The call timer does not reset but continues from the whisper state.

Scenario 2

Anna, while her phone is idle, places an intercom call to Gerald's phone, the preconfigured intercom target.

Figure 58: Whisper

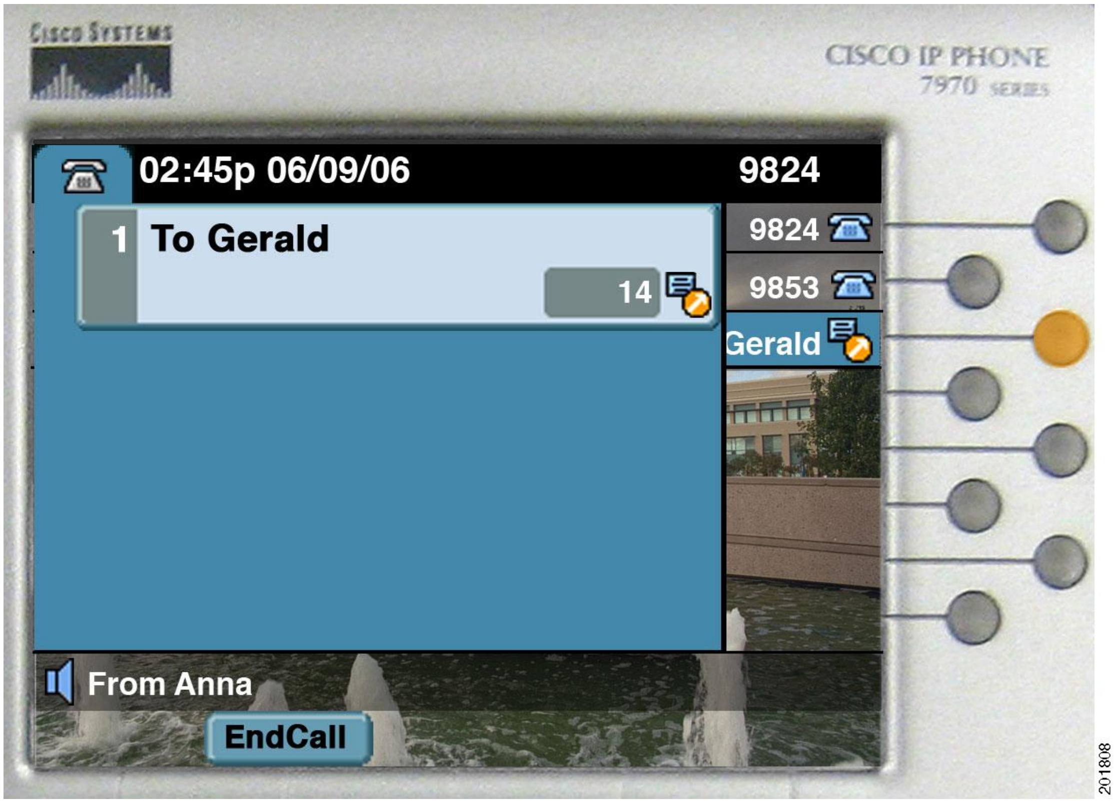
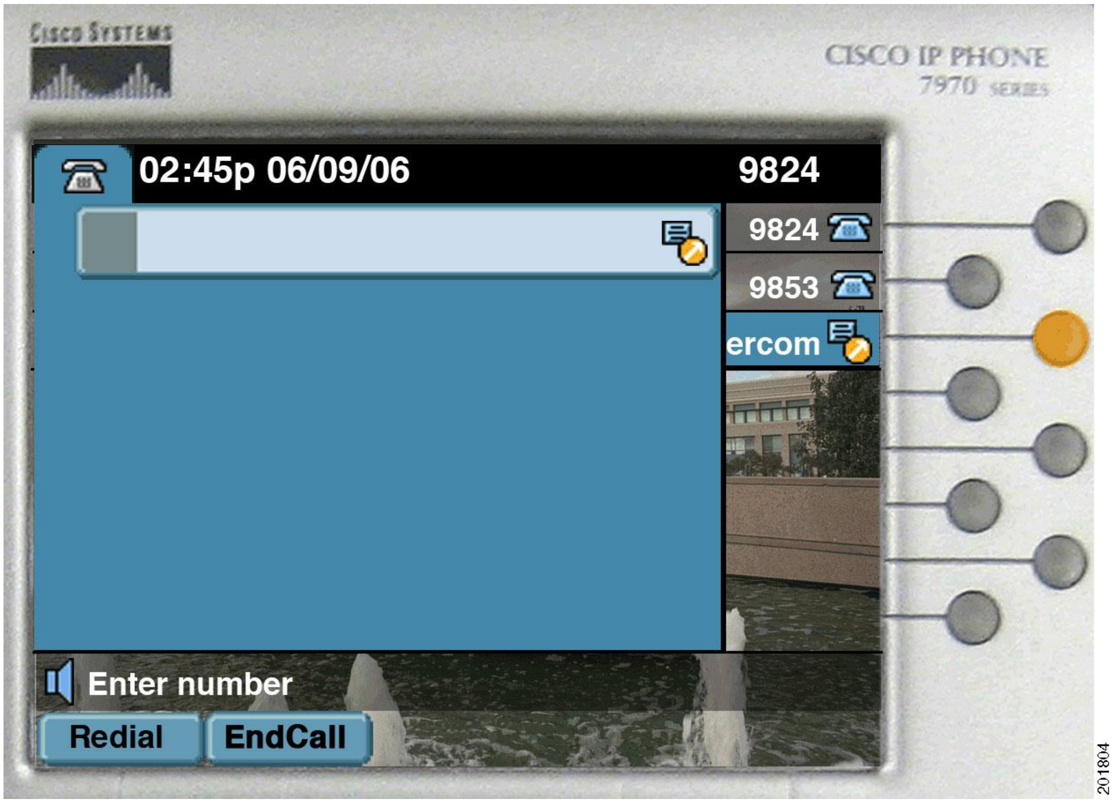


Figure 59: Connected



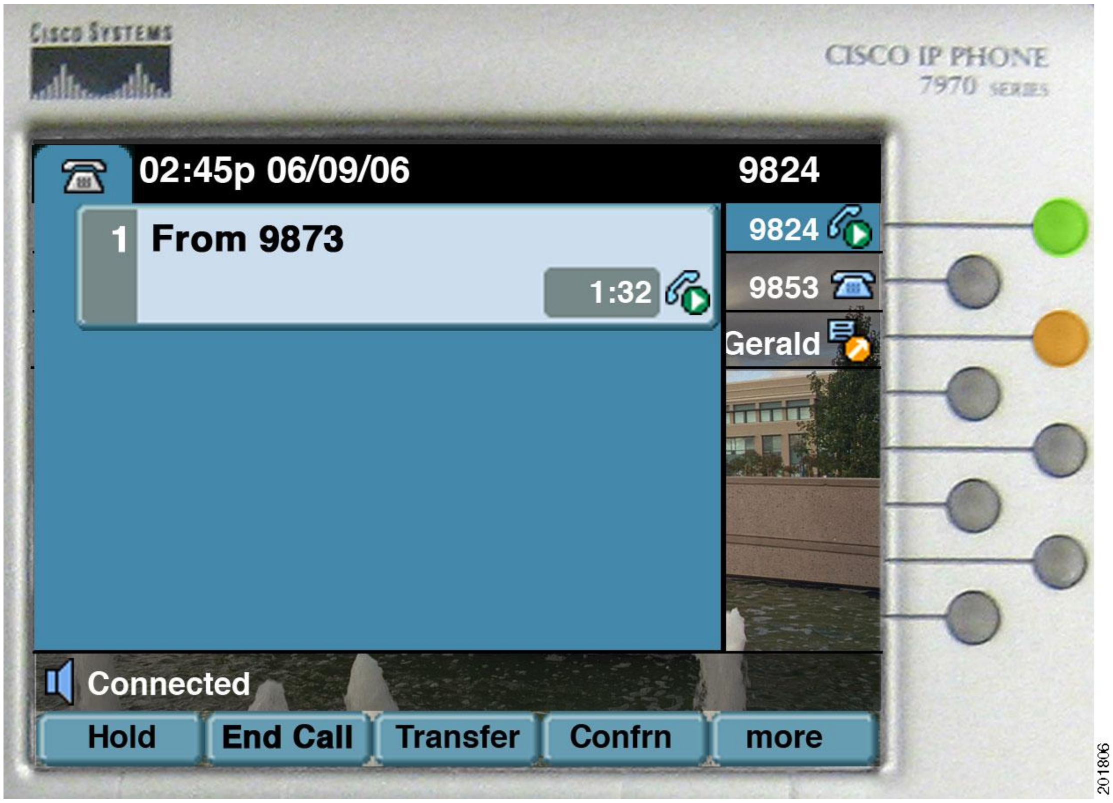
- Gerald addresses the intercom call by pressing the intercom line key.
  - The intercom key displays solid green.

Note The call timer does not reset.

Scenario 3

Anna, while on a connected or held call, receives an intercom call from Gerald, the preconfigured intercom target

Figure 60: Whisper

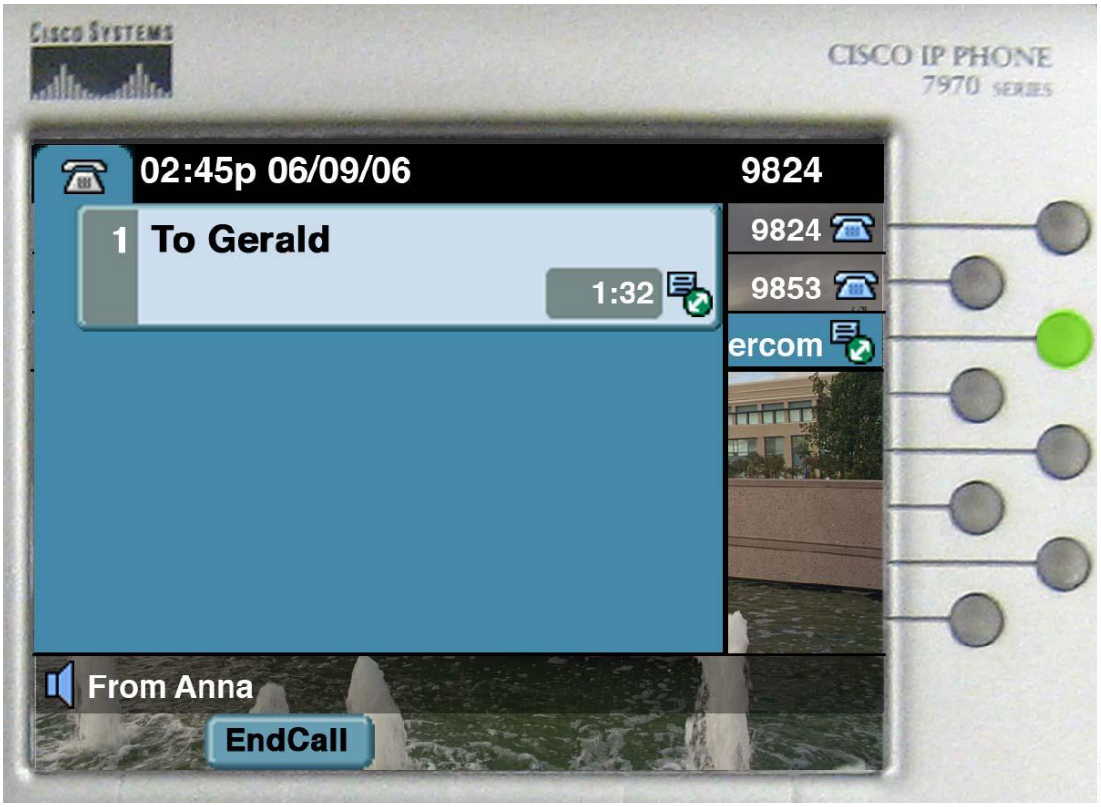


- While Anna is speaking on the phone, the preconfigured intercom line indicator flashes amber, which indicates that Gerald is calling Anna on the intercom line.
  - The line key displays solid green.
  - The intercom key displays solid amber.

Note When Auto Line Select is disabled, which represents the default, the current call retains focus.

- The phone that Anna is using plays an auto-answer alert tone, followed by the voice of Gerald.
- Anna can hear Gerald, but Gerald cannot hear Anna until she addresses the intercom call.
- The current caller, who is at 9873 and is on the line with Anna, can hear Anna but cannot hear Gerald.

Figure 61: Connected



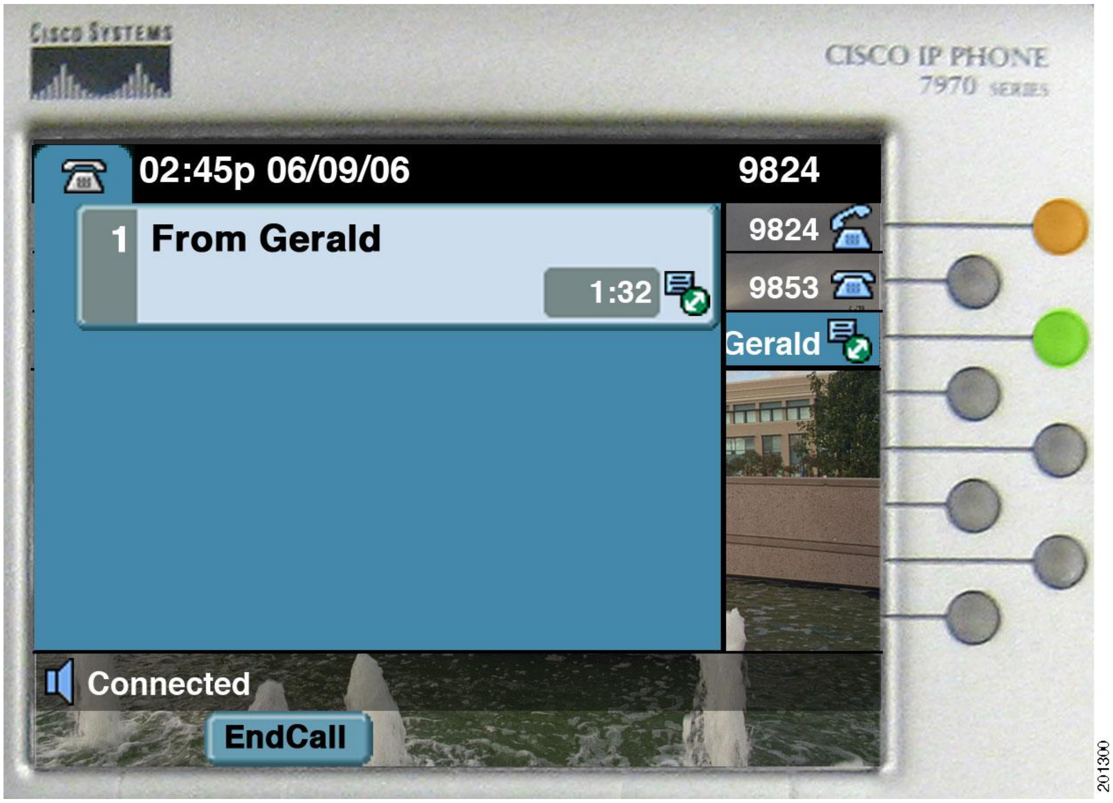
- Anna addresses the intercom call by pressing the intercom line key.
    - The line key flashes green.
- The intercom call gains focus, and the previous call gets put on hold.
    - The intercom line key displays solid green.

Note The call timer represents the cumulative call time from the whisper state and the current connected state.

Scenario 4

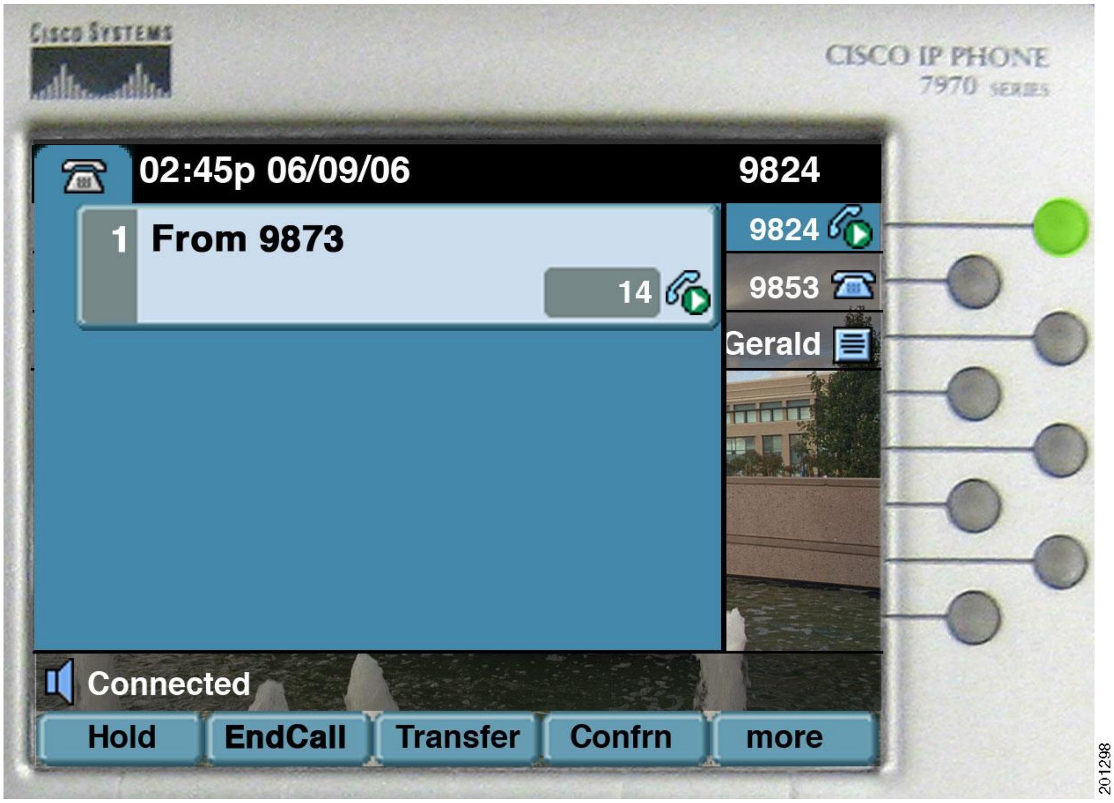
Anna, while on a whispered or connected intercom call, receives a new call on the primary line.

Figure 62: Connected



- Anna is talking to Gerald on an intercom line when a call displays for 9824, which is her extension. The intercom call retains focus.
    - The line key flashes amber.
    - The intercom key displays solid green.

Figure 63: Idle

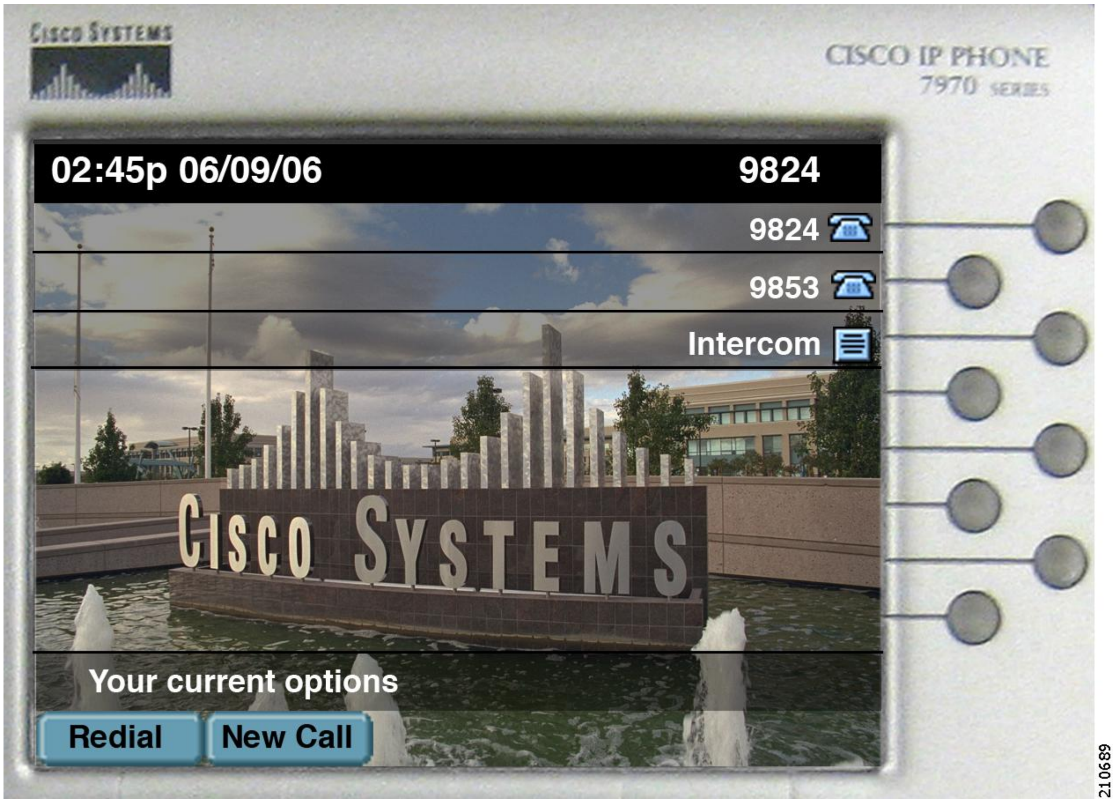


- Anna accepts the incoming call by pressing the 9824 line key.
  - The line key displays solid green.
- The incoming call receives focus and gets connected.
- The system clears the intercom call.
  - The intercom key displays dark.

Scenario 5

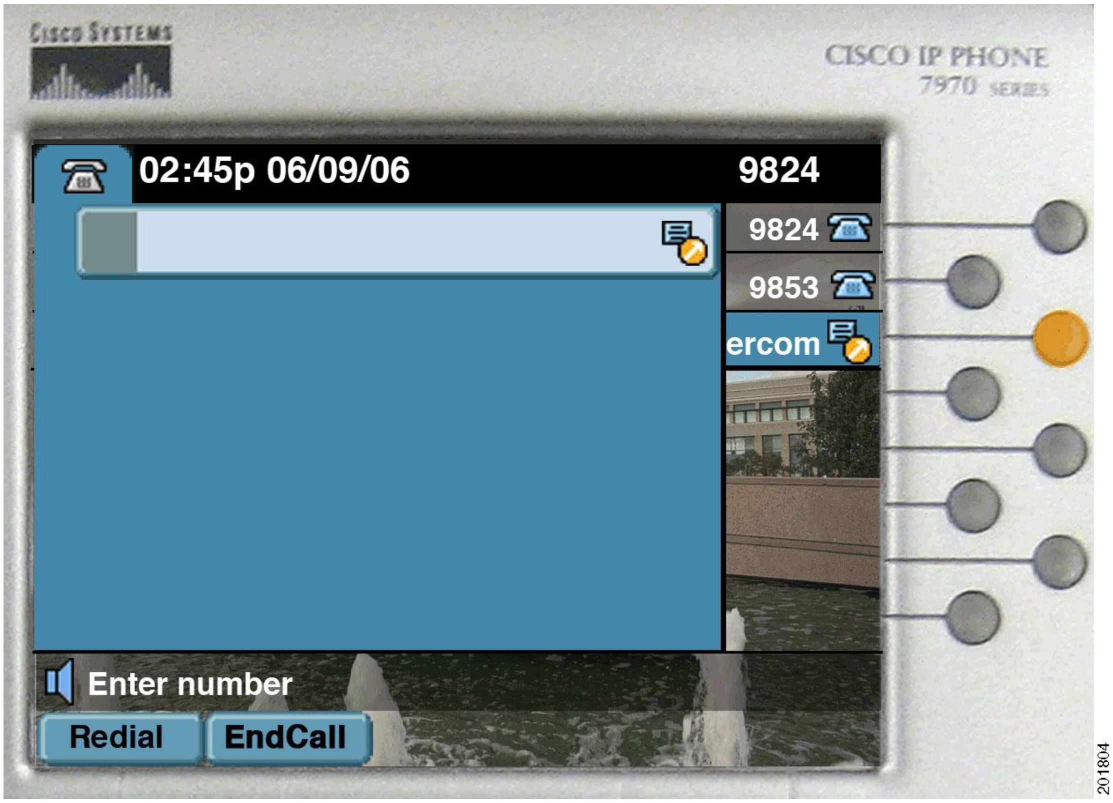
Anna, while idle, places an intercom call to Gerald. The intercom line has no preconfigured target.

Figure 64: Idle



- All the line keys display dark.

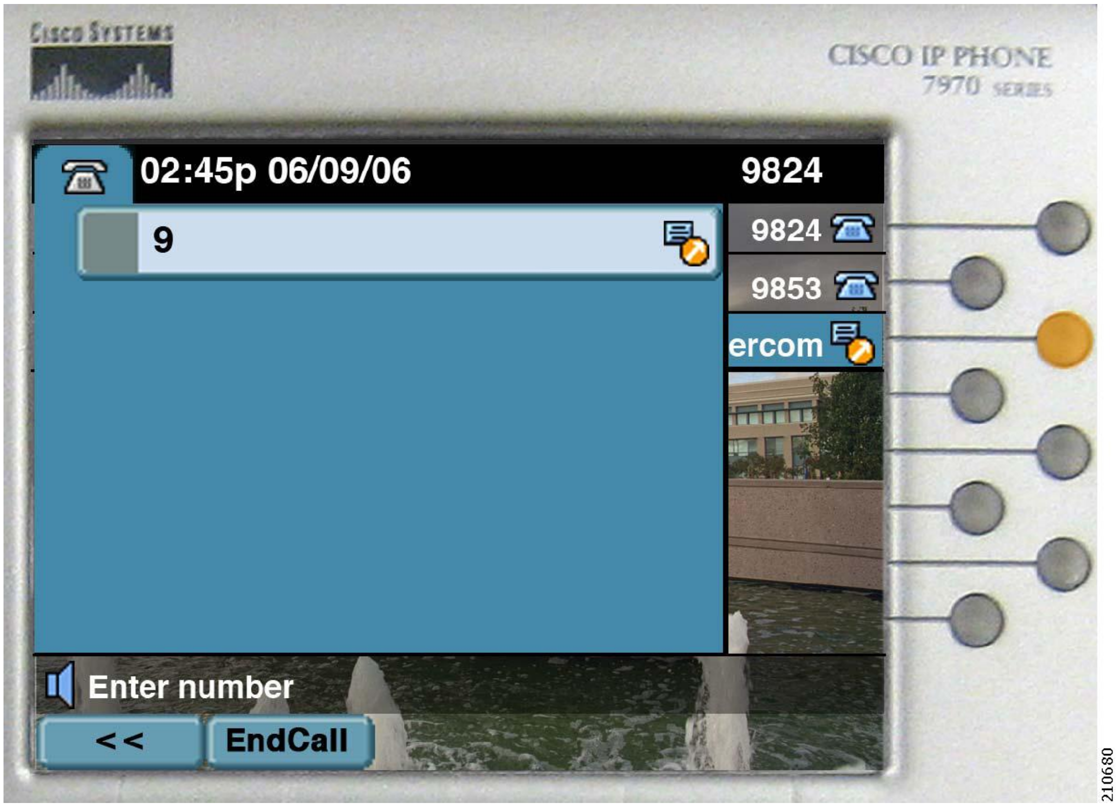
Figure 65: Dial Out



- Anna presses the intercom line key, which invokes the dial-out state.
    - The intercom key displays solid amber.
- The phone receives an “inside” dial tone.

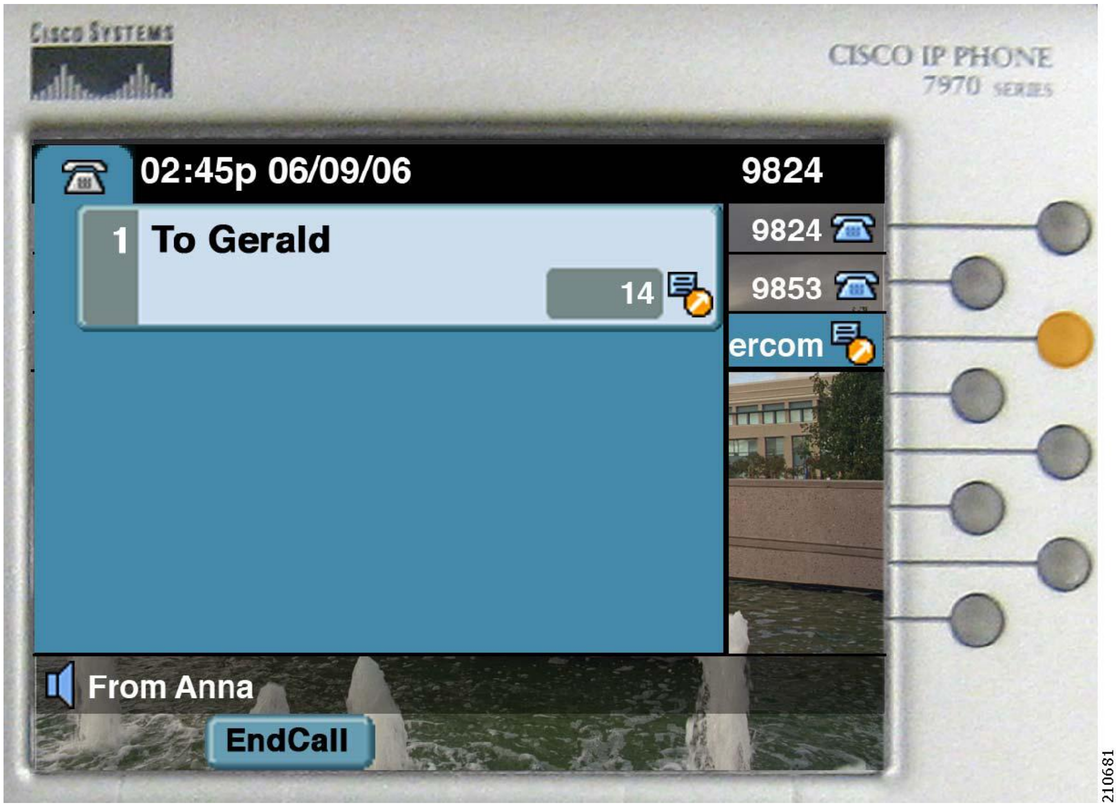
Note At this time, if Anna dials any number other than an intercom number, the phone receives a fast busy tone.

Figure 66: Digits After First



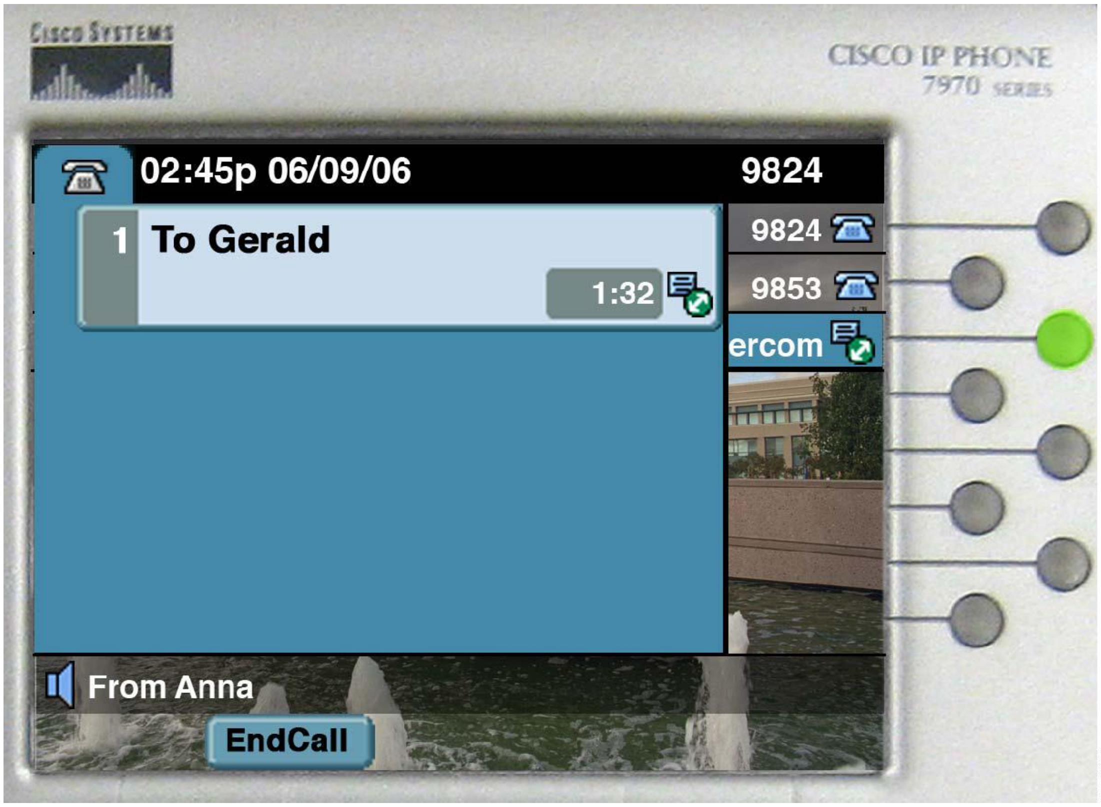
- Anna begins to dial, which invokes the digits after first state.
  - The intercom kay displays solid amber.

Figure 67: Whisper



- After Anna dials the intercom number, the whisper state exists.
    - The intercom key displays solid amber.
- The phone plays an auto-answer alert.
- Gerald can hear Anna, but Anna cannot hear Gerald until he addresses the intercom call.

Figure 68: Connected



- Gerald addresses the intercom call by pressing the intercom line key.
  - Anna can see that the intercom key displays solid green.
- The call timer does not reset but, instead, continues from the whisper state.

CHAPTER 33

Internet Protocol Version 6 (IPv6)

This chapter provides information about Internet Protocol version 6 (IPv6), which is the latest version of the Internet Protocol (IP). Packets are used to exchange data, voice, and video traffic over dual-stack IP networks, and increase the number of network address bits from 32 bits in IPv4 to 128 bits. IPv6 support in the Cisco Unified Communications Manager network allows the network to behave transparently in a dual-stack environment and provides additional IP address space and autoconfiguration capabilities to devices that are connected to the network.

IPv6 dual-stack mode is supported for SCCP and SIP signaling and media. All other interfaces support IPv4 mode.

Use this information in conjunction with the document, *Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager*, which provides design guidelines for deploying IPv6 in your Cisco Unified Communications network.

Note For information about IPv6 support for your IP phone or Cisco Unity Connection, see the Cisco Unified IP Phone Administration Guide that supports your phone model or the Cisco Unity Connection documentation.

Internet Protocol Version 6 (IPv6)

This chapter provides information about Internet Protocol version 6 (IPv6), which is the latest version of the Internet Protocol (IP). Packets are used to exchange data, voice, and video traffic over dual-stack IP networks, and increase the number of network address bits from 32 bits in IPv4 to 128 bits. IPv6 support in the Cisco Unified Communications Manager network allows the network to behave transparently in a dual-stack environment and provides additional IP address space and autoconfiguration capabilities to devices that are connected to the network.

IPv6 dual-stack mode is supported for SCCP and SIP signaling and media. All other interfaces support IPv4 mode.

Use this information in conjunction with the document, *Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager*, which provides design guidelines for deploying IPv6 in your Cisco Unified Communications network.

Note For information about IPv6 support for your IP phone or Cisco Unity Connection, see the Cisco Unified IP Phone Administration Guide that supports your phone model or the Cisco Unity Connection documentation.

Configure IPv6

Internet Protocol version 6 (IPv6), which is the latest version of the Internet Protocol (IP) that uses packets to exchange data, voice, and video traffic over dual-stack IP networks, increases the number of network address bits from 32 bits in IPv4 to 128 bits. IPv6 support in the Cisco Unified Communications Manager network allows the network to behave transparently in a dual-stack environment and provides additional IP address space. IPv6 also supports autoconfiguration capabilities for devices that are connected to the network.

This section lists the high-level tasks that you must complete to configure IPv6. To complete these tasks, you will need to refer to the following Cisco Unified Communications Manager documentation, which contains detailed procedures and information about configuration parameters:

- *Installing Cisco Unified Communications Manager*
- *Cisco Unified Communications Manager Administration Guide*
- *Cisco Unified Communications Manager Operating System Administration Guide*

Perform the following steps to configure IPv6 in your network.

Before you begin

Before you configure IPv6, review all IPv6-related documentation.

- *Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager*
- *Cisco IOS IPv6 Configuration Library*
- *Implementing VoIP for IPv6*
- This IPv6 chapter

Procedure

Step 1 Provision a local IPv6-capable DNS and DHCP server.

Caution You can provision your DNS server for IPv6 prior to upgrading from an earlier release of Cisco Unified Communications Manager to the current release. However, do not configure the DNS records for Cisco Unified Communications Manager for IPv6 until after you upgrade to the current release. Configuring the DNS records for Cisco Unified Communications Manager for IPv6 prior to upgrading to the current release causes the upgrade to fail and causes your system to become nonfunctional after you reboot.

Tip Cisco recommends that the Cisco Unified Communications Manager node use a global address or a unique local address (ULA). If the Cisco Unified Communications Manager node obtains the IPv6 address from the DHCPv6 server or via stateless address autoconfiguration, ensure that the Cisco Unified Communications Manager node only obtains one global address or one unique local IPv6 address from the DHCPv6 server. If you manually assign the address, it will override any address obtained from the DHCPv6 server.

Step 2 Make sure that you have compatible network hardware and Cisco IOS software that is installed and configured; for example, configure your Integrated Services Router (ISR) G2 gateways and Cisco IOS MTP for IPv6.

Step 3 Install the current release of Cisco Unified Communications Manager.

Before you install subsequent nodes (subscribers) in the cluster, add the IPv4 server information to the Server Configuration window in Cisco Unified Communications Manager Administration.

Step 4 Enable IPv6 in the Cisco Unified Communications Operating System and ensure that the Cisco Unified Communications Manager node obtains an IPv6 address. Cisco recommends that the Cisco Unified Communications Manager node use a static non-link-local IPv6 address.

Tip For each node in the cluster, perform these tasks. Performing these tasks requires a reboot of the node.

Step 5 In the Enterprise Parameters Configuration window in Cisco Unified Communications Manager Administration, choose True for the Enable IPv6 enterprise parameter.

Tip After you update this enterprise parameter, restart the Cisco CallManager, Cisco IP Voice Media Streaming App, Cisco CTIManager, Cisco Certificate Authority Proxy Function, and the Cisco IPVMS services in Cisco Unified Serviceability.

Step 6 For the node that you are configuring in Cisco Unified Communications Manager Administration, choose **System** > **Server** and enter the unique local address or a host name that can resolve to a IPv6 address in the IPv6 Name field.

Tip For each node in the cluster, perform this task.

Tip If you enter a host name, remember to update the DNS server with the appropriate Cisco Unified Communications Manager name and address information.

Caution You can provision your DNS server for IPv6 prior to upgrading to the current release. However, do not configure the DNS records for IPv6 for Cisco Unified Communications Manager until after you upgrade to the current release. Configuring the DNS records for IPv6 for Cisco Unified Communications Manager prior to upgrading to the current release causes the upgrade to fail and causes your system to become nonfunctional after you reboot.

Step 7 In Cisco Unified Communications Manager Administration, configure phone-related and SIP trunk-related IPv6 settings.

For example, configure the IP Addressing Mode and Allow Auto-Configuration for Phones settings in the Common Phone Profile Configuration window; then, apply the common device profile configuration to the phone or SIP trunk.

Step 8 Restart the Cisco CallManager, Cisco IP Voice Media Streaming App, Cisco CTIManager, Cisco Certificate Authority Proxy Function and the Cisco IPVMS services in Cisco Unified Serviceability.

Related Topics

Media Termination Points, on page 751
Internet Protocol Version 6 (IPv6), on page 739
Cisco Unified CM, on page 743
Run IPv6 CLI Commands or Configure IPv6 in the Ethernet IPv6 Window, on page 762
Configure Service and Enterprise Parameters for IPv6, on page 765

IPv6 for Cisco Unified CM Feature

This section provides information about IPv6 for Cisco Unified CM.

CTI Applications

CTI provides IP address information through the JTAPI and TAPI interfaces, which can support IPv4 and IPv6 addresses. To support IPv6, applications need to use a JTAPI /TAPI client interface version that supports IPv6. Consider the following information for CTI applications and CTI port/route points:

- CTI applications connect to CTI Manager by using either an IPv4 or an IPv6 address. If you set the Enable IPv6 enterprise parameter to True in Cisco Unified Communications Manager Administration, CTI Manager can support CTI connections from applications that use IPv6 addresses.
- CTI applications can register CTI ports/route points that use IPv6 or IPv4 addresses. CTI applications that handle media events for CTI ports/route points can register devices with either a IPv4 or IPv6 address, depending on the configuration for the device.
- CTI applications can monitor/control CTI-supported devices that have IPv6 capability.
- If a call uses IPv6, IPv6 information, including CallingPartyAddress and media IP address, gets passed to the CTI application.

Cisco IP Voice Media Streaming Application Service

The Media Termination Point (MTP) device, software conference bridge, annunciator, and unicast Music On Hold provided by the Cisco IP Voice Media Streaming Application service support both IPv4 and IPv6 audio media connections. The MTP device, software conference bridge, annunciator, and unicast Music On Hold are configured automatically in dual mode when the platform is configured for IPv6 and the IPv6 enterprise parameter is enabled. If the platform is not configured for IPv6, the MTP device, software conference bridge, annunciator, and unicast Music On Hold are configured automatically in IPv4 only mode.

The MTP device, software conference bridge, annunciator and Music On Hold support only IPv4 for the TCP control channel. The annunciator, Music On Hold, and MTP in pass-through mode support secure media SRTP connections to both IPv4 and IPv6 addresses.

Note Multicast Music On Hold supports only IPv4.

Cisco Unified CM

This section describes how Cisco Unified Communications Manager supports devices that use IPv4, IPv6, or IPv4 and IPv6. In addition, this section describes how Cisco Unified Communications Manager runs in dual-stack mode, how Cisco Unified Communications Manager can process calls for IPv4 and IPv6 devices, and how Cisco Unified Communications Manager can reserve and allocate bandwidth for IPv4 and IPv6 calls.

Tip This document uses the terminology, dual stack (or dual-stack mode), which assumes that the device or server uses both an IPv4 and an IPv6 address.

Cisco Unified Communications Manager Server

Cisco Unified Communications Manager can interact with and support devices that use IPv6 only, but you cannot configure the Cisco Unified Communications Manager server as IPv6 only because Cisco Unified Communications Manager must interact with and support devices/features that support IPv4 only (or both IPv4 and IPv6). For Cisco Unified Communications Manager to support devices that use IPv6, including dual-stack devices, which can provide both IPv4 and IPv6 addresses, you must configure Cisco Unified Communications Manager, so it runs in dual-stack mode; that is, you must ensure that the Cisco Unified Communications Manager server has both an IPv4 address and an IPv6 address that is configured for it, so it can interact and support devices that use IPv4 only, IPv6 only, or both IPv4 and IPv6.

Tip Intracluster Cisco Unified Communications Manager node-to-node communication uses IPv4.

Before the Cisco Unified Communications Manager server can run in dual-stack mode, you must perform the following tasks:

Call Processing

By running in dual-stack mode, Cisco Unified Communications Manager can set up calls under the following circumstances:

- When all devices support IPv4 only.
- When all devices support IPv6 only.
- When all devices run in dual-stack mode, in which case, Cisco Unified Communications Manager uses the configuration for the IP Addressing Mode Preference for Signaling setting for signaling events and the IP Addressing Mode Preference for Media enterprise parameter for media events.
- When one device supports IPv4 and another device supports IPv6, in which case, Cisco Unified Communications Manager attempts to insert into the call an MTP that can translate IPv4 to IPv6.

Tip Even if your device can support multiple IPv6 addresses, Cisco Unified Communications Manager only handles one IPv6 address. In addition, if your device supports an IPv4 and IPv6 address, Cisco Unified Communications Manager can simultaneously handle both addresses.

Call Admission Control (CAC)

Because using IPv6 requires 20 more bytes of data in its header than IPv4, an IPv6 call requires more bandwidth than a similar IPv4 call that uses the same codec/media payload type. For example, a G.711 call that uses IPv4 uses 80 kb/s of bandwidth; whereas, a G.711 call that uses IPv6 uses 88 kb/s of bandwidth.

To reserve and adjust location-based bandwidth for a call that uses IPv6, Cisco Unified Communications Manager can calculate the bandwidth that is needed for an IPv6 call for all codecs that are supported with Cisco Unified Communications Manager. After the device contacts Cisco Unified Communications Manager for bandwidth reservation during the call setup, Cisco Unified Communications Manager identifies the IP version; if the call uses IPv6, Cisco Unified Communications Manager reserves the bandwidth for IPv6, and if the call uses IPv4, Cisco Unified Communications Manager reserves the bandwidth for IPv4. If Cisco Unified Communications Manager cannot identify the IP version that is used for the call, for example, the call terminates to a SIP trunk or the device supports both IP versions, Cisco Unified Communications Manager initially reserves bandwidth that supports IPv6 and later adjusts the bandwidth after media negotiation occurs.

Tip Cisco Unified Communications Manager reserves bandwidth for one call leg at a time, so, if an MTP is inserted into the call and location-based CAC is required, ensure that the MTP is colocated with one of the devices, so location-based CAC reserves the bandwidth across the WAN based on the side that is opposite of the MTP. For example, if a call occurs from an IPv4 to IPv6 device, which causes an insertion of the MTP on the IPv4 side, Cisco Unified Communications Manager reserves bandwidth across the WAN based on IPv6. Alternatively, if the MTP is inserted for the device that uses IPv6, Cisco Unified Communications Manager reserves bandwidth across the WAN based on IPv4.

If you want to do so, you can configure the Call Counting CAC Enabled, Audio Bandwidth for Call Counting CAC, and the Video Bandwidth Unit for Call Counting CAC service parameters in Cisco Unified Communications Manager, so the call uses a fixed bandwidth value instead of having Cisco Unified Communications Manager reserve and adjust bandwidth during the call. Be aware that configuring these service parameters can cause Cisco Unified Communications Manager to oversubscribe or undersubscribe bandwidth for the call.

Procedure

Step 1 On the Cisco Unified Communications Manager server, enable IPv6 in the Cisco Unified Communications Operating System.

Step 2 Determine how the Cisco Unified Communications Manager server will get its IPv6 address, and ensure that the Cisco Unified Communications Manager server obtains its IPv6 address.

In the Cisco Unified Communications Operating System, you can request a non-link-local address from the DHCPv6 server, configure a static non-link-local IPv6 address for the Cisco Unified Communications Manager server, or obtain an non-link-local IPv6 address via stateless address autoconfiguration. (Cisco recommends a static non-link-local IPv6 address for the server.)

Ensure that the Cisco Unified Communications Manager server only obtains one non-link local IPv6 address. If the server obtains more than one IPv6 address, Cisco Unified Communications Manager may not behave as expected.

If the Cisco Unified Communications Manager server obtains an IPv6 address via stateless address autoconfiguration and you also have a static IPv6 address that is configured for the server, Cisco Unified Communications Manager ignores the IPv6 address that is obtained via stateless address autoconfiguration and uses the static address.

Step 3 For Cisco Unified Communications Manager, set the Enable IPv6 enterprise parameter to True, which ensures that Cisco Unified Communications Manager runs in dual-stack mode.

Caution You must enable IPv6 in the Cisco Unified Communications Operating System and set the Enable IPv6 enterprise parameter to True. If you do not perform both of these tasks, the Cisco CallManager service runs in IPv4 and phones that you configure with an IP Addressing Mode of IPv6 Only cannot register with Cisco Unified Communications Manager.

Caution After you perform these tasks on the server, you must restart the server for the changes to take effect.

Step 4 In Cisco Unified Communications Manager Administration, configure the Host Name/IP Address and IPv6 Name fields in the Server Configuration window, which ensures that Cisco Unified Communications Manager runs in dual-stack mode. Cisco Unified Communications Manager considers the Host Name/IP Address field mandatory; that is, you must configure this field even if devices in your network only support IPv6. If devices in your network support IPv6 only or IPv4 and IPv6, you must configure the IPv6 Name field in addition to the IP Address/Hostname field; be aware that you must enter the non-link local IPv6 address for the Cisco Unified Communications Manager in the IPv6 Name field.

The phones use these fields, which are included in the TFTP configuration file, to retrieve the IP addresses of the Cisco Unified Communications Manager server, so phone registration occurs.

Related Topics

Cisco Unified IP Phones, on page 745
Media Termination Points, on page 751
SIP Trunks, on page 753
Interactions and Restrictions, on page 756
Configure Service and Enterprise Parameters for IPv6, on page 765

Cisco Unified IP Phones

This section describes use cases for IPv4 and IPv6 calls between the phone and Cisco Unified Communications Manager. This section does not describe how the phone gets its IP address and other network settings.

Tip For additional information on using IPv6 with your phone, see the Cisco Unified IP Phone Administration Guide that supports your phone model and this release of Cisco Unified Communications Manager. The phone administration guide describes IPv6 settings that display on the phone.

See the following use cases, which assume that Cisco Unified Communications Manager can listen on the correct port, that an MTP is available to translate IP address versions, and that the device has the correct address version.

Tip Every time that the phone boots up, it boots up in dual-stack mode; that is, it can support both IPv4 and IPv6. After the phone processes the configuration file from the TFTP server, the IP Addressing Mode from the Common Device Configuration window gets set on the phone. Based on the IP Addressing Mode, the phone may disable DHCP or DHCPv6 and may release addresses that do not support the IP Addressing Mode; for example, if the IP Addressing Mode is IPv6 Only, the phone releases the IPv4 address.

Tip If the phone has multiple, unique local or multiple global addresses, the first address that is assigned to the phone specifies the address that gets sent to Cisco Unified Communications Manager for signaling and media events. If a phone that runs in dual-stack mode loses a specific address type, the phone unregisters from Cisco Unified Communications Manager and reregisters with the remaining address type.

Tip For media negotiation, Cisco Unified Communications Manager dynamically determines the IP address to use for the call; that is, Cisco Unified Communications Manager identifies whether the devices share the IP Addressing Mode. For example, if one device has an IP Addressing Mode of IPv4 and IPv6 and the other device has an IP Addressing Mode of IPv4 Only, Cisco Unified Communications Manager uses IPv4 for the media negotiation and requires no MTP for translating IP address versions. If the devices on the call only support one IP address version and the versions are not compatible, Cisco Unified Communications Manager uses the IP address version of the device and tries to insert an MTP into the call that can translate IPv4 to IPv6. If all devices on the call support both IP address versions, Cisco Unified Communications Manager uses the configuration for the IP Addressing Mode Preference for Media enterprise parameter for the media negotiation.

Phone Has IP Addressing Mode of IPv4 Only

If the IP Addressing Mode for the phone is IPv4 Only, the phone connects to Cisco Unified Communications Manager by using an IPv4 address. Signaling and media negotiation occurs by using an IPv4 address. If an IPv4 address is not available for the phone, the user cannot make calls.

Phone Has IP Addressing Mode of IPv6 Only

If the IP Addressing Mode for the phone is IPv6 Only and you set the Enable IPv6 enterprise parameter to True, the phone uses a global scope or unique local scope IPv6 address to connect to Cisco Unified Communications Manager. Signaling and media negotiation occur by using this IPv6 address. If an IPv6 address is not available for the phone, the user cannot make calls. Likewise, if an IPv6 address is not configured for the phone, the phone cannot register with Cisco Unified Communications Manager.

Tip Cisco Unified Communications Manager does not support all features on phones where the IP Addressing Mode is IPv6 Only. For a list of features that are not supported, see the Interactions and Restrictions, on page 756.

Phone Has IP Addressing Mode of IPv4 and IPv6

If the IP Addressing Mode for the phone is IPv4 and IPv6 (dual stack mode) and you set the Enable IPv6 enterprise parameter to True, Cisco Unified Communications Manager considers the IP address support for the phone and the configuration for IP Addressing Mode Preference for Signaling setting before connecting the call.

If only one IP address version is available on the phone, the phone uses the address that is available to connect to Cisco Unified Communications Manager for signaling negotiation. If both IP addresses types are available on the phone, the phone uses the configuration for the IP Addressing Mode for Signaling setting for signaling negotiation.

The following table lists the endpoints and protocols that support both IPv4 and IPv6 addressing:

Table 85: Dual Stack Support for Endpoints

Protocol	Endpoint
SCCP	Cisco Unified IP Phones: • 6901 • 6911 • 6921 • 6941 • 6945 • 6961 • 7906G • 7911G • 7931G • 7942G • 7945G • 7962G • 7965G • 7975G

SIP	Cisco Unified SIP Phone 3905 Cisco Unified IP Phones: • 7821 • 7841 • 7861 • 8961 • 9951 • 9971 SIP Telepresence endpoints: • C-series (C90, C60, C40, C20) • Profile-series • SX-series (SX20) • MX-series (MX200, MX300) • EX-series (EX60, EX90) Cisco Desktop Collaboration Experience Phone: • DX650
SIP and SCCP	Cisco Unified IP Phones: • 6921 • 6941 • 6945 • 6961

Tip After you configure the phone in Cisco Unified Communications Manager Administration, you can view the IP address for the phone in the Find and List Phones window. The window displays addresses for IPv4-only endpoints and IPv6-only endpoints, as well as for endpoints that have both IPv4 and IPv6 addresses (dual-stack). The address displays for the mode in which the endpoint is operating and lists "unknown" for the addressing mode that is not in use. You can click the IPv4 or IPv6 address in the Find and List Phones window, which points to the URL for the web server on the phone. This function is not available for phones that do not support IPv6 web servers, such as phones running SCCP IPv6.

Tip In the Phone Configuration window for a specific phone, you can view the IPv4 address and the IPv6 address, if applicable, that the phone uses. For phones in dual-stack mode that have both an IPv4 and IPv6 address, you can click the IPv4 or IPv6 address in the Phone Configuration window, which points to the URL for the web server on the phone. This function is not available for phones that do not support IPv6 web servers, such as phones running SCCP IPv6.

SIP Endpoints

IP endpoints that use Session Initiation Protocol (SIP) can register with Cisco Unified Communications Manager using an IPv6 address. After these endpoints have registered with Cisco Unified Communications Manager , they can operate in IPv6 Only mode, IPv4 Only mode, or in dual stack mode using the ANAT extension.

Cisco Unified Communications Manager supports all media types for calls that originate from and terminate on IPv6/dual stack SIP endpoints on the same cluster and on different clusters over SIP trunks. The supported media types include:

- audio
- video
- BFCP
- FECC
- IX channels

You can specify the signaling and media address preference for these endpoints types by using the settings on the Common Device Configuration and Enterprise Parameter panel. If you configure the endpoint as dual-stack and both IPv4 and Ipv6 addresses are available, the endpoint uses the IP Addressing Mode Preference for Signaling setting to determine which addressing mode to use. The endpoint uses the IP Addressing Mode Preference for Media setting to advertise the ANAT address preference in the dual-stack offer SDP. For more information about these settings, see the *Cisco Unified Communications Manager Administration Guide*.

DHCPv6

DHCPv6, which is the version of Dynamic Host Configuration Protocol that supports IPv6, can assign an IPv6 address and other network settings to the phone after you connect it to the network. In addition, DHCPv6 can assign an IPv6 address to the Cisco Unified Communications Manager server; that is, if you do not plan to assign a static IP address to the server. (Cisco recommends that you assign a static IP address to the server.)

Cisco Unified Communications Manager does not provide DHCPv6 server capabilities, so you must configure a DHCPv6 server in your network if you plan to use DHCPv6 to assign IPv6 network configuration settings to the phone or server. If you want to allow the phone to receive its IP address via DHCPv6 rather than stateless address autoconfiguration, make sure that you set the Allow Auto-Configuration for Phones setting to Off. For information on this setting, see the Access IPv6 and IPv4 Configuration in Unified CM Administration, on page 768.

Note Because Cisco Network Registrar (CNR) 6.2 provides both DNS and DHCP support for IPv4 and IPv6, consider using Cisco Network Registrar for your DNS and DHCP support. For more information on this product, see the Cisco Network Registrar User's Guide, 6.2.

Note If you want to do so, you can configure a Cisco IOS router or switch as a DHCPv6 server; for example, you can configure a Cisco Catalyst 3560 Series Switch or a Cisco Catalyst 3750 Series Switch that runs 12.2(46)SE (or later) as a DHCPv6 server. Before you configure this router/switch, verify that your router/switch supports the Cisco vendor-specific DHCPv6 information options that are required for IPv6 and DHCPv6 support.

Note For highest scope rules, consider configuring a DHCPv6 server, so it assigns only unique local addresses to the phone. If you must use global unicast addresses, configure a TLS connection and SRTP, as described in the Cisco Unified Communications Manager Security Guide.

Tip For additional information on DHCP, see the *Cisco Unified Communications Manager System Guide*, and *Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager*.

DNS

For IPv6, DNSv6 handles the AAAA record, which can map IPv6 addresses. For IPv4, DNS handles the A record, which can map IPv4 addresses. For IPv4 and IPv6, the following fields rely on DNS; that is, if you configure hostnames for the fields:

- Host Name/IP Address (Server Configuration window) - You can enter an IPv4 address or host name.
- IPv6 Name (Server Configuration window) - You can enter an IPv6 address or host name.
- Destination Address (SIP Trunk Configuration window) - You can enter a valid V4 dotted IP address, a fully qualified domain name (FQDN), or DNS SRV record if the SIP trunk is configured to use a DNS SRV port as a destination.
- Destination Address IPv6 (SIP Trunk Configuration window) - You can enter a valid IPv6 address (global unicast, unique local, or a hostname), a fully qualified domain name (FQDN), or a DNS SRV record if the SIP trunk is configured to use a DNS SRV port as a destination.

Caution You can provision your DNS server for IPv6 prior to upgrading from Cisco Unified Communications Manager to the current release. However, do not configure the DNS records for Cisco Unified Communications Manager for IPv6 until after you complete the upgrade to the current release. If you configure the DNS records for Cisco Unified Communications Manager for IPv6 before you complete the upgrade, the upgrade can fail and cause your system to become nonfunctional after you reboot.

Caution If the AAAA record or A record do not map correctly, calls may fail.

Note Because Cisco Network Registrar (CNR) 6.2 provides both DNS and DHCP support for IPv4 and IPv6, consider using CNR for your DNS and DHCP support. For more information on this product, see the Cisco Network Registrar User's Guide, 6.2.

Gateways

MGCP and H.323 gateways do not support devices that function in IPv6-only mode. To communicate with IPv6-only devices that connect to these gateways, Cisco Unified Communications Manager inserts an MTP that can translate IPv4 to IPv6 during a call.

The Cisco ATA 186 and 188 Analog Telephone Adaptors do not support IPv6.

Analog phone gateways can operate in IPv4 only, IPv6 only, or IPv4 and IPv6 (dual-stack mode).

The following gateway models are supported for IPv6:

- MTP/Transcoder: ISR G2 29XX and 39XX
- SIP Gateways (hardware platform configuration): ISR G2 29XX and 39XX, AS5350XM, and AS5400XM
- SIP Gateways (number of ports that are supported): VG350, VG224, VG204XM, and VG202XM
- SCCP Analog Gateways: VG350, VG224, VG204XM, and VG202XM

Cisco IOS SIP gateways can support IPv6 only, IPv4 only, or IPv4 and IPv6 simultaneously in dual-stack mode. Before Cisco Unified Communications Manager can interact with these gateways, you must configure it in the SIP Trunk Configuration window in Cisco Unified Communications Manager Administration. For Cisco Unified Communications Manager considerations for the gateway, review the SIP Trunks, on page 753 and the Media Termination Points, on page 751. In addition to configuring the gateway in Cisco Unified Communications Manager Administration, you must configure the gateway, as described in *Implementing VoIP for IPv6*.

Media Termination Points

Both Cisco IOS Enhanced MTP and the software MTP provided by the Cisco IP Voice Media Streaming Application support the following:

- IPv4 to IPv6 translation
- media interoperation between IPv4 and IPv6 networks
- dual-stack mode

The software MTP does not support multimedia capability. When the software MTP is used for IPv4 to IPv6 translation, the call becomes audio-only.

This section describes how Cisco Unified Communications Manager inserts MTPs into calls that require IPv4 to IPv6 translation. For information on how to configure your Cisco IOS MTP so that the MTP can support IP translation, see *Implementing VoIP for IPv6*.

Note Although the Cisco IOS MTP can support multiple IPv6 addresses, the MTP sends either a global or unique local address to Cisco Unified Communications Manager for signaling and media events.

Tip When Cisco Unified Communications Manager allocates an MTP, the MTP may get used for more than one feature at the same time. Because the MTP can get used for multiple features, Cisco Unified Communications Manager prioritizes MTP allocation to ensure that IPv6 and IPv4 are supported before other features that rely on MTP get supported.

Under the following circumstances, Cisco Unified Communications Manager inserts an MTP that can translate IPv4 to IPv6 (or vice versa):

- The devices on the call do not support the same IP address version.
- For the SIP trunk, you check the Media Termination Points Required check box or configure the Use Trusted Relay Point as On and Cisco Unified Communications Manager is communicating with devices that use IPv6 addresses. If you check the Media Termination Points Required check box for the SIP trunk or you need an MTP inserted into the call for any other reason besides IPv4 to IPv6 translation, the following considerations exist:
    - If both parties of the call can negotiate IPv4 without using an MTP, Cisco Unified Communications Manager does not insert an MTP into the call.
    - When the IP Addressing Mode is IPv6 Only or IPv4 and IPv6 for the SIP trunk, Cisco Unified Communications Manager allocates an MTP that can translate IPv4 to IPv6 (or vice versa) for the call. If no MTP that can translate IP address versions is available for the call, Cisco Unified Communications Manager allocates an MTP that supports IPv4 for the SIP trunk that is configured in dual-stack mode; for a SIP trunk that is configured as IPv6 Only, Cisco Unified Communications Manager sends an INVITE message without SDP session descriptions.

When Cisco Unified Communications Manager communicates with the MTP, Cisco Unified Communications Manager requests either an IPv4 or IPv6 address. If Cisco Unified Communications Manager requests an IPv4 address, the MTP opens an RTP port that supports IPv4. If Cisco Unified Communications Manager supports IPv6, the MTP opens an RTP port that supports IPv6.

If the request for an MTP that can translate IPv4 to IPv6 fails, the call may fail because IPv6 is required for the call. If an MTP that can translate IP address versions is inserted into the call, any intermediate media device that is inserted between the IPv6 device and the MTP must handle IPv6 requests. If Cisco Unified Communications Manager has two MTPs available and each MTP can perform only one function, Cisco Unified Communications Manager attempts to insert both MTPs into the call, the first MTP for the IPv4-to-IPv6 translation and the second MTP to support other features that require MTP. If a call requires a transcoder and an IPv6-capable MTP and the available transcoder does not support IPv6, Cisco Unified Communications Manager tries to insert the IPv6-capable MTP on the leg of the call that supports IPv6 and the transcoder on the leg of the call that supports IPv4; under these circumstances, the call fails if the IP address capabilities do not match between the MTP and transcoder.

Note For information on specific call scenarios where SIP trunks (and MTPs) get used, see *Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager*.

SIP Trunks

If configured appropriately, SIP trunks can interact with devices that support IPv4 only, IPv6 only, or dual stack mode (IPv4 and IPv6). Just like Cisco Unified Communications Manager and other components, the SIP trunk uses the configuration for the Enable IPv6 enterprise parameter to determine whether to support devices that use IPv6.

IPv4 or IPv6 Signaling for SIP Trunks

The following factors determine whether to use IPv4 or IPv6 for signaling events for SIP trunks:

- The direction of the call
- IP Addressing Mode for the SIP trunk, as configured in the Common Device Configuration window and applied to the trunk
- IP Addressing Mode Preference for Signaling configuration for the SIP trunk, as configured in the Common Device Configuration window (or Enterprise Parameter Configuration window) and applied to the trunk
- Configured Destination Address(es) for the SIP trunk

  If you configure only one destination address, that is, either the Destination Address, which supports IPv4, or the Destination IPv6 Address, which supports IPv6, ensure that the IP Addressing Mode that you configure for the SIP trunk matches the IP address type that you configured for the destination address. If the configuration does not match, no call gets established over the trunk.

  If you configure both the Destination Address and the Destination IPv6 Address, make sure that you configure the IP Addressing Mode as IPv4 and IPv6, so the trunk is in dual-stack mode. For a dual-stack trunk, the IP Addressing Mode Preference of Signaling configuration that you applied to the SIP trunk determines whether IPv4 or IPv6 gets used for signaling events for outgoing calls over SIP trunks.

IPv4 or IPv6 Media for SIP Trunks

The following factors determine whether to use IPv4 or IPv6 for media events for SIP trunks:

- The direction of the call
- Whether the call is an early offer or delayed offer call
- IP address preference in the SDP offer
- IP Addressing Mode for the SIP trunk, as configured in the Common Device Configuration window and applied to the trunk
- Configuration for the IP Addressing Mode Preference for Media enterprise parameter, as configured in the Enterprise Parameter Configuration window
- Configuration for the Enable ANAT check box (and whether ANAT is required or supported in the INVITE)
- IP Addressing Mode for the phone

Note For information on specific call scenarios where SIP trunks (and MTPs) are used, see *Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager*.

IPv6 Video Interoperability

Cisco Unified Communications Manager supports the transmission of video and application media streams on SIP lines and SIP trunks in IPv6 mode as well as in dual stack mode.

Cisco Unified Communications Manager also supports interworking with other Unified Communications Manager clusters and Video Communications Servers (VCS) over SIP lines and SIP trunks that have been configured to use IPv4 or IPv6.

IP Address Negotiation

For media negotiation for dual-stack devices, Cisco Unified Communications Manager dynamically determines the IP address to use for the call; that is, if any device on the call only supports one IP version, that IP version gets used, and an MTP that can translate IP versions gets inserted into the call. If all devices on the call support both IP versions, and same ANAT address preference is specified by both the devices or at least by one device, that preferred address is negotiated for media. However, if ANAT address preference that is advertised by both devices do not match on both sides or both the devices do not advertise any address preference, for example SCCP, then the configuration for the IP Addressing Mode Preference for Media enterprise parameter gets used.

TFTP Server

The TFTP server uses IPv4 to communicate with most components, such as the database, in Cisco Unified Communications Manager. If configured appropriately, however, the TFTP server can communicate with devices that use IPv4, IPv6, or both types of addresses.

Running in dual-stack mode, the TFTP server can respond to file requests from both IPv4 and IPv6 networks. For requests from IPv4 networks, the TFTP server responds by using an IPv4 stack; for requests from IPv6 networks, the TFTP server responds by using an IPv6 stack; that is, if you set the Enable IPv6 enterprise parameter to True.

IPv6 support applies to TFTP requests from devices and HTTP requests from off-cluster TFTP servers where the local TFTP server is configured as their alternate file server.

Tip In an IPv6 network, the DHCPv6 server uses the Cisco vendor-specific DHCPv6 information options in the DHCPv6 response message to pass the TFTP IPv6 address to the device. If the device obtains an IPv6 address and sends a request to the TFTP server while the TFTP server is using IPv4 to process requests, the TFTP server does not receive the request because the TFTP server is not listening for the request on the IPv6 stack. In this case, the device cannot register with Cisco Unified Communications Manager.

Tip For more information on the Cisco vendor-specific DHCPv6 information options, see the *Cisco Unified Communications Manager System Guide* and *Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager*.

The TFTP server uses the configuration for the Enable IPv6 enterprise parameter to determine how to communicate with the phone. If you set the Enable IPv6 enterprise parameter to False, the TFTP server uses IPv4 to communicate with the phone. If you set the parameter to True, the TFTP server uses IPv4 or IPv6, depending on the IP Addressing Mode for the phone. If the configuration changes for the Enable IPv6 enterprise parameter, the TFTP server receives a change notification with the new configuration, and the TFTP server enables or disables its IPv6 capabilities without requiring you to restart the Cisco TFTP service.

The configuration file that the TFTP server serves to the phone contains the configuration for the following settings:

- IP Addressing Mode, IP Addressing Mode Preference for Signaling, IP Addressing Mode Preference for Media, and Allow Auto-Configuration for the Phone
- Host Name/IP Address (IPv4 setting) for the Cisco Unified Communications Manager node
- IPv6 Name for the Cisco Unified Communications Manager node (only if you set the Enable IPv6 enterprise parameter to True)
- IPv6 address for the CAPF server (only if you set the Enable IPv6 enterprise parameter to True and activate the Cisco Certificate Authority Proxy Function service)

Before the TFTP server can serve configuration files to phones that use IPv6 addresses, you must set the Enable IPv6 enterprise parameter to True. If this parameter is set to False, the TFTP server uses an IPv4 address in the configuration file, even if you configured an IP Addressing Mode of IPv6 Only for the devices.

The TFTP server obtains the IPv4 and/or IPv6 address from the Cisco Unified Communications Operating System and listens on those addresses for file requests from the phone.

In the Service Parameter Configuration window, you can also configure alternate Cisco file servers, which are TFTP servers that are on a different cluster. These parameters, which support either IPv4 or IPv6 addresses or host names that resolve to an IP address, determine the IP stack that the TFTP uses to communicate between primary and alternate file servers. If an alternate file server supports dual-stack mode and you want to set both IPv4 and IPv6 addresses for the same server in these parameter fields, you must add both IP addresses, one per field, and the TFTP server tries each address in the order that you configure.

System Requirements for IPv6

The following IPv6 system requirements exist for Cisco Unified Communications Manager:

- Cisco Unified Communications Manager installed on each server in the cluster
- DHCPv6 server that can issue IPv6 addresses and DNS server that can resolve host names to IPv6 addresses; consider using Cisco Network Registrar (CNR).

  If you want to do so, you can configure a Cisco IOS router or switch as a DHCPv6 server; for example, you can configure a Cisco Catalyst 3560 Series Switch or a Cisco Catalyst 3750 Series Switch that runs 12.2(46)SE (or later) as a DHCPv6 server. Before you configure this router/switch, verify that your router/switch supports the Cisco vendor-specific DHCPv6 information options that are required for IPv6 and DHCPv6 support.
- Cisco IOS release that is compatible with the current release of Cisco Unified Communications Manager, and that is installed and configured on the gateways and the Cisco IOS MTP

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://www.cisco.com/go/cfn`.

You do not need a Cisco.com account to access Cisco Feature Navigator.

Interactions and Restrictions

Some Cisco Unified Communications Manager features do not work for devices with an IP Addressing Mode of IPv6 Only. Before you configure IPv6 Only for a device, review the following section, which describes Cisco Unified Communications Manager feature interactions and restrictions for IPv6.

Caution You must enable IPv6 in the Cisco Unified Communications Operating System and set the Enable IPv6 enterprise parameter to True; if you do not perform both of these tasks, the Cisco CallManager service runs in IPv4, and phones that you configure with an IP Addressing Mode of IPv6 Only cannot register with Cisco Unified Communications Manager. After you perform these tasks, remember to restart the node. For the order of tasks that you perform for IPv6, see Configure IPv6, on page 740.

Caution You can provision your DNS server for IPv6 before you perform an upgrade to the current release. However, do not configure the DNS records for Cisco Unified Communications Manager for IPv6 until after you complete the upgrade. Configuring the DNS records for Cisco Unified Communications Manager for IPv6 before you perform the upgrade causes the upgrade to fail and causes your system to become nonfunctional after you reboot.

Bulk Administration Tool

For information on how the Bulk Administration Tool (BAT) supports IPv6, see the *Cisco Unified Communications Manager Bulk Administration Guide*.

Call Detail Records

When IPv6 is used for a call, call detail records (CDRs) can display IPv6 addresses. For more information on CDRs, see the *Cisco Unified Communications Manager Call Detail Records Administration Guide*.

Cisco Certificate Authority Proxy Function

For information on how Cisco Certificate Authority Proxy Function works with IPv6, see the *Cisco Unified Communications Manager Security Guide*.

Cisco Extension Mobility

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, make sure that you configure the phone with an IP Addressing Mode of IPv4 Only or IPv4 and IPv6.

Cisco Unified Communications Manager CDR Analysis and Reporting

For information on Cisco Unified Communications Manager CDR Analysis and Reporting, see the *Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide*.

Cisco Unified Communications Operating System

See the Configure IPv6, on page 740 and the Run IPv6 CLI Commands or Configure IPv6 in the Ethernet IPv6 Window, on page 762.

Cisco Unified Serviceability

Alarms that report IPv4 addresses may also report IPv6 addresses, depending on the configuration in your network. For information on how to configure alarms and view alarm definitions in Cisco Unified Serviceability, see the *Cisco Unified Serviceability Administration Guide*.

SNMP supports IPv4, although the CISCO-CCM-MIB includes columns and storage for IPv6 addresses, preferences, and so on.

Cisco Unity Connection and Cisco Unity

Cisco Unity Connection supports dual-stack mode for SIP or SCCP interfaces. Cisco Unity communicates with Cisco Unified Communications Manager using IPv4.

Cisco Unified Communications Manager Assistant

Cisco Unified Communications Manager Assistant does not support IPv6, so you cannot use phones with an IP Addressing Mode of IPv6 Only with Cisco Unified Communications Manager Assistant. If you want to use Cisco Unified Communications Manager Assistant with the phone, make sure that you configure the phone with an IP Addressing Mode of IPv4 Only or Dual Stack (with IPv4 and IPv6 addresses).

Real Time Monitoring Tool

In RTMT, you can monitor CTI applications, CTI devices, and CTI lines that use IPv6 addresses. When you search for the CTI application, CTI device, or CTI line, enter the IPv6 address, and check the **AppIpv6Addr** check box in the attribute window.

In addition, you can perform a device search on phones or SIP trunks that use IPv6 addresses. When you choose **CallManager** > **Device Search** > **Open Device Search** > **Phones** (or **SIP Trunks**), make sure that you specify an IPv6 address and check the **Ipv6Address** check box in the attributes window.

Log files may display IPv4 and IPv6 addresses, depending on the configuration in your network.

In RTMT, performance monitoring counters display for the IP6 object.

Cisco Web Dialer

Cisco Web Dialer supports IPv4, so, to connect to CTI Manager, Cisco Web Dialer uses an IPv4 address. Cisco Web Dialer works with devices with an IP Addressing Mode of Dual Stack (with IPv4 and IPv6 addresses).

Conferences (Audio)

The conference feature in Cisco Unified Communications Manager supports the following protocols:

- Dual-stack mode for the software conference bridge provided by the Cisco IP Voice Media Streaming Application
- IPv4-only mode for Cisco IOS conference bridges

Note Security is not supported when the conference bridge is provided by the Cisco IP Voice Media Streaming Application.

During a conference, if an endpoint supports IPv4 only, the IPv4 media is negotiated between the endpoint and the conference bridge. The SIP trunk-to-MCU is configured in IPv4 only mode when the MCU is used for the conference.

If the endpoint supports IPv6 only, IPv6 media is negotiated between the endpoint and the conference bridge.

Dual-stack mode is supported when the conference bridge is provided by the Cisco IP Voice Media Streaming Application. If dual-stack mode is also supported by the SCCP endpoint, the media preference configured in the enterprise parameter (IPv4 or IPv6) is negotiated between the endpoint and the conference bridge. If dual-stack mode with ANAT is supported by the SIP device, the ANAT address preference advertised by the SIP device is negotiated between the SIP device and the conference bridge. Cisco Unified Communications Manager does not need to insert an MTP for IPv4 to IPv6 translation when the conference bridge is provided by the Cisco IP Voice Media Streaming Application. Cisco Unified Communications Manager inserts an MTP only if you are using a conference bridge that does not support dual-stack mode conferences.

If an MTP is inserted in a conference, for it to support security you must configure the MTP in pass-through mode, which means that the MTP does not transform the media payload during the call. When you configure an MTP in pass-through mode, the MTP receives the encrypted packet on one call leg and sends out the same packet on a different leg of the call. For secure conferences with secure conference bridges that do not support dual mode and encrypted devices with an IP Addressing Mode of IPv6 Only, Cisco Unified Communications Manager inserts an MTP into the conference to translate IPv4 to IPv6 (and vice versa). If you configure the MTP for pass-through mode, the encrypted IPv6 phones communicate with the conference bridge using SRTP. If you do not configure the MTP for pass-through mode, the media gets downgraded to RTP.

Conferences (Video)

The video conference feature supports IPv4 mode with conductors and MCUs. If an endpoint supports IPv4-only, IPv4 media is negotiated between the endpoint and the conference bridge. The SIP trunk-to-MCU is configured in IPv4-only mode when the MCU is used for the conference.

For IPv6-only devices, Cisco Unified Communications Manager inserts an MTP into the conference to translate IPv4 to IPv6. Video conferencing using IPv6 is not supported on Cisco IOS conference bridges.

Device Mobility

Device mobility supports IPv4 addresses only, so you cannot use phones with an IP Addressing Mode of IPv6 Only with device mobility.

Differentiated Services Control Point (DSCP)

Be aware that Differentiated Services Control Point (DSCP) values are the same for both IPv6 and IPv4.

Disaster Recovery System

For information on Disaster Recovery System, see the *Disaster Recovery System Administration Guide*.

Early Offer Support for Voice and Video Calls

IPv6 is not supported for early-offer calls over outbound SIP Trunks. You can enable or disable this feature using the **Early Offer support for voice and video calls (insert MTP if needed)** check box on the SIP Profile panel.

H.323 Devices

H.323 clients, gateways, and H.225 intercluster trunks do not support IPv6. To communicate with IPv6-only devices that connect to these gateways, Cisco Unified Communications Manager inserts an MTP that can translate IPv4 to IPv6 during a call.

IM and Presence Service

Changes that you make to enterprise parameters using Cisco Unified Communications Manager Administration also change the enterprise parameter settings for IM and Presence Service clusters in your deployment.

⚠

Caution You must enable the IPv6 enterprise parameter for the IM and Presence Service node and enable the IPv6 Ethernet IP setting for Eth0 on each IM and Presence Service node using Cisco Unified IM and Presence Operating System Administration; otherwise, the node attempts to use IPv4 for IP traffic. Any packets that are received that have an IPv6 address will not be delivered. For more information, see the *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.

The node cannot revert to using IPv4 if the node is configured to use an IPv6 connection to an external database, LDAP server or Exchange server, or if a federation deployment using IPv6 is configured for the node.

Intercom

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 initiated intercom.

Mobile Connect and Mobile Voice Access

Cisco Unified Mobility features in Cisco Unified Communications Manager, such as Mobile Connect and Mobile Voice Access, support IPv4. Mobility features are also supported on IPv6, with the exception of Mobile Voice Access. If conversion between IPv4 and IPv6 is required to support a mobility feature, such as when a mobile phone uses IPv4 and another phone uses IPv6, Cisco Unified Communications Manager inserts a Media Termination Point (MTP) that can translate IPv4 to IPv6 into the call.

Monitoring and Recording

For monitoring and recording, the phone can handle an IPv4 media stream for customer-to-agent calls while it handles an IPv6 media stream for recording and monitoring (or vice versa).

Music On Hold

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. So, devices with an IP Addressing Mode of IPv6 Only cannot support multicast Music On Hold. Under these circumstances, Cisco Unified Communications Manager plays a tone, instead of music, when the phone is on hold. However, devices with an IP Addressing Mode of IPv6 only can stream unicast Music On Hold without Cisco Unified Communications Manager inserting an MTP for IPv4 to IPv6 conversion.

NTP Servers

To avoid potential compatibility, accuracy, and network jitter problems, ensure that the external NTP servers that you specify for the primary node are NTP v4 (version 4).

QRT

Users with phones with an IP Addressing Mode of IPv6 Only cannot report audio and other problems by pressing the QRT softkey on the phone. In addition, the QRT report does not include the streaming statistics for a phone that has an IP Addressing Mode of IPv6 Only.

RSVP

If you deploy RSVP as the call admission control mechanism in your network, do not deploy IPv6. The RSVP feature does not support IPv6. RSVP calls support IPv4. If RSVP is required for the call and any device in the call is configured for or uses an IPv6 address, Cisco Unified Communications Manager rejects the call, and the caller receives a busy tone.

SDL

SDL TCP connections support IPv6, but SDL links support IPv4. If you configure a hostname in the Server Configuration window in Cisco Unified Communications Manager Administration, SDL queries the DNS A record, which ensures that IPv4 is used. If you specify an IP address, an IPv4 address gets passed down to the SDL layer.

Security (TLS and SRTP)

For information on how TLS and SRTP work with IPv6, see the *Cisco Unified Communications Manager Security Guide*.

T.38 Fax

Whether a T.38 fax call uses IPv4 or IPv6 depends on the preference of Cisco Unified Communications Manager and the capabilities of the devices in the call. If one device in the call uses IPv6 and the other device can use IPv4 and IPv6, the call uses IPv6, regardless of the configuration for the signaling and media enterprise parameters in Cisco Unified Communications Manager Administration.

Cisco Unified Communications Manager supports the following types of T.38 fax calls:

- SIP-to-SIP call that uses IPv6
- SIP-to-SIP call that uses IPv4
- SIP-to-non-SIP call that uses IPv4

- SIP-to-non-SIP call where the SIP device uses IPv6 and the non-SIP device uses IPv4 with an MTP that can translate IP address versions

  During the middle of a T.38 fax call, Cisco Unified Communications Manager does not insert an MTP that converts the IP version types; the MTP must already exist in the call.

Transfer

The transfer components in Cisco Unified Communications Manager uses the IP Addressing Mode and the IP address of the device to determine how to handle the transfer. If the IP capabilities do not match when you transfer a call, Cisco Unified Communications Manager allocates an MTP that can translate IP version, so the transfer can occur.

Web Browser on the Phone

On the Cisco Unified IP Phone, the HTTP interface for the web browser supports IPv4 addresses, so the phone does not allow web access to servers that use an IPv6 address.

Video and Application Media Streams

Cisco Unified Communications Manager supports IPv6 video calls, presentation sharing, far-end camera control, and IX media streams when all the media streams of a call use the same address type. Mixed addressing mode, where different address types are used for different media streams, is not supported.

Cisco Unified Communications Manager negotiates the address type of the call based on address type of audio for all media streams and inserts an MTP to perform IPv4 to IPv6 translation if there is address mode mismatch for audio. However, when an endpoint does not advertise the same address type for all media streams, Cisco Unified Communications Manager rejects the media streams that have a different address type than audio, and MTP is not inserted to match the same addressing types for all media streams.

Cisco Unified Video Advantage does not support IPv6; video is disabled for any IPv6 or dual-stack phone or SCCP endpoint that is associated with Cisco Unified Video Advantage.

Install and Activate IPv6

After you install Cisco Unified Communications Manager, your network can support IPv6 if you perform the necessary configuration tasks. For information on configuration tasks that you must perform, see the Configure IPv6, on page 740.

IPv6 impacts the Cisco CallManager, CTIManager, and Certificate Authority Proxy Function services in Cisco Unified Serviceability. Depending on the configuration tasks that you perform in Cisco Unified Communications Manager Administration, you may need to restart these services after you configure IPv6.

IPv6 Configuration

This section provides information to configure IPv6.

Tip Before you configure IPv6, review the configuration summary task for this feature.

Related Topics

Configure IPv6, on page 740

Run IPv6 CLI Commands or Configure IPv6 in the Ethernet IPv6 Window

To enable IPv6 in the Cisco Unified Communications Operating System and to ensure that the Cisco Unified Communications Manager node gets an IPv6 address, you must perform one of the following tasks:

- Run the IPv6 CLI commands in the command line interface.
- Enable IPv6 and configure the IPv6 address in the Ethernet IPv6 window in the Cisco Unified Communications Operating System.

⚠

Caution Before you set the Enable IPv6 enterprise parameter to True in Cisco Unified Communications Manager Administration, perform the following procedure. If you set the enterprise parameter to True before you enable IPv6 in the Cisco Unified Communications Operating System, the Cisco CallManager service runs in IPv4, and phones that have IP Addressing Mode of IPv6 Only cannot register with Cisco Unified Communications Manager.

⚠

Caution Changes that you make to enterprise parameters using Cisco Unified Communications Manager Administration also change the enterprise parameter settings for IM and Presence Service clusters in your deployment.

The following table provides a description of the Ethernet IPv6 configuration settings and the equivalent CLI commands that support the graphical user interface (GUI) options.

Table 86: IPv6 CLI Commands and Ethernet IPv6 Configuration Settings

Configuration Setting in Ethernet IPv6 Window	Equivalent CLI Command	Description
Enable IPv6 check box	**set network ipv6 service enable**	These settings enable IPv6 in the Cisco Unified Communications Operating System. **Caution** For IPv6 to work, you must either check the Ethernet IPv6 check box or issue the equivalent CLI command. You must perform this task before you set the Enable IPv6 enterprise parameter to True.

Configuration Setting in Ethernet IPv6 Window	Equivalent CLI Command	Description
Router Advertisement radio button	Not applicable	If you want to use stateless address autoconfiguration to obtain a non-link-local IPv6 address for the Cisco Unified Communications Manager node, click the Router Advertisement radio button. Click this radio button if you do not plan to configure a static non-link-local IPv6 address for the Cisco Unified Communications Manager node or if you do not want DHCPv6 server to issue a non-link-local IPv6 address to the node. Ensure that the Cisco Unified Communications Manager node only obtains one non-link-local IPv6 address. If the node has more than one IPv6 address, Cisco Unified Communications Manager may not behave as expected. If the Cisco Unified Communications Manager node obtains an IPv6 address via stateless address autoconfiguration and you also have a static IPv6 address that is configured for the node, Cisco Unified Communications Manager ignores the IPv6 address that is obtained via stateless address autoconfiguration and uses the static address.

Configuration Setting in Ethernet IPv6 Window	Equivalent CLI Command	Description
DHCP radio button	**`set network ipv6 dhcp enable`**	If you want the DHCPv6 server to issue a non-link-local IPv6 address to the Cisco Unified Communications Manager node, click the DHCP radio button or issue the equivalent CLI command. Ensure that the Cisco Unified Communications Manager node only obtains one non-link-local IPv6 address. If the node has more than one IPv6 address, Cisco Unified Communications Manager may not behave as expected.
Manual Entry radio button, IPv6 Address, Subnet Mask	**`set network ipv6 static_address <addr> <mask>`**	These Ethernet IPv6 settings and equivalent CLI command allow you to configure a static IPv6 address for the Cisco Unified Communications Manager node. Configuring a static non-link-local IPv6 address assumes that you do not want the Cisco Unified Communications Manager node to get the IPv6 address from the DHCPv6 server or via stateless address autoconfiguration.
IPv6 Address	**`show network ipv6 settings`**	These settings allow you to view the IPv6 address for the Cisco Unified Communications Manager node.

Tip If you chose to use the CLI commands instead of configuring the Ethernet IPv6 settings in the Cisco Unified Communications Operating System, you must reboot the node for the changes to take effect. For information on how to run CLI commands and for other IPv6 CLI commands, see the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

Note After you enable IPv6 through the CLI, you must enter the **IPv6 Name** field from **Server** > **Server Configuration**.

Procedure

Step 1 In Cisco Unified Communications Operating System, choose **Settings** > **IP** > **Ethernet IPv6**.

The **Ethernet IPv6 Configuration** window displays.

Step 2 Modify the Ethernet settings values in the appropriate fields in the **Ethernet IPv6 Configuration** window.

Step 3 Check the **Update with Reboot** check box. For the IPv6 settings in this window to take effect, you must reboot the node.

Step 4 Click **Save**. The node reboots immediately after you click Save.

Step 5 Perform this procedure for each node in the cluster.

Configure Service and Enterprise Parameters for IPv6

The following table describes the enterprise and service parameters that you can configure for IPv6. To configure enterprise parameters in Cisco Unified Communications Manager Administration, choose **System** > **Enterprise Parameters**. To configure service parameters in Cisco Unified Communications Manager Administration, choose **System** > **Service Parameters**.

Tip For a step-by-step procedure on how to configure enterprise parameters, see the *Cisco Unified Communications Manager Administration Guide*. For a step-by-step procedure on how to configure service parameters, see the *Cisco Unified Communications Manager Administration Guide*.

Table 87: Enterprise and Service Parameters for IPv6

Parameter	Description
Enable IPv6	This enterprise parameter specifies whether Cisco Unified Communications Manager can negotiate calls by using IPv6 and whether the phone can advertise an IPv6 address. Before you set this parameter to True, make sure that you enabled IPv6 in the Cisco Unified Communications Operating System on all servers in the cluster. Setting this parameter to True causes the Cisco CallManager service to run in dual-stack mode, which is required for interacting with devices that support IPv6. The default value equals False, which means that Cisco Unified Communications Manager cannot negotiate calls by using IPv6 and phones cannot advertise an IPv6 address. After you update this enterprise parameter, restart the Cisco CallManager, Cisco IP Voice Media Streaming App, Cisco CTIManager, Cisco Certificate Authority Proxy Function, and the Cisco IPVMS services in Cisco Unified Serviceability. **Caution** Changes that you make to enterprise parameters using Cisco Unified Communications Manager Administration also change the enterprise parameter settings for IM and Presence Service clusters in your deployment.
IP Addressing Mode Preference for Media	This enterprise parameter, which applies only to dual-stack devices, specifies the preferred addressing mode that Cisco Unified Communications Manager uses for media events when both IPv4 and IPv6 addresses are available from each device on the call. The default value equals Prefer IPv4.
IP Addressing Mode Preference for Signaling	This enterprise parameter, which applies only to dual-stack devices, specifies how the dual-stack phone connects to Cisco Unified Communications Manager for signaling events and how the dual-stack SIP trunk connects to the peer device for signaling events. The default value equals Prefer IPv4.

Parameter	Description
Allow Auto-Configuration for Phones	This parameter determines whether the phone is allowed to obtain an address through stateless autoconfiguration. Valid values specify On (the phone obtains its address as specified by the router advertisements, which may be stateless or stateful, depending on the router configuration) or Off (the phone always uses DHCPv6 to obtain its IPv6 address).
Call Counting CAC Enabled	This service parameter, which supports the Cisco CallManager service, determines whether Cisco Unified Communications Manager uses call counting as part of the locations-based call admission control (CAC) feature. Call counting uses a fixed bandwidth value to reserve and adjust bandwidth per call, regardless of the codec or media payload or the Internet Protocol Version (IPv6 or IPv4) that is used for each call. Call counting may potentially oversubscribe or undersubscribe bandwidth because a fixed-value bandwidth gets reserved per call no matter what the actual bandwidth is for the call. Cisco recommends that you leave this parameter set to the default value of False (disabled) unless your network requires the call counting feature. To enable call counting for CAC, choose True for the parameter; to disable call counting for CAC, choose False. This service parameter applies to IPv4 and IPv6 calls.
Audio Bandwidth For Call Counting CAC	This service parameter, which supports the Cisco CallManager service, specifies the amount of bandwidth to deduct from the available bandwidth for audio calls after you set the Call Counting CAC Enabled parameter to True. For each audio call, the amount of bandwidth that you enter in this field gets deducted, regardless whether more or less bandwidth is actually used for the call. This service parameter applies to IPv4 and IPv6 calls.

Parameter	Description
Video Bandwidth For Call Counting CAC	This service parameter, which supports the Cisco CallManager service, specifies the units of bandwidth to deduct from the available bandwidth for video calls after you set the Call Counting CAC Enabled parameter to True. For each video call, the available bandwidth gets reduced by the number of units that are required to account for the actual bandwidth usage. For example, if you specify 512 kbps as the bandwidth unit in this parameter, and a video call utilizes 384 kbps, then one unit, 512 kbps, gets deducted from available bandwidth. If you specify 512 kbps in this parameter and a video call negotiated 768 kbps, then two units of bandwidth (1064 kbps) get deducted from the available bandwidth. This service parameter applies to IPv4 and IPv6 calls.
Alternate Cisco File Server(s)	These service parameters, which support the Cisco TFTP service, allow you to configure alternate Cisco file servers, which are TFTP servers that are on a different cluster. These parameters, which support either IPv4 or IPv6 addresses or host names that resolve to an IP address, determine the IP stack that the TFTP uses to communicate between primary and alternate file servers. If an alternate file server supports dual-stack mode and you want to set both IPv4 and IPv6 addresses for the same server in these parameter fields, you must add both IP addresses, one per field, and the TFTP server tries each address in the order that you configure.

Access IPv6 and IPv4 Configuration in Unified CM Administration

The following table describes the IPv6 and IPv4 settings that are in Cisco Unified Communications Manager Administration, except for IPv6 service and enterprise parameters, which are described in Configure Service and Enterprise Parameters for IPv6, on page 765. For some IPv6 settings in the following table, equivalent settings for IPv4 display in Cisco Unified Communications Manager Administration; for example, in the SIP Trunk Configuration window, you can configure the Destination Address IPv6 setting or the Destination Address setting, or both settings, depending on the IP support in your network.

Configuration Setting	Description
System > **Server**	

Configuration Setting	Description
Host Name/IP Address	This field supports IPv4. If your network uses DNS that can map to IPv4 addresses, you can enter the host name of the Cisco Unified Communications Manager node. Otherwise, you must enter the full IPv4 address of the node. **Tip** If your network supports IPv6 (or IPv4 and IPv6), configure the IPv6 Name field in addition to the Host Name/IP Address field.
IPv6 Name	This field supports IPv6. If your network uses DNS that can map to IPv6 addresses, you can enter the host name of the Cisco Unified Communications Manager node. Otherwise, enter the non-link-local IP address of the Cisco Unified Communications Manager node. Phones that run SCCP or SIP use this field, which gets included in the TFTP configuration file, to retrieve the IPv6 address of the Cisco Unified Communications Manager node, so phone registration occurs. **Tip** You can provision your DNS server for IPv6 prior to upgrading to the current release. However, do not configure the DNS records for Cisco Unified Communications Manager for IPv6 until after you complete the upgrade. Configuring the DNS records for Cisco Unified Communications Manager for IPv6 prior to completing the upgrade causes the upgrade to fail and causes your system to become nonfunctional after you reboot. **Tip** In addition to configuring the IPv6 Name field, you must configure the Host Name/IP Address field, so Cisco Unified Communications Manager can support features/devices that use IPv4 (or IPv4 and IPv6).
Call Routing > **SIP Route Patterns**	

Configuration Setting	Description
IPv4 Pattern	Enter the domain, sub-domain, IPv4 address or IP subnetwork address. **Tip** For the IP subnetwork address, in Classless Inter-Domain Routing (CIDR) notation, enter X.X.X.X/Y, where Y equals the network prefix that denotes the number of bits in the address that will be the network address. **Tip** If the SIP trunk supports IPv6 or both IPv4 and IPv6 (dual-stack mode), configure the IPv6 Pattern in addition to the IPv4 pattern.
IPv6 Pattern	Cisco Unified Communications Manager uses SIP route patterns to route or block both internal and external calls. The IPv6 address in this field provides the basis for routing internal and external calls to SIP trunks that support IPv6. **Tip** If the SIP trunk supports both IPv4 and IPv6, configure the IPv4 Pattern in addition to the IPv6 Pattern.
Device > **Device Settings** > **Common Device Configuration**	

Configuration Setting	Description
IP Addressing Mode	Choose the version of IP address that the device (SIP trunks, or phones that run SIP or SCCP) uses to connect to Cisco Unified Communications Manager. From the drop-down list box, choose one of the following options: • IPv4 Only - For both media and signaling events, the device uses an IPv4 address to connect to Cisco Unified Communications Manager. If an IPv4 address is not available for the device, the call fails. If you choose this option, the phone releases an IPv6 address. If you choose this option, the SIP trunk uses an IPv4 address to connect to the peer device. • IPv6 Only - For both media and signaling events, the device uses an IPv6 address to connect to Cisco Unified Communications Manager. If an IPv6 address is not available for the device, the call fails. If you choose this option, the phone releases an IPv4 address. If you choose this option, the SIP trunk uses an IPv6 address to connect to the peer device. • IPv4 and IPv6 (Default) - Choose this option for dual-stack devices, which can have both an IPv4 and IPv6 address. For both media and signaling events, the dual-stack device uses either an IPv4 or an IPv6 address to connect to Cisco Unified Communications Manager. If the device has both IPv4 or IPv6 addressing available, it uses the settings configured for the following parameters: • **IP Addressing Mode Preference for Signaling** parameter for signaling events • **IP Addressing Mode Preference for Media** enterprise parameter for media events

Configuration Setting	Description
IP Addressing Mode Preference for Signaling	For dual-stack phones, which support both IPv4 and IPv6 addresses, choose the version of IP address that the phone prefers to establish a connection to Cisco Unified Communications Manager during a signaling event. For dual-stack SIP trunks, choose the version of IP address that the SIP trunk uses to connect to the peer device for signaling events. From the drop-down list box, choose one of the following options: • IPv4 - The dual-stack device prefers to establish a connection via an IPv4 address during a signaling event. • IPv6 - The dual-stack device prefers to establish a connection via an IPv6 address during a signaling event. • Use System Default - The configuration for the enterprise parameter, IP Addressing Mode Preference for Signaling, applies.

Configuration Setting	Description
Allow Auto-Configuration for Phones	This drop-down list box supports IPv6 for dual-stack Cisco Unified IP Phones that run SCCP or SIP. From the drop-down list box, choose one of the following options: • On - Depending on how the M bit is set via stateless address autoconfiguration on the router, the phone is allowed to use the IPv6 Network ID that is advertised in the Router Advertisements (RAs) to autoconfigure its IPv6 address. Phones also require a TFTP server address to register with Cisco Unified Communications Manager. You can manually configure the TFTP server address via the interface on the phone, or you can obtain it from a DHCPv6 server. **Tip** To indicate to the phone that it needs to use the DHCPv6 server to obtain other information, ensure that the O bit is set via stateless address autoconfiguration on the router. • Off - The phone obtains its IPv6 address and TFTP server address from the DHCPv6 server. • Default - To use the configuration for the Allow Auto-Configuration for Phones enterprise parameter, choose this option. Although Cisco Unified Communications Manager does not use this configuration, the TFTP file that the phone obtains includes this information.
Device > **SIP Trunk**	

Configuration Setting	Description
Destination Address	The Destination Address, which supports IPv4, represents the remote SIP peer with which this trunk will communicate. The allowed values for this field specify a valid V4 dotted IP address, fully qualified domain name (FQDN), or DNS SRV record only if the Destination Address is an SRV field is checked. SIP trunks only accept incoming requests from the configured Destination Address and the specified incoming port that is specified in the SIP Trunk Security Profile that is associated with this trunk. If the remote end is a Cisco Unified Communications Manager cluster, DNS SRV represents the recommended choice for this field. The DNS SRV record should include all Cisco Unified Communications Managers within the cluster. **Tip** For SIP trunks that can support IPv6 or IPv6 and IPv4 (dual-stack mode), configure the Destination Address IPv6 field in addition to the Destination Address field.
Destination Address IPv6	The Destination IPv6 Address represents the remote SIP peer with which this trunk will communicate. Enter one for the following values in the field: • A valid IPv6 address (global unicast, unique local, or a host name) • A fully qualified domain name (FQDN) • A DNS SRV record, but only if you check the Destination Address is an SRV check box. SIP trunks only accept incoming requests from the configured Destination IPv6 Address and the specified incoming port that is specified in the SIP Trunk Security Profile that is associated with this trunk. If the remote end is a Cisco Unified Communications Manager cluster, consider entering the DNS SRV record in this field. The DNS SRV record should include all Cisco Unified Communications Managers within the cluster. **Tip** For SIP trunks that run in dual-stack mode or that support an IP Addressing Mode of IPv6 Only, configure this field. If the SIP trunk runs in dual-stack mode, you must also configure the Destination Address field.
Device > **Device Settings** > **SIP Profile**	

Configuration Setting	Description
Enable ANAT	This option allows a dual-stack SIP trunk to offer both IPv4 and IPv6 media. When you check both the Enable ANAT and the Media Termination Point Required check boxes, Cisco Unified Communications Manager inserts a dual-stack MTP and sends out an offer with two m-lines, one for IPv4 and another for IPv6. If a dual- stack MTP cannot be allocated, Cisco Unified Communications Manager sends an INVITE without SDP. When you check the Enable ANAT check box and the Media Termination Point Required check box is unchecked, Cisco Unified Communications Manager sends an INVITE without SDP. When both the Enable ANAT and Media Termination Point Required check boxes display as unchecked (or when an MTP cannot be allocated), Cisco Unified Communications Manager sends an INVITE without SDP. When you uncheck the Enable ANAT check box but you check the Media Termination Point Required check box, consider the information, which assumes that an MTP can be allocated: • Cisco Unified Communications Manager sends an IPv4 address in the SDP for SIP trunks with an IP Addressing Mode of IPv4 Only. • Cisco Unified Communications Manager sends an IPv6 address in the SDP for SIP trunks with an IP Addressing Mode of IPv6 Only. • For dual-stack SIP trunks, Cisco Unified Communications Manager determines which IP address type to send in the SDP based on the configuration for the IP Addressing Mode Preference for Media enterprise parameter.

Related Topics

Run IPv6 CLI Commands or Configure IPv6 in the Ethernet IPv6 Window, on page 762

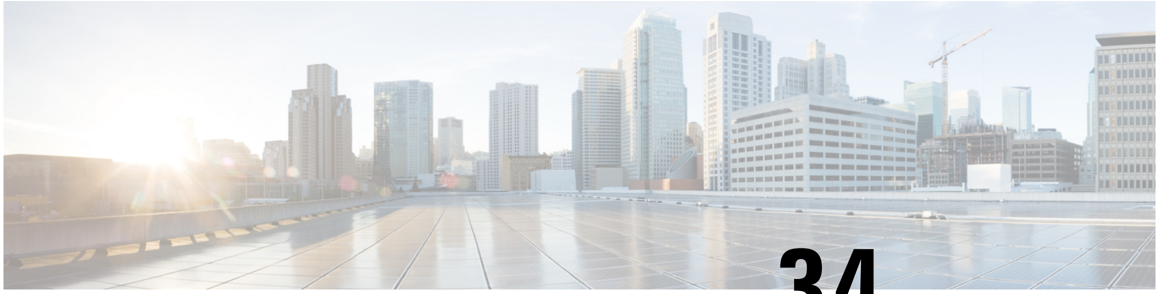
Provide Information to Users

No special considerations exist for phone (end) users, although IPv6 menu options display on the phone. Be aware, though, that if you do not configure the IP address support correctly in your network, users may receive a busy tone, dead air, and so on, when trying to place or answer calls on the phone.

Tip For additional information on using IPv6 with your phone, see the Cisco Unified IP Phone Administration Guide that supports your phone model and this version of Cisco Unified Communications Manager.

Troubleshooting IPv6

For information on troubleshooting IPv6, see the *Cisco Unified Communications Manager Troubleshooting Guide*.



CHAPTER 34

Licensing

Cisco Unified Communications Manager Licensing is managed by the Enterprise License Manager. Licenses are installed on Enterprise License Manager, which collects license usage information from the Unified Communications Manager and reports back license compliance or non-compliance. The Unified Communications Manager calculates license usage based upon the total number of users and devices on the system.

Unified Communications Manager Licensing

All licensing for Unified Communications Manager is centralized and held on the Cisco Prime License Manager. Unified Communications Manager communicates with the Cisco Prime License Manager to express its licensing requirements. When users, phones, or other services are provisioned in the Unified Communications Manager, license requirements are added and the Unified Communications Manager sends the corresponding license requirements to the Cisco Prime License Manager. The Cisco Prime License Manager then compares the Unified Communications Manager license requirements with the available licenses installed and reports back license compliance or non-compliance. Unified Communications Manager licensing types are available as Cisco Unified Workspace Licensing (UWL) or Cisco User Connect Licensing (UCL).

UWL allows organizations to access a wide range of Cisco Collaboration applications and services in a cost-effective, simple package. It includes soft clients, application server software and licensing on a per user basis. Depending on your needs and device of choice, Cisco Unified Workspace Licensing is available in Professional Edition and Standard Edition.

UCL is a user-based license for individual Cisco Unified Communications products. It includes a soft client, application server software licensing, and basic unified communications applications. Depending on your needs and device of choice, UCL is available in Essential, Basic, Enhanced, or Enhanced Plus.

The following are the license types for the Unified Communications Manager:

Essential	Essential User Connect License - supports one device providing basic voice or analog device (phone or fax). (For example: analog phone, ATA 186, ATA 187, Cisco 3905, Cisco 6901)

Basic	Basic User Connect License - supports one device, including all Essential devices, plus basic (voice and video) call control features. (For example: Cisco 6911, Cisco 6921)
Enhanced	Enhanced User Connect License - supports one device, including all Basic devices, plus advanced (voice and video) call control features including desktop, mobile clients. (For example: Cisco 3911, Cisco 3951, Cisco 6941, Cisco 6945, Cisco 6961, Cisco 79xx, Cisco 89xx, Cisco 99xx, Cisco E20, Cisco TelePresence EX60, Cisco TelePresence EX90, third party SIP)
Enhanced Plus	Enhanced Plus User Connect License - supports up to two devices, and including all Enhanced devices.
CUWL Standard	CUWL Standard Unified Workspace Licensing (UWL) license for Unified CM - supports advanced (voice and video) call control features including desktop and mobile with maximum of ten devices per user.
CUWL Professional	CUWL Professional Unified Workspace Licensing (UWL) license for Unified CM - includes CUWL Standard features and professional collaboration workspace application features with maximum of ten devices per user.
TelePresence Room	TelePresence Room license - supports room based immersive and multipurpose Cisco TelePresence System endpoints and Spark Room. (For example: Cisco TelePresence System Series 3200, 3000, 1300; Cisco TelePresence MX Series; Cisco TelePresence TX Series; Cisco TelePresence System Profile Series)

For more information, see the *Cisco Prime License Manager User Guide*.

License Usage Report

The License Usage Report provides the summary and detailed information on system license usage as it is reported to the Cisco Prime License Manager.

Usage details are available by license type, users, and unassigned devices. Usage information is updated once every six hours, and may be updated manually by clicking on Update Usage Details. Clicking Update Usage Details is a resource intensive process and may take a few minutes depending on the size of your system. There is a link provided to review the Unified Communications licensing information in **View all license type descriptions and device classifications**.

The **Status** message displays if there is an alarm or licensing alert (license non-compliance). See Alarms alerts and license status notification for further information on status messages. See License Compliance for further information on license compliance and non-compliance.

The **License Requirements by Type** table shows the current system license requirements. It shows current license usage (number of licenses required) by license type and summarizes the number of users and unassigned devices that are requiring licenses by license type. The Report links by license type are provided by (number of) Users or (number of) Unassigned devices and allow drill-down links. For the User report, the **user id** link provides details on user configuration per the user id. The *view details* link provides license requirements per user id. For the Unassigned Devices report, the Device Type and License Type that is required is displayed for each unassigned device.

License Usage Reports are also available summarized by **Users and Unassigned devices**. The Users row lists the total number of users configured on the system. View Usage Report for the users provides a report for all users configured on the system and their corresponding license requirements. View Usage Report for the Unassigned Devices shows the total number of unassigned devices (devices with no associated user).

Note Assigning a user ID to a device using Cisco Unified Communications Administration moves the device from “Unassigned Devices” to “Users” in the License Usage Report. However, adding a device to the list of controlled devices for an end user does not modify the “License Usage Report” results for the device.

The **Cisco Prime License Manager** section shows if the Unified Communications Manager is managed by an Cisco Prime License Manager. If it has been added to an Cisco Prime License Manager product inventory, it provides a link to the Cisco Prime License Manager server login page. The Unified Communications Manager must connect with the Cisco Prime License Manager at lease once every 24 hours. This connection and communications of license requirements from the Unified Communications Manager and Cisco Prime License Manager is called synchronization. The Cisco Prime License Manager status shows the Time and date stamp of the last successful synchronization between the Unified Communications Manager and Cisco Prime License Manager.

License Compliance

When first installed, the Unified Communications Manager is fully operational in demonstration mode for a grace period of 60 days, until it has successfully synchronized with the Cisco Prime License Manager and licenses are installed on Cisco Prime License Manager. After the Cisco Prime License Manager is registered, licenses are installed, and synchronization with the Unified Communications Manager takes place, the Cisco Prime License Manager communicates with the Unified Communications Manager product instance on a daily basis. The Unified Communications Manager reports the total license requirements by license type to the Cisco Prime License Manager. The Cisco Prime License Manager totals the license requirements for all connected product instances and compares the total license requirements to the total available installed licenses (the license requirements and installed license types are totaled for all product instances of the same product type.) The Cisco Prime License Manager then reports the status back to the product instance as:

- In compliance, or;
- Non-compliance

Non-compliance occurs in the following situations:

- There are an insufficient number of licenses, or;
- There has not been a successful synchronization with the Cisco Prime License Manager

Licenses in the non-compliant state for Unified Communications Manager are enforced after a 60-day grace period. At the conclusion of the grace period, Unified Communications Manager enforces non-compliance with the following service degradation:

- Devices and Users cannot be provisioned. Changing the configuration of a user that affects licensing (For example: the Enable IM and Presence and the Enable Mobility check boxes) is not allowed.
- Devices and Users cannot be de-provisioned. Any configuration changes that involve licensing (For example: disabling IM and Presence or Mobility) is allowed.

For information about licensing operations, see the *Cisco Prime License Manager User Guide*.

Licensing Troubleshooting

Unified Communications Manager licensing is managed by Cisco Prime License Manager, which handles licensing fulfillment, supports allocation and reconciliation of licenses across supported products. Cosc Prime Manager also provides enterprise-level reporting of usage and entitlement, which includes status messages. Alarms are generated by Unified Communications Manager.

Unified Communications Manager generates the following alarms for licensing.

Table 88: Alarms

Alarm	Description	Recommended Action
CiscoElmNotConnected	Cisco Prime License Manager Not Connected (WARNING ALARM)	Connect Cisco Prime License Manager to the product
CiscoNoProvisionTimeout	The grace period for licensing has expired (WARNING ALARM)	Upload additional licenses. Verify that Cisco Prime License Manager is connected to the product.
CiscoSystemTimeChange	System time has changed (INFORMATIONAL_ALARM)	Determine why the system time changed.
CiscoGraceTimeLeft	Grace period countdown towards no provisioning allowed (INFORMATIONAL_ALARM)	Upload additional licenses. Verify that Cisco Prime License Manager is connected to the product.
CiscoSystemInOverage	System is in overage which means licensed resource limit has been exceeded on the system (WARNING_ALARM)	Upload additional licenses. Verify that Cisco Prime License Manager is connected to the product.
CiscoSystemSecurityMismatch	Certificate Mismatch between Cisco Unified Communications Manager and Cisco Prime License Manager (ERROR_ALARM)	Verify the Cisco Prime License Manager certificates. This could be a "man-in-the-middle" attack.

The following is a list of all status messages as they appear on the License Usage report window.

Table 89: Status Messages

Device	State	Alarm Message	Description
Unified Communications Manager	Demo mode	The system is operating on demo licenses that will expire in 60 days. Add this system to a Cisco Prime License Manager and install sufficient licenses to cover its usage before expiration in order to avoid losing the ability to provision users and devices.	New installation – starter license

Device	State	Alarm Message	Description
Unified Communications Manager	License overage	The system is operating with an insufficient number of licenses. Configure additional licenses in your Cisco Prime License Manager in order to restore the ability to provision users and devices.	License resource limits have been exceeded and the system is operating with insufficient licenses.
Unified Communications Manager	Cisco Prime License Manager not connected	The system has not synchronized successfully with Cisco Prime License Manager for 10 days. If successful synchronization does not occur within the next 50 days, you will no longer be able to provision users and devices.	Unified Communications Manager to Enterprise License Manager connectivity has been lost or a successful synchronization has not occurred.

For further license troubleshooting information, see the *Cisco Prime License Manager User Guide*.

CHAPTER 35

Local Route Groups

This chapter provides information about local route groups.

Configure Local Route Groups

The Local Route Group feature helps reduce the complexity and maintenance efforts of provisioning in a centralized Cisco Unified Communications Manager deployment that uses a large number of locations. The fundamental breakthrough in the Local Route Group feature comprises decoupling the location of a PSTN gateway from the route patterns that are used to access the gateway.

The Local Route Group feature provides the ability to reduce the number of route lists and route patterns that need to be provisioned for implementations of Cisco Unified Communications Manager where each of N sites needs to have access to the local gateways of the other N-1 remote sites. One such scenario occurs with Tail End Hop Off (TEHO).

Perform the following steps to configure the Local Route Group feature.

Procedure

Step 1 Review the interactions and restrictions for this feature.

Step 2 If you have not already done so, activate the Cisco CallManager service in Cisco Unified Serviceability.

Step 3 Use the **Call Routing** > **Route/Hunt** > **Route List** menu option in Cisco Unified Communications Manager Administration to configure a local route list that contains the Standard Local Route Group as a member of the route list.

Step 4 Use the **System** > **Device Pool** menu option in Cisco Unified Communications Manager Administration to configure the Local Route Group setting for the device pools in the Cisco Unified Communications Manager implementation. For each device pool that you configure, specify a route group to use as local route group for that device pool. For each device pool, users may also configure the Called Party Transformation CSS for the devices in that device pool.

Step 5 If the dial plan is not globalized and the Local Route Group needs to use transformation patterns for called party, use the **Device** > **Gateway and Device** > **Trunk** menu options in Cisco Unified Communications Manager Administration to configure the gateways and trunks in each location.

For each device that you want to configure for the Local Route Group feature, configure the following fields:

- Called Party Transformation CSS - Choose a CSS to allow localization of the called party number on the device.
- Use Device Pool Called Party Transformation CSS - Check this check box to use the Called Party Transformation CSS that is specified by the device pool to which this device belongs. If the check box is left unchecked, the Called Party Transformation CSS specified for the device gets used.

Step 6 Use the **Call Routing** > **Transformation Pattern** > **Called Party Transformation Pattern** menu item in Cisco Unified Communications Manager Administration to configure the called party transformation pattern for the digits before a call is routed out through a gateway.

Step 7 Use the **Call Routing** > **Route/Hunt** > **Route Pattern** menu item in Cisco Unified Communications Manager Administration to configure the route patterns to use route lists that are configured to use the Standard Local Route Group.

Step 8 Use the **Call Routing** > **Route Plan Report** menu option in Cisco Unified Communications Manager Administration to generate and view the route plan report for your implementation. Check the route plan report to verify that the provisioning that you performed is correct for your Local Route Group configuration.

Related Topics

Local Route Groups, on page 783

Local Route Groups Feature, on page 784

Interactions, on page 790

Restrictions, on page 792

Local Route Groups Feature

The Local Route Group feature helps reduce the complexity and maintenance efforts of provisioning in a centralized Cisco Unified Communications Manager deployment that uses a large number of locations. The fundamental breakthrough in the Local Route Group feature comprises decoupling the location of a PSTN gateway from the route patterns that are used to access the gateway.

Cisco Unified Communications Manager uses a special Local Route Group that can be bound to a provisioned route group differently based on the Local Route Group device pool setting of the originating device. Devices, such as phones, from different locales can therefore use identical route lists and route patterns, but Cisco Unified Communications Manager selects the correct gateway(s) for their local end.

Note This document uses the term provisioned route group to specify a route group that an administrator configures through use of the **Call Routing** > **Route/Hunt** > **Route Group** menu option in Cisco Unified Communications Manager Administration.

The Local Route Group feature provides the ability to reduce the number of route lists and route patterns that need to be provisioned for implementations of Cisco Unified Communications Manager where each of N sites needs to have access to the local gateways of the other N-1 remote sites. One such scenario occurs with Tail End Hop Off (TEHO).

In simple local routing cases, the provisioning gets reduced from N route patterns and N route lists to one route pattern and one route list. In cases with Tail End Hop Off (TEHO), local route groups allow configuration of N route patterns and N route lists instead of N2 route patterns and N2 route lists. Because values for N are now reaching much more than 1000 for larger implementations, enormous scalability savings result.

Previously, Cisco Unified Communications Manager treated gateways as devices to which multiple patterns are assigned. A tight, somewhat inflexible, binding existed between a gateway and the patterns that Cisco Unified Communications Manager associated with the gateway. When a call was placed, Cisco Unified Communications Manager viewed the situation as “Caller X has dialed some digits. These digits match pattern Y. Pattern Y directly associates with route lists, route groups, and gateways A, B, and C.”

Local Route Group

When the administrator adds a new route group to a route list, the Route List Configuration window presents the administrator with all available route groups from which to select. This list includes as its first member the special route group that is named Standard Local Route Group. This local route group specifies a virtual local route group.

The local route group does not statically get bound to any provisioned route group. The local route group does not display in the Find and List Route Groups configuration window; and, therefore, cannot be deleted or modified. You can, however, add the local route group to any route list; when so added, the local route group serves as a placeholder for a provisioned route group that will later get bound to the local route group dynamically during call setup.

After you add the local route group to a route list, you can later remove it from that list, or you can modify its search-order places in the list as with any provisioned route group.

Bind a Provisioned Route Group to a Local Route Group

Deferring the binding of a provisioned route group to the local route group until call setup ensures that the desired provisioned route group can be the one that is local to the device that is placing the call. Thus, a device in location X would use a provisioned route group that contains gateways for the location X PSTN while a device in location Y would use a different provisioned group of gateways for the location Y PSTN.

You need to ensure that each device in the system is provisioned to know its local route group. To avoid specifying this information in the configuration window for each device, because the number of devices can be many thousands, Cisco Unified Communications Manager Administration locates the information in the device pool for the device, because device pools specify common site-specific information.

The Local Route Group field in the Device Pool Configuration window includes a drop-down list box that lists all available (provisioned) route groups. This list excludes the special Standard Local Route Group name (because only provisioned route groups should be configured for a device pool) but presents the special name, <NONE>, which specifies the first (default) choice. Choose <NONE> if no binding is desired.

Whenever the default value <NONE> is selected for a device pool, any call that uses a route list that includes the local route group, Standard Local Route Group, gets routed as if the Standard Local Route Group is absent from the list.

With this mechanism, a call that is placed from any device over a route list that contains the special Standard Local Route Group behaves as follows:

1. The route list algorithm searches through the list of included route groups, in the designated order, until an unused trunk can be found. (The previous and current implementations do not differ.)

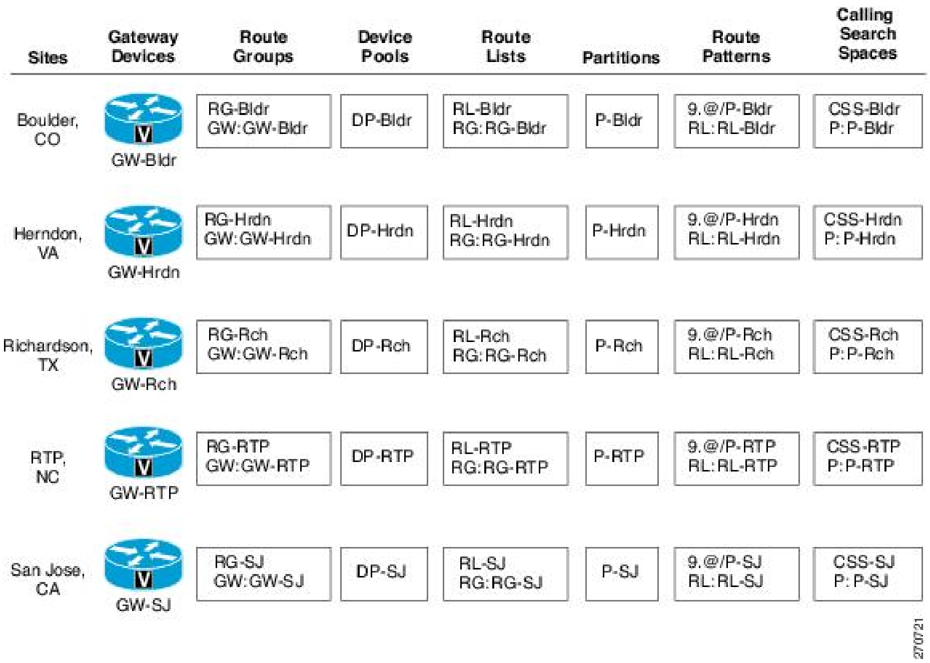
2. If the search encounters the special Standard Local Route Group, the system automatically replaces this route group with the name of the local route group that is provisioned for the calling device, unless the search encounters one of the following situations:
   - If the provisioned route group specifies <NONE>, the Standard Local Route Group route group gets skipped entirely.
   - If by skipping the Standard Local Route Group in this way, the search ends (that is, the Standard Local Route Group was the last or only route group in the route list), routing aborts, and the user receives reorder tone or an equivalent notification.

Simple Local Routing

Simple local routing comprises cases in which each site needs to route offnet calls to its local gateways. Provisioning of route patterns and route lists can get reduced from the need to configure N route patterns and N route lists to a configuration where only one route pattern and one route list are needed.

For this case further assume that all phones that home to a particular site belong to a single calling search space (CSS) that is unique to that site. For example, phones at the Boulder site belong to the CSS-Bldr calling search space and so forth. The following figure illustrates a possible provisioning of this system without using the Local Route Group feature, so regardless of site, a phone always prefers its local gateway when making an offnet call by dialing 9 followed by a seven-, ten-, or eleven-digit pattern. As more sites get added, each of the columns must include new entries (rows). If N sites exist, you need N different route lists, route patterns, partitions, and calling search spaces.

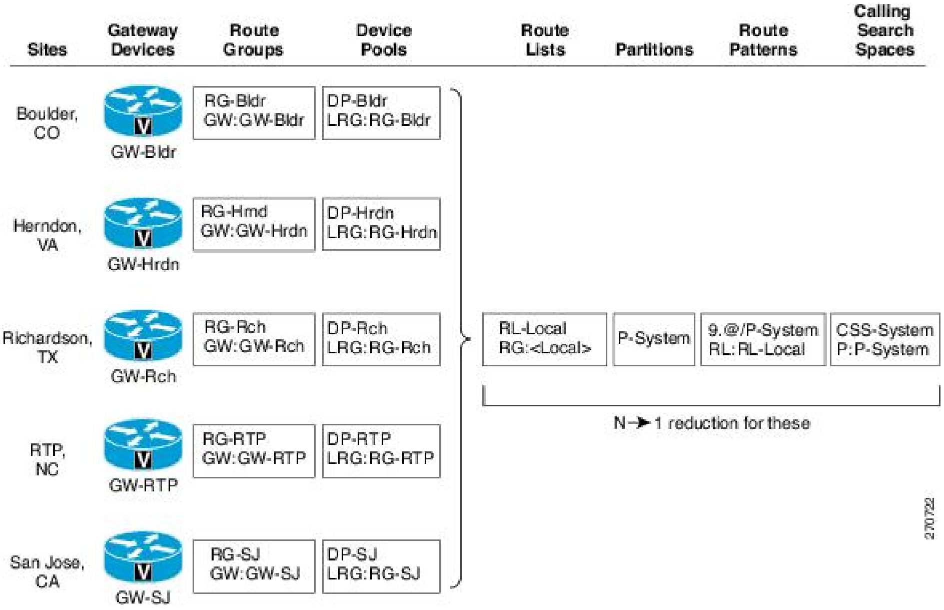
Figure 69: Provisioning Local Offnet Access Without Local Route Groups



Sites	Gateway Devices	Route Groups	Device Pools	Route Lists	Partitions	Route Patterns	Calling Search Spaces
Boulder, CO	GW-Bldr	RG-Bldr GW:GW-Bldr	DP-Bldr	RL-Bldr RG:RG-Bldr	P-Bldr	9.@/P-Bldr RL:RL-Bldr	CSS-Bldr P:P-Bldr
Herndon, VA	GW-Hrdn	RG-Hrdn GW:GW-Hrdn	DP-Hrdn	RL-Hrdn RG:RG-Hrdn	P-Hrdn	9.@/P-Hrdn RL:RL-Hrdn	CSS-Hrdn P: P-Hrdn
Richardson, TX	GW-Rch	RG-Rch GW:GW-Rch	DP-Rch	RL-Rch RG:RG-Rch	P-Rch	9.@/P-Rch RL:RL-Rch	CSS-Rch P:P-Rch
RTP, NC	GW-RTP	RG-RTP GW:GW-RTP	DP-RTP	RL-RTP RG:RG-RTP	P-RTP	9.@/P-RTP RL:RL-RTP	CSS-RTP P:P-RTP
San Jose, CA	GW-SJ	RG-SJ GW:GW-SJ	DP-SJ	RL-SJ RG:RG-SJ	P-SJ	9.@/P-SJ RL:RL-SJ	CSS-SJ P: P-SJ

In the same implementation, use of the Local Route Group feature allows configuration of a single route list, partition, route pattern, and CSS, regardless of the number of sites, as shown in the following figure.

Figure 70: Provisioning Local Offnet Access With Local Route Groups



In this case, the following configuration applies:

- All phones belong to a single CSS-System calling search space and to a single P-System partition.
- All phones for a given site belong to a single device pool unique to that site.
- The Local Route Group field in each device pool identifies the specific route group for that site. In this example, RG-Bldr for Boulder, RG-Rch for Richardson, and so on.

Thus, the route lists, route patterns, partitions and calling search spaces for this case each get reduced from N to 1. The number of gateways, route groups, and device pools remain N for N sites.

A new partition, P_System, and a new calling search space, CSS_System, get added for accessing the 9.@ pattern from all sites. The calling search space, CSS_Boulder, can contain both P_Boulder and P_System as well, as can the CSS of the other sites.

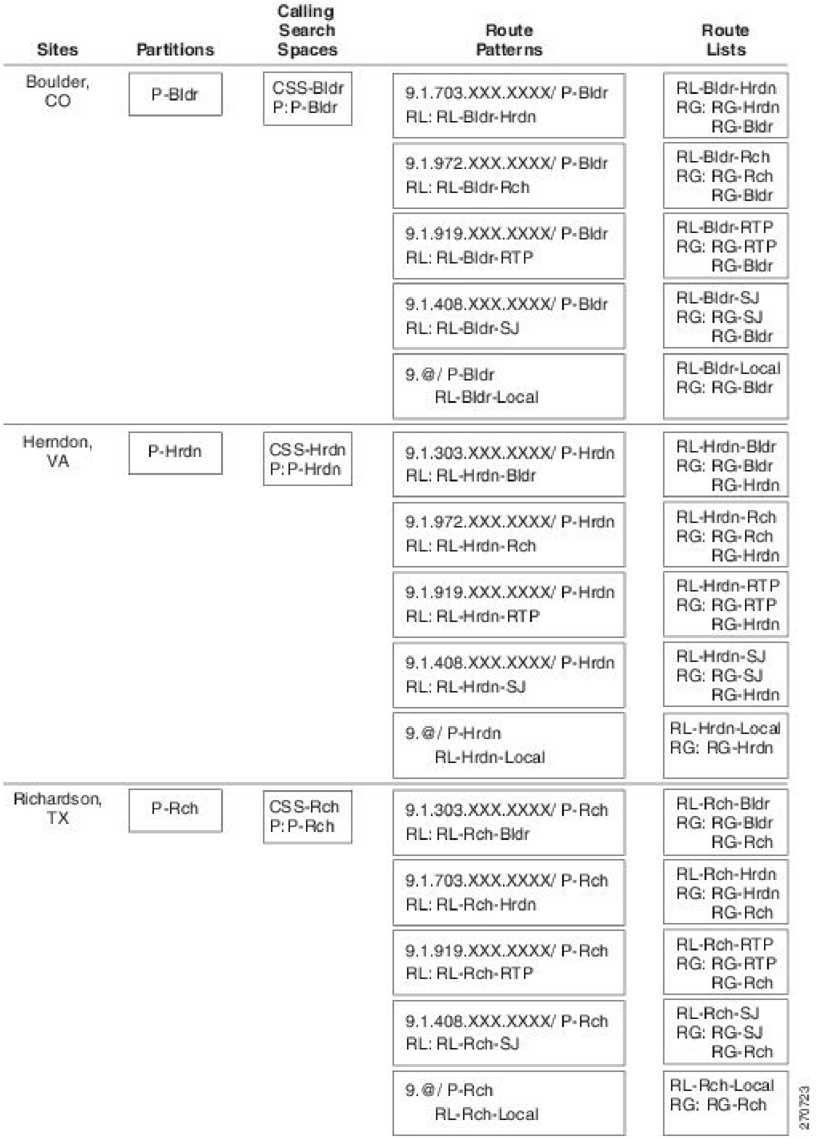
Tail End Hop Off

Tail End Hop Off (TEHO) refers to routing long-distance calls across the VoIP network and dropping them off to the Public Switched Telephone Network (PSTN), as a local call, at a remote gateway. In TEHO situations, you can reduce the configuration complexity from the need to configure N2 entities to needing only N entities. The following assumptions for TEHO apply:

- Each site has a different route pattern and route list for each of the other N-1 sites.
- For a given site, S, each of the N-1 route lists to another (remote) site has, as first preference, a route group of one or more gateways that are local to that other site followed by, as second preference, a route group that is local to S. Therefore, when sufficient trunking resources are available to honor the first preference, a long-distance call uses a gateway at the remote site to go offnet and thus bypass any tolls; otherwise, the call defaults to a local gateway and incurs toll charges.

Again, Cisco Unified Communications Manager has an identical routing policy for all sites. The second preference of routing a call through the local PSTN of a site (if the system fails to drop off the call as a local call at the remote PSTN) forces the customer to provision separate instances of all routing information for each site, as illustrated in the following figure. (The figure illustrates the configuration for some of the sites.) Each site has a unique set of route patterns and route lists to each of the other N-1 sites, as well as a generic local route list for all other calls that the remote access codes do not cover. This requirement entails a total of N×(N-1)+N, or N2, route lists and route patterns for the general case.

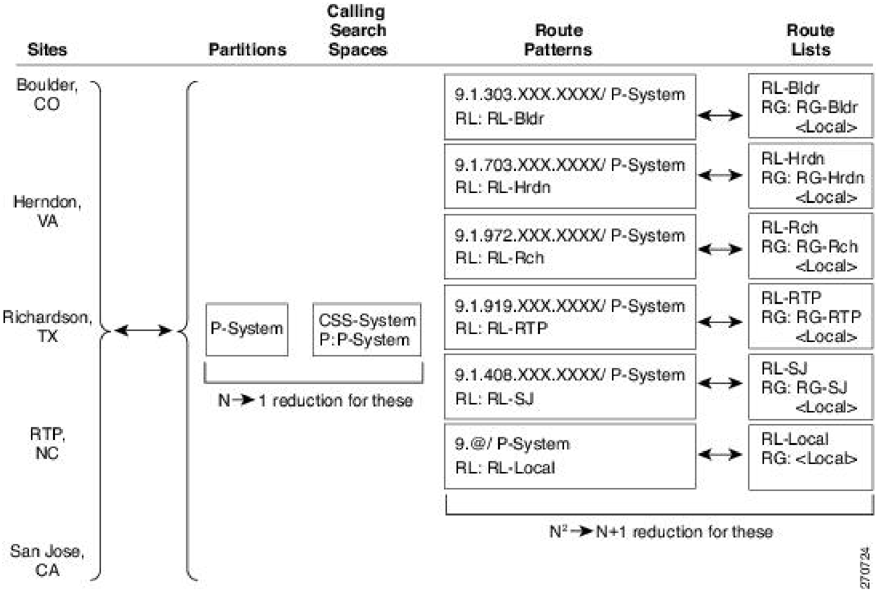
Figure 71: Provisioning TEHO Without Local Route Groups



Sites	Partitions	Calling Search Spaces	Route Patterns	Route Lists
Boulder, CO	P-Bldr	CSS-Bldr P: P-Bldr	9.1.703.XXX.XXXX/ P-Bldr RL: RL-Bldr-Hrdn	RL-Bldr-Hrdn RG: RG-Hrdn RG-Bldr
			9.1.972.XXX.XXXX/ P-Bldr RL: RL-Bldr-Rch	RL-Bldr-Rch RG: RG-Rch RG-Bldr
			9.1.919.XXX.XXXX/ P-Bldr RL: RL-Bldr-RTP	RL-Bldr-RTP RG: RG-RTP RG-Bldr
			9.1.408.XXX.XXXX/ P-Bldr RL: RL-Bldr-SJ	RL-Bldr-SJ RG: RG-SJ RG-Bldr
			9.@/ P-Bldr RL-Bldr-Local	RL-Bldr-Local RG: RG-Bldr
Herndon, VA	P-Hrdn	CSS-Hrdn P: P-Hrdn	9.1.303.XXX.XXXX/ P-Hrdn RL: RL-Hrdn-Bldr	RL-Hrdn-Bldr RG: RG-Bldr RG-Hrdn
			9.1.972.XXX.XXXX/ P-Hrdn RL: RL-Hrdn-Rch	RL-Hrdn-Rch RG: RG-Rch RG-Hrdn
			9.1.919.XXX.XXXX/ P-Hrdn RL: RL-Hrdn-RTP	RL-Hrdn-RTP RG: RG-RTP RG-Hrdn
			9.1.408.XXX.XXXX/ P-Hrdn RL: RL-Hrdn-SJ	RL-Hrdn-SJ RG: RG-SJ RG-Hrdn
			9.@/ P-Hrdn RL-Hrdn-Local	RL-Hrdn-Local RG: RG-Hrdn
Richardson, TX	P-Rch	CSS-Rch P: P-Rch	9.1.303.XXX.XXXX/ P-Rch RL: RL-Rch-Bldr	RL-Rch-Bldr RG: RG-Bldr RG-Rch
			9.1.703.XXX.XXXX/ P-Rch RL: RL-Rch-Hrdn	RL-Rch-Hrdn RG: RG-Hrdn RG-Rch
			9.1.919.XXX.XXXX/ P-Rch RL: RL-Rch-RTP	RL-Rch-RTP RG: RG-RTP RG-Rch
			9.1.408.XXX.XXXX/ P-Rch RL: RL-Rch-SJ	RL-Rch-SJ RG: RG-SJ RG-Rch
			9.@/ P-Rch RL-Rch-Local	RL-Rch-Local RG: RG-Rch

Using the Local Route Group feature, the N×(N-1) route patterns and route lists that are needed for remote sites reduce to N, and the N local route patterns and local route lists reduce to 1. Overall, the total number of route lists and route patterns decreases from N2 to N+1, and calling search spaces and partitions decrease from N to 1, as illustrated in the following figure.

Figure 72: Provisioning TEHO With Local Route Groups


Sites
Partitions
Calling Search Spaces
Route Patterns
Route Lists
Boulder, CO
Herndon, VA
Richardson, TX
RTP, NC
San Jose, CA
P-System
CSS-System P:P-System
N→1 reduction for these
9.1.303.XXX.XXXX/ P-System RL: RL-Bldr
9.1.703.XXX.XXXX/ P-System RL: RL-Hrdn
9.1.972.XXX.XXXX/ P-System RL: RL-Rch
9.1.919.XXX.XXXX/ P-System RL: RL-RTP
9.1.408.XXX.XXXX/ P-System RL: RL-SJ
9.@/ P-System RL: RL-Local
RL-Bldr RG: RG-Bldr <Local>
RL-Hrdn RG: RG-Hrdn <Local>
RL-Rch RG: RG-Rch <Local>
RL-RTP RG: RG-RTP <Local>
RL-SJ RG: RG-SJ <Local>
RL-Local RG: <Local>
N²→N+1 reduction for these
270724

In the previous figure, note the crucial element, which is the use of the Standard Local Route Group as the second choice in each route list. The setting in the device pool of the originating device dynamically determines the actual provisioned route group that gets used during a specific call.

Called Party Transformations

While loose coupling occurs between the enterprise number and the route group/gateway, very tight coupling occurs between the route group/gateway and the patterns that the PSTN expects. If the gateway chosen is in a 7-digit dialing location, the PSTN expects 7 digits; if the chosen gateway is in a 10-digit location, the PSTN expects 10 digits to access local numbers.

Example 1

A call gets placed from Dallas; the called number specifies 9.5551212. If the Dallas local gateway is busy or not accessible, assuming that the San Jose gateway is selected, 9.5551212 must be converted to 1 214 555 1212 for the San Jose gateway to dial out.

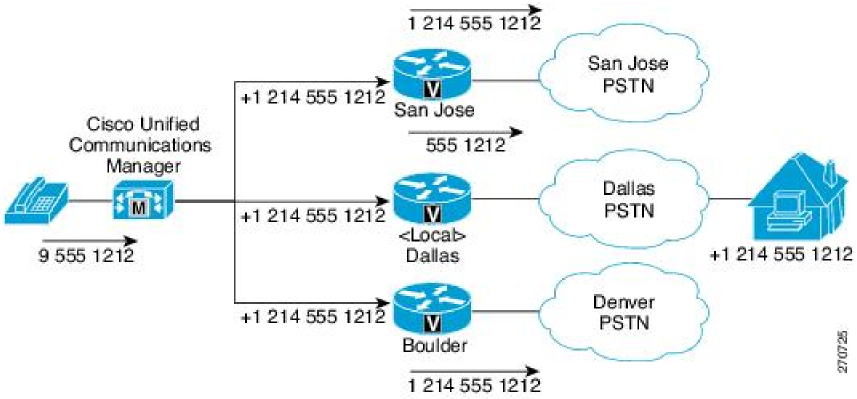
In the same example for a Local Route Group case, a call gets placed from Dallas. The called number specifies 9.5551212, so the system must perform the following actions:

1. Take the digits as dialed by the originator, discard PreDot, and insert the prefix +1 214.
2. Convert the call number to a globally unique E.164 string (+1 214 555 1212).

If a San Jose gateway gets selected, the system converts the global string +1 214 555 1212 to 1 214 555 1212; if a Dallas gateway gets selected, the system converts the global string to 214 555 1212.

See the following figure for an illustration of this example.

Figure 73: Called Digits Transformation



Example 2

A call gets placed from RTP; the called number specifies 5551212. If the RTP local gateway is busy or not accessible, assuming that the San Jose gateway is selected, 5551212 must get converted to 1 919 555 1212 for the San Jose gateway to dial out.

In the same example for a Local Route Group case, a call gets placed from RTP. The called number specifies 9.5551212, so the system must perform the following actions:

1. Take the digits as dialed, discard PreDot, and insert the Prefix 91919.
2. Convert the called number to a global dialing string (9 1 919 555 1212).

If a San Jose gateway gets selected, the system converts the global string 91 919 555 1212 to 1 919 555 1212; if the RTP gateway gets selected, the system converts the global string to 555 1212.

System Requirements for Local Route Groups

The following system requirement applies to the local route group feature:

- Cisco Unified Communications Manager 7.0(1) or later

Interactions and Restrictions

This section describes the interactions and restrictions for local route groups.

Interactions

This section describes how the local route group feature interacts with other Cisco Unified Communications Manager features and applications.

Device Support

All Cisco Unified Communications Manager device types that are capable of originating a call support support the Local Route Group feature, including the following devices:

- Skinny devices
- H.323 devices
- SIP devices
- MGCP devices, including all PRI variants, BRI, and MGCP phones
- CTI devices

Forwarding

For forwarded calls, Cisco Unified Communications Manager must use the Local Route Group that is provisioned in the device pool settings that are associated with the redirected party to find the provisioned local route group. Thus, if phone A calls (local) phone B and phone B forwards the call to (remote) phone C, the Local Route Group value from the phone A device pool gets used rather than the corresponding value for phone B.

Supplementary Services

Many supplementary services can originate calls. When this happens, the local route group gets skipped.

The following features can initiate calls:

- CallBack
- MWI
- Mobility (FollowMe)
- Path Replacement

If by skipping the Standard Local Route Group route group, the search ends (that is, the Standard Local Route Group represents the last or only route group in the route list), routing aborts.

The following features can redirect calls:

- Barge
- CallBack
- Call Park
- Conference
- Directed Call Park
- Forwarding
- Immediate Divert
- MeetMe Conference
- Call Pickup

As explained in the Forwarding, on page 791, Cisco Unified Communications Manager uses the Local Route Group that is provisioned in the device pool settings that are associated with the redirected party to find the provisioned local route group.

Route Plan Report

The Route Plan Report displays the route details, such as route list, associated route groups, and trunks/gateways, including the special Standard Local Route Group route group. An example follows.

Example of Route Plan Report Display for Route Patterns with No Local Route Group

BoulderRouteList

|__ BoulderRG

__BoulderGW1

|__BoulderGW2

Example of Route Plan Report Display with Local Route Group

SystemRouteList

|__Standard Local Route Group

Cisco Unified Mobility

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.

Restrictions

Review this section for applicable restrictions before you configure local route groups.

Mixed Route Lists

You cannot insert SIP route groups and Q.SIG route groups into a route list at the same time. With the Local Route Group feature, this mixed route list rule cannot get enforced during provisioning because the binding between the Standard Local Route Group and a provisioned route group occurs dynamically during the call setup. Therefore, some Q.SIG related features may not be available. The binding from Standard Local Route Group to a Q.SIG route group should be avoided.

Install and Activate Local Route Groups

After you install Cisco Unified Communications Manager, Release 7.0(1) or later, you can configure local route groups.

Configure Local Route Groups

This section contains information about local route group configuration.

Tip Before you configure local route groups, review the configuration summary task for this feature.

Related Topics

Configure Local Route Groups, on page 783

Set the Local Route Group Service Parameters

The Local Route Group feature does not require the configuration of any additional service parameters.

CHAPTER 36

Logical Partitioning

This chapter provides information about the Logical Partitioning feature which specifies the capability of a telephony system to control calls and features on the basis of specific allowed or forbidden configurations. A common telephony system can provide access to Voice over Internet Protocol (VoIP) and Public Switched Telephone Networks (PSTN), and configuration can control access.

Configure Logical Partitioning

Logical partitioning allows configuration of Cisco Unified Communications Manager systems, so single-line phones, multiline phones, and analog phones can get configured to prevent restricted calls that mix VoIP and PSTN resources when calls occur between different geolocations. Only geolocations (in the Phone Configuration window) and geolocation filters (in the Device Pool Configuration window) can get configured for phones.

Perform the following steps to configure logical partitioning.

Procedure

Step 1 Enable logical partitioning by setting the value of the Enable Logical Partitioning enterprise parameter to True.

Step 2 Define a set of geolocations on a new Geolocation Configuration window.

Step 3 Assign geolocations to device pools, devices, trunks, gateways, or MGCP ports.

Step 4 Assign geolocations to the default geolocation that the Default Geolocation enterprise parameter specifies.

Step 5 Define the Logical Partitioning Default Policy, which determines whether to allow or deny PSTN calls between devices that associate with valid geolocations and geolocation filters when no explicit Allow/Deny policy is configured in the Logical Partitioning Policy Configuration window for the related geolocation policy records.

Use the Enterprise Parameters Configuration window to set the value for the Logical Partitioning Default Policy enterprise parameter.

Step 6 For devices that do not participate in logical partitioning policy checks, define the geolocation as Unspecified or leave undefined.

Note Devices that do not associate with a geolocation or geolocation filter do not participate in logical partitioning policy checks. This lack of association can get defined at the individual-device level, the device-pool level, or the enterprise-parameter level.

Step 7 Define a set of filter rules in a new Geolocation Filter Configuration window.

Step 8 Assign geolocation filters to device pools, trunks, intercluster trunks, gateways, or MGCP ports.

Step 9 Assign geolocation filter to the default filter that the Logical Partitioning Default Filter enterprise parameter specifies.

Step 10 Define a set of logical partitioning policy records in a new Logical Partitioning Policy Configuration window.

Step 11 Define a set of policies between geolocation policy record device-type pairs:

```
{{Geolocation Policy1, devType1}, {Geolocation Policy2, devType2}, policyValue}
```

Step 12 To allow devices in different clusters to participate in logical partitioning policy checks, turn on location conveyance as follows:

- Check the Send Geolocation Information check box in the intercluster trunk (ICT) or SIP trunk of the local cluster.
- Check the Send Geolocation Information check box in the ICT or SIP trunk of the remote cluster.

Related Topics

Logical Partitioning, on page 795
Enterprise Parameters for Logical Partitioning, on page 802
Geolocation Configuration, on page 582
Geolocation Filter Configuration, on page 588
Logical Partitioning Policy Configuration, on page 830
Configure Location Conveyance, on page 577

Logical Partitioning Feature

Logical partitioning specifies a call control feature in Cisco Unified Communications Manager that provides functionality, so communication between the following pairs of VoIP entities can be controlled:

1. A VoIP phone and a VoIP gateway
2. A VoIP gateway and another VoIP gateway
3. An intercluster trunk and a VoIP phone
4. An intercluster trunk and a VoIP gateway

Options exist to configure Cisco Unified Communications Manager, so any such set of VoIP devices may be allowed communication with each other and any device can be restricted to one device or to a group of devices. No logical partitioning policy logic exists on endpoints.

Be aware that logical partitioning is required to control such communication not only during basic call establishment but also during mid-call as a result of midcall features.

The Cisco Unified Communications Manager basic routing policy constructs of calling search spaces and partitions suffice to prevent forbidden basic calls from being established but are not sufficient to prevent forbidden calls from being created as a result of midcall features. In Cisco Unified Communications Manager, such midcall features are often termed Join and Redirect features, because these primitives often get used internally to affect these features.

Logical partitioning enhances Cisco Unified Communications Manager to handle such midcall scenarios. Configuration for logical partitioning remains independent of supplementary features, where the policy checking gets performed based on devices being joined or redirected to a supplementary feature.

Note Logical partitioning policy checks get performed later than digit analysis/calling search space/partition logic during call processing.

The logical partitioning solution comprises the following elements:

- Identifiers - A framework to associate a unique identifier with every device.
- Policies - Allow administrator the ability to define rules or policies that determine the interconnection between any two devices (a VoIP phone and a gateway) in the Cisco Unified Communications Manager system. The configured policies work bidirectionally between the pair of devices.
- Policy Checking - Call processing and features such as transfer, pickup, and ad hoc conference check the defined policies before allowing the calls or features between participants.

Identifiers

Identifiers specify a device type for every device (element) in a Cisco Unified Communications Manager logical partitioning solution. Device types classify all elements into two types: interior and border. The following table specifies the Cisco Unified Communications Manager devices that associate with each device type:

Table 90: Device Types and Associated Cisco Unified Communications Manager Devices

Device Type	Cisco Unified Communications Manager Device
Border	Gateway (for example, H.323 Gateway) Intercluster trunk (ICT), both gatekeeper-controlled and non-gatekeeper-controlled H.225 trunk SIP trunk MGCP port (E1, T1, PRI, BRI, FXO)

Device Type	Cisco Unified Communications Manager Device
Interior	Phones (SCCP, SIP, third party) CTI route points VG224 analog phones MGCP port (FXS) Cisco Unity Voice Mail (SCCP)

Note For MGCP PRI Q.SIG devices, the internal Cisco Unified Communications Manager device type in Geolocation Info will be “QsigDevice,” which is mapped to “Interior.” “Interior” is used for onnet devices.

Note For Q.SIG ICT trunk, Q.SIG H225 trunk & Q.SIG H323 gateways, the internal Cisco Unified Communications Manager device type in Geolocation Info is “AccessDevice,” which is mapped to “Border.” “Border” is used for offnet devices.

Note You cannot edit the classification of Cisco Unified Communications Manager elements: only border and interior designations are allowed, and a particular device can be classified only according to the scheme specified in the previous table. For example, a SIP trunk can be classified only as a border element.

See the Geolocation Identifiers, on page 580 for further information. See Geolocation Examples, on page 580 for examples of geolocation identifiers.

Allow and Deny Policies

Based on the system requirements for VoIP network topology, you can configure Cisco Unified Communications Manager to provide the following default system policy for logical partitioning:

- Deny - Calls or features get blocked between VoIP device participants of types 1 to 4 (previously enumerated).

  To allow VoIP communication, ensure the Allow policy is configured through logical partitioning configuration.

- Allow - Be aware that calls or features are allowed between VoIP device participants of types 1 to 4 (previously enumerated).

  To deny VoIP communication, ensure the Deny policy is configured through logical partitioning configuration.

Applicability to Requirements From Indian Telecom Regulations

Regulations of the Telecom Regulatory Authority of India (TRAI) require that voice traffic over the enterprise data network and the Public Switched Telephone Network (PSTN) must be strictly separated and no mixing of calls between the two networks can occur for the purpose of toll bypass.

The following list shows basic scenarios that are restricted (that is, not allowed):

- The call that passes through a PSTN gateway connects directly by using WAN to a VoIP phone or VoIP PSTN gateway in a different geographic location.
    - If PSTN gateway is located in India, this remains strictly restricted. If the PSTN is in another country and a VoIP phone is in India and if connection results in revenue loss to Indian telecom service providers, the connection gets considered restricted.

The following list gives basic scenarios that are permitted:

- Call directly between two VoIP phones in different geographic locations
- Call from a VoIP phone to a PSTN gateway in the same geographic location

A call that passes through a PSTN gateway must never connect directly to a VoIP phone or VoIP PSTN gateway in a different site or geographic location (geolocation) through use of IP telephony.

Requirement for Deployments

While following TRAI regulations and avoiding toll bypass, a single-line phone should be able to reach outside VoIP (closed user group [CUG]) or PSTN networks, provided that the suggested configuration guidelines are met.

Note Ensure logical partitioning is enabled to avoid any toll bypass.

Available Cisco Unified Communications Manager Support

Cisco Unified Communications Manager prior to implementation of the logical partitioning feature provides the following support:

- Phones can use the same line to reach the VoIP or PSTN networks.
- The existing calling search space (CSS) and partitions mechanism allows partitioning of the network for basic calls only.

Limitations with a Single Line

The following limitations exist when a single line is used without (or prior to) configuration of the logical partitioning feature:

- Possible midcall Join - A call that connects to a VoIP network on WAN and another call that is made to a PSTN network may get joined upon invocation of a supplementary feature such as Transfer.
- Possible redirects - A call that comes from a VoIP network on WAN may get redirected to a PSTN network upon invocation of a supplementary feature such as Forwarding.

Without the logical partitioning feature, you cannot configure supplementary features to prevent invocation of the restricted scenarios.

Existing Deployments Prior to Use of Logical Partitioning

In India and other countries, separate lines on phones get used to separate the VoIP (CUG) and PSTN networks. This implementation previously prevented use of low-cost analog phones and single-line VoIP phones.

In deployments that use two-line phones, invocation of supplementary features like Join Across Lines (JAL) or Direct Transfer Across Line (DTAL) can result in scenarios that are restricted by TRAI regulations. For such deployments to conform to the regulations, you need the logical partitioning feature.

History

Originally, Indian regulations required that Voice over IP (VoIP) systems be physically separate from PSTN interconnect systems. Users used phones on a VoIP system strictly for interoffice phone calls, but any calls that needed to go to or come from the PSTN had to be made by using the PSTN system. Telecom Regulatory Authority of India (TRAI) regulations as of 2008 permit a single system to support both types of calls, as long as the system can be configured so that forbidden calls cannot complete. In a Cisco Unified Communications Manager system, the term logical partitioning specifies this capability.

The Enterprise VoIP implementations that use releases of Cisco Unified Communications Manager prior to Release 7.1(x) in India use the same Cisco Unified IP Phone for both the VoIP and PSTN connectivity. Cisco Unified Communications Manager does not support specific configurations for controlling the mixing of VoIP and PSTN traffic when supplementary features are invoked from a single line with participants in VoIP or PSTN domains. To comply with regulations, previous VoIP implementations in India used separate lines on VoIP phones for PSTN and VoIP calls.

Cisco Unified Communications Manager uses the concept of partitions and calling search spaces (CSS) for configuration of the respective lines. Thus, control remains separate for the VoIP and PSTN domains, and features like Transfer cannot be performed on single-line phones, because invoking such features could result in joining the VoIP with the PSTN network.

With this limitation, enterprise VoIP deployments in India that use Cisco equipment remained limited to using phones with minimum of two lines, which is not a cost-effective solution for most customers. This limitation also prevented solutions that use low-cost analog phones that are single line by design and use VG224/VG248 gateways.

To overcome the limitations, a Cisco Unified Communications Manager solution now allows logical partitioning of a single line on Cisco Unified IP Phones through administrator policies. Be aware that control of call joining or call redirection is required, based on an attribute tag or the geolocation of the parties.

Overview of Logical Partitioning Architecture

The logical partitioning solution entails provisioning the following elements:

- Configure geolocation identifiers
    - Administrator can define sets of geolocations (civic addresses).
    - Administrator can assign these geolocations to VoIP phones, VoIP gateways, IP trunks, device pools, and enterprise parameters.
    - Administrator can define filters that select a subset of fields from geolocation and associate with VoIP gateways, IP trunks, device pools, and enterprise parameters.

- Configure policies

- Allow administrator to define geolocation policy records and define matrices of geolocation policy records that contain a policy that indicates whether a connection is permitted or denied. The configured policies work bidirectionally between the pair of devices.

  - Communicate geolocation information across clusters

- Allow communication of geolocation information from one cluster to another, both at call establishment as well as midcall joins and redirects.

Logical Partitioning Use of Geolocations and Geolocation Filters

Cisco Unified Communications Manager administrators must define the following items:

- A geolocation for every device that uses logical partitioning. See the Geolocation Characteristics, on page 578 for details.
- A geolocation filter for every device that uses logical partitioning. See the Geolocation Filters Feature, on page 588 for details.

Cisco Unified Communications Manager administrators then assign geolocations and geolocation filters to devices.

The following entities in a Cisco Unified Communications Manager cluster or system can have geolocation and geolocation filter values that are assigned:

- Device pools
- CTI route points
- Phones (optional)
- CTI ports

Note Phones do not specify a drop-down list box for associating a phone with a geolocation filter.

- SIP trunks
- Intercluster trunks (ICT)
- H.323 gateways
- MGCP ports of the following types: T1, E1, PRI, FXO

Media devices, such as media termination points (MTP), conference bridges (CFB), annunciators, and music on hold (MOH) servers, do not need to be associated with geolocations and geolocation filters.

Internally, the device layer of Cisco Unified Communications Manager associates with geolocation values that call processing uses. The following sequence takes place:

1. Devices read the GeolocationPkid and GeolocationFilterPkid for its configuration at device or device-pool level.
2. The devices communicate this Pkid and deviceType information in CC (for example, CcRegisterPartyA) and PolicyAndRSVPRegisterReq messages during call signaling.
3. The call processing and feature layer uses this information for logical partitioning policy checking.

The standard record for a geolocation specifies Unspecified. Use this value when no geolocation needs to associate with a device. For a device, if the geolocation specifies Unspecified or the geolocation filter specifies None, no identifier gets created, and the device does not participate in logical partitioning policy checks.

Be aware that the Default Geolocation enterprise parameter and the Logical Partitioning Default Filter enterprise parameter can be configured from drop-down list boxes on the Enterprise Parameters Configuration window.

Examples of Geolocations and Geolocation Filters

See Geolocation Examples, on page 580 for examples of geolocations.

See Geolocation Filters Feature, on page 588 for examples of geolocation filters.

Logical Partitioning Geolocation Usage for Shared Lines and Route Lists

When the called party specifies a group device, a different geolocation can apply for each device in a group. For the early attended scenarios, the actual connected device is not known until the device gets answered. Thus, the Geolocation information gets aggregated until the device answers.

- The Call Control and Feature layer receives temporary geolocation information (“MixedDevice”) until the device answers.
- The logical partitioning policy checks in the feature layer or LPSession process get ignored until the device answers and the actual geolocation information for the device becomes available.
- This behavior impacts the Early attended Transfer and Early attended Conference features by delaying the logical partitioning policy check until answer time.

Logical Partitioning Usage of Geolocation Identifiers

Geolocation identifiers get constructed from a combination of geolocations, geolocation filters, and device types of Cisco Unified Communications Manager devices.

See the Geolocation Identifiers, on page 580 of the Geolocations and Location Conveyance, on page 575 for details.

Enterprise Parameters for Logical Partitioning

You can use the following enterprise parameters to configure logical partitioning:

- Enable Logical Partitioning - This parameter determines whether the logical partitioning feature is enabled. Logical partitioning policies get used for restricting calls and other supplementary features such as transfer, forward, conferences including Meet-Me, and so on. Valid values specify True (enable logical partitioning) or False (do not enable logical partitioning). When this parameter is set to False, calls do not get validated against any logical partitioning policy. This represents a required field. The default value specifies False.

- Default Geolocation - This parameter determines the default geolocation setting for all devices and device pools that do not have a specified geolocation in Cisco Unified Communications Manager Administration. Valid values include the names of all the geolocations that have been configured in the Geolocation Configuration window in Cisco Unified Communications Manager Administration. The default geolocation can get overridden on a per-device and per-device-pool basis in the Device Configuration window or the Device Pool Configuration window in Cisco Unified Communications Manager Administration. This represents a required field. The default value specifies Unspecified.

- Logical Partitioning Default Policy - This parameter determines the default policy for allowing or denying calls between geolocations. Before calls between geolocations are allowed to proceed, Cisco Unified Communications Manager checks to be sure that calls are allowed between the specified geolocations based on the setting in the Logical Partitioning Policy Configuration window in Cisco Unified Communications Manager Administration. If Use System Default is specified in the Logical Partitioning Policy Configuration window, the value in this parameter determines whether calls are allowed or denied. Valid values specify Allow (allow calls to proceed) or Deny (do not allow calls to proceed). This represents a required field. The default value specifies Deny.

- Logical Partitioning Default Filter - This parameter determines the default filter for geolocations in the logical partitioning feature. Applying a filter to geolocations allows you to reduce the number of fields on the Geolocation Configuration window that apply to devices and device pools that belong to that geolocation. To choose a filter in this parameter, you must ensure that the filter is already configured in the Geolocation Filter Configuration window in Cisco Unified Communications Manager Administration. Valid values include None (do not include any geolocation fields) and the names of all the filters that are configured in the Geolocation Filter Configuration window in Cisco Unified Communications Manager Administration. The default value specifies None.

Logical Partitioning Policies

Ensure logical partitioning policies are configured for the required interconnection behavior between the following entities:

- Between PSTN gateways and VoIP phones
- Between PSTN gateway and PSTN gateway
- Between an intercluster trunk (ICT) and a VoIP phone
- Between an ICT and a VoIP gateway

The System Default Policy enterprise parameter (Default value=DENY) represents the default policy when no configured policy is found.

Ensure Allow and Deny policies are configured. See the Logical Partitioning Feature, on page 796 for configuration details.

In the Logical Partitioning Policy Configuration window (**Call Routing** > **Logical Partitioning Policy Configuration** menu option in Cisco Unified Communications Manager Administration), the administrator must create geolocation policy records from a subset of the fields that are configured for geolocations. See the Logical Partitioning Policy Configuration, on page 830 for details of using Cisco Unified Communications Manager Administration to create logical partitioning policy records.

Configure logical partitioning policies between pairs of geolocation policy records and device types.

Example of Logical Partitioning Policy

({geolocpolicy1, devType1}, {geolocpolicy2, devType2}, Allow)

The following tables show the construction of a logical partitioning policy among geolocations, device types, and policy types.

First, assume the following geolocation policy records:

Geolocation Policy	Record Data
BLRBLD1GeolocPolicy	(country=IN, A1=KA, A3=Bangalore, LOC=BLD1)
BLRBLD2GeolocPolicy	(country=IN, A1=KA, A3=Bangalore, LOC=BLD2)
MUMBLD1GeolocPolicy	(country=IN, A1=MH, A3=Mumbai, LOC=BLD1)
blankGeolocPolicy	() – All fields blank

From these records, you can configure the following sample logical partitioning policies. The system default policy specifies DENY.

Source			Target	
DevType1	GeolocationPolicy1	DevType2	GeolocationPolicy2	Policy
Border	BLRBLD1GeolocPolicy	Interior	BLRBLD1GeolocPolicy	ALLOW
Border	BLRBLD1GeolocPolicy	Border	BLRBLD1GeolocPolicy	ALLOW
Border	BLRBLD2GeolocPolicy	Interior	BLRBLD2GeolocPolicy	ALLOW
Border	BLRBLD2GeolocPolicy	Border	BLRBLD2GeolocPolicy	ALLOW
Border	MUMBLD1GeolocPolicy	Interior	MUMBLD1GeolocPolicy	ALLOW
Border	MUMBLD1GeolocPolicy	Border	MUMBLD1GeolocPolicy	ALLOW

The first logical partitioning policy,

Border	BLRBLD1GeolocPolicy	Interior	BLRBLD1GeolocPolicy	ALLOW

allows all the traffic to and from gateways that match BLRBLD1GeolocPolicy to and from VoIP phones that match BLRBLD1GeolocPolicy.

If more granular policies are required, the geolocation NAM field allows naming the devices within a building.

Example

- Between desktop phones and gateway1 in BLD1 of Bangalore

  Interior:(country=IN, A1=KA, A3=Bangalore, LOC=BLD1, NAM=deskphone)

  Border:(country=IN, A1=KA, A3=Bangalore, LOC=BLD1, NAM=gateway1) = Allow

- Between Cisco IP Softphones and ICT1 in BLD1 of Bangalore

  Interior:(country=IN, A1=KA, A3=Bangalore, LOC=BLD1, NAM=softphone)

  Border:(country=IN, A1=KA, A3=Bangalore, LOC=BLD1, NAM=ICT1) = Allow

Devices that have geolocation fields that match the preceding policies can communicate as per policy.

See the Logical Partitioning Policy Configuration, on page 830 for details of how to use Cisco Unified Communications Manager Administration to configure logical partitioning policies.

LPPolicyManager and Policy Tree

LPPolicyManager specifies a singleton process that interfaces with database and maintains policies in call processing as logical partitioning policy tree. During Cisco Unified Communications Manager service startup, the LPPolicyManager reads the policies from database tables and constructs the logical partitioning policy tree.

The add/delete/update of a policy in the database results in change notification to LPPolicyManager, and the change takes place in the logical partitioning policy tree.

Call processing interfaces with LPPolicyManager to read the logical partitioning policies that correspond to the geolocation policy records for the devices.

The LPPolicyManager provides utility functions for these search types:

- Geolocation information for a pair of devices
- Geolocation information for existing devices versus a new participant
- Geolocation information for existing devices versus list of new participants

Policy Tree Example

This section presents examples of a policy tree.

The following figure provides an example of a policy tree for logical partitioning policies for India between geolocation policy records for gateways in Bangalore (BLD1, BLD2) and VoIP phones in Bangalore (BLD1, BLD2).

Note Normally, only one pair of policies gets configured between a particular source geolocation policy record and a particular target geolocation policy record.

The policy tree gets constructed so that a paired policy is represented as a source and target portions on the tree.

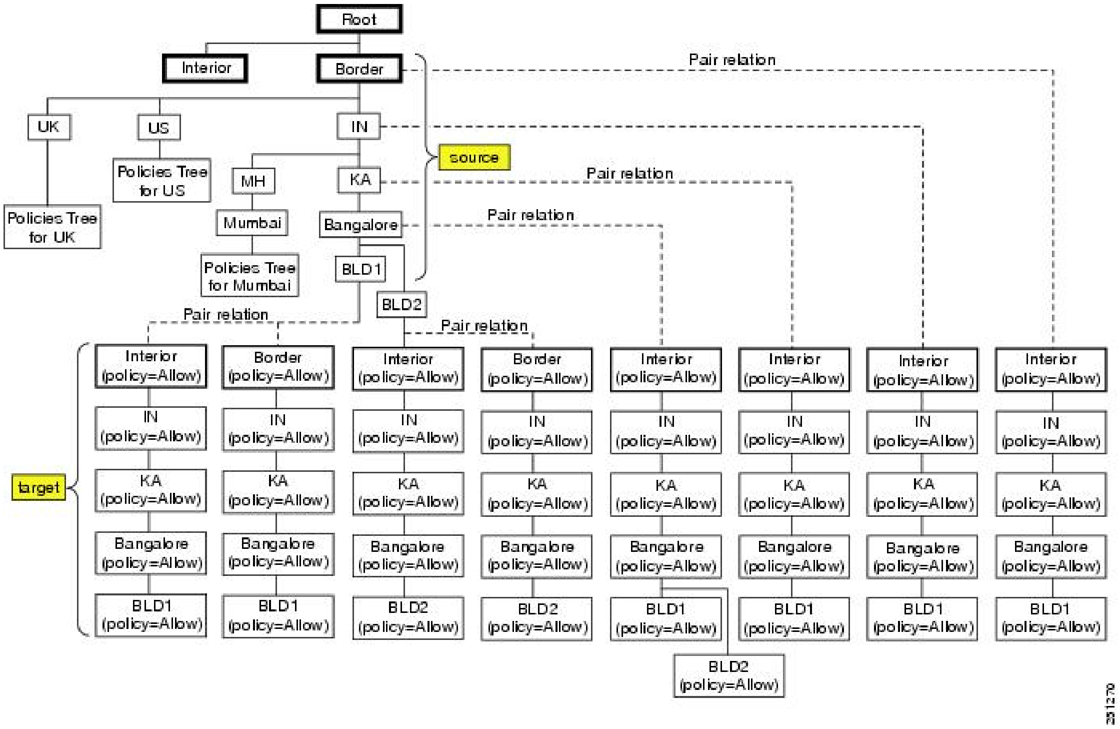
For example, the policy records with data Src=Border:IN:KA:Bangalore:BLD1 and Target=Interior:IN:KA:Bangalore:BLD1 with policy Allow associate with the following nodes:

- Border, IN, KA, Bangalore, BLD1 in the source portion
- Interior, IN, KA, Bangalore, BLD1 in the target portion

For this example, the Allow policy gets configured in the leaf node of the target portion.

The figure shows that the target portion of the tree can have a possible policy at each level. That is, each node (Interior, IN, KA, Bangalore, and BLD1) can have a policy.

Figure 74: Example Policy Tree for Logical Partitioning Policies for India



See the Logical Partitioning Policy Search Algorithm, on page 807 for a discussion of the logical partitioning policy search algorithm for searching through a policy tree and a listing that shows all permutations of possible policies that are found in this example policy tree.

Policy Tree Construction

The policy tree construction follows a fixed algorithm. The policy tree includes a source portion and a target portion.

1. [GLP_X Border GLP_Y Interior] policy gets added. The construction takes the source portion from GLP_X Border and the target portion from GLP_Y Interior.

2. [GLP_Y Interior GLP_X Border] policy gets added. The construction takes the source portion from GLP_X Border and the target portion from GLP_Y Interior.

   Thus, the Border-to-Interior policy specifies that the Border part always originates in the source portion of the tree. The policy gets added in a leaf node.

3. [GLP_X Border GLP_Y Border] policy gets added.

First, a determination decides whether to add GLP_X in the source portion or GLP_Y in the source portion.

If no existing policy matches any tokens of GLP_X or GLP_Y (due to other GLP policy), the tree construction takes the source portion from GLP_X Border and the target portion from GLP_Y Border.

If an existing policy matches some tokens in the source portion, the source portion gets taken from that GLP.

Example 1: GLP_Y Border GLP_X Interior is already configured.

Because GLP_Y is already used in the source portion, to add the [GLP_X Border GLP_Y Border] policy, the GLP_Y gets added in the source portion.

Example 2: If the two policies, [GLP_X Border GLP_Y Interior] and [GLP_Y Border GLP_X Interior] exist, two source branches exist that both start with Border.

Assume that GLP_B overlaps more tokens with GLP_X (as compared to GLP_Y) and GLP_A does not match any Border branches.

To add the [GLP_A Border GLP_B Border] policy, the policy gets searched as to whether GLP_A or GLP_B can fit in the existing source branches.

As GLP_B matches some tokens from GLP_X, the portion of the tree gets shared with GLP_X.

Assume that Border:IN:KA:BLR:BLD1 to Border:IN:MH:MUM:BLD1 exists.

Adding Border:IN:MH:Pune:BLD1 to Border:IN:KA:BLR:BLD2 policy uses the source portion of Border:IN:KA:BLR and adds BLD2 in the leaf of the source tree and adds a target portion of Border:IN:MH:Pune:BLD1.

Thus, for Border-to-Border policies, the policy tree gets constructed to fit best in the existing source and target branches. Consider sharing as many nodes as possible as preferable.

Logical Partitioning Policy Search Algorithm

This section explains the logical partitioning policy search algorithm.

The logical partitioning policy search algorithm functions as follows:

- Policies get searched during call control or feature interactions.
- The configured tree of policies gets used for run-time searching of the configured policy by using tree traversal.
- The policy gets searched between a pair of devices by using geolocation information (that is, geolocation, geolocation filter, and device type) of both the source (A) device and target (B) device.

Basic Operation

Construct a list of name/value pairs from the geolocation and geolocation filter information (that is, pairList1 and pairList2).

Example: pairList =”Country=IN:A1=KA:A3=Bangalore:LOC=BLD1”

Input for the search specifies {pairList1, devType1}, {pairList2, devType2}.

The following steps take place during the policy search:

1. If devType1=Border and devType2=Interior, set {devTypeA=devType1, pairListA= pairList1} and {devTypeB=devType2, pairListB= pairList2}.
2. If devType1=Interior and devType2=Border, set {devTypeA=devType2, pairListA= pairList2} and {devTypeB=devType1, pairListB= pairList1}.
3. Match the exact pair by searching the nodes of a policy tree. Use values from {devTypeA, pairListA} and find the source branch of the tree.

4. Use values from {devTypeB, pairListB} and find the target (paired) branch of the tree.
5. If an exact match is found in the tree and the policy is configured, use the policy data that is configured in the leaf node and return the policy value.
6. If exact match is not found, find a match by stripping one column from pairListB input (that is, go one level up on target [paired] branch of policy tree and check whether policy data is configured in the corresponding node).
7. If a match is found, return the policy value; otherwise, continue going up the paired branch of the policy tree and check whether policy data is configured.
8. If a policy is not found, go one level (node) up on the source branch that corresponds to pairListA.
9. Repeat steps until a policy is found or the root node is reached.
10. If devType1=Border and devType2=Border, search for exact match by traversing. Use {devTypeA=devType1, pairListA= pairList1}, and {devTypeB=devType2, pairListB= pairList2}. If not found, traverse and use {devTypeA=devType2, pairListA= pairList2} and {devTypeB=devType1, pairListB= pairList1}.

Note The tree layout can specify any order, based on how the administrator added policies, so you need to use both combinations to search the tree.

Assume that the policy is searched with the following data:

(devTypeA = “Border”, pairListA = “Country=IN:A1=KA:A3=Bangalore:LOC=BLD1”, devTypeB = “Interior”, pairListB = “Country=IN:A1=KA:A3=Bangalore:LOC=BLD1”).

The following table shows all permutations of possible policies, any value specifies a match. The search algorithm proceeds in the order that the table specifies for finding the configured policy.

The first found match specifies an entry from which the configured policy gets used.

Table 91: Example of Policy Variations in Policy Configuration and Order of Policy Search

GeolocationValueA	GeolocationValueB	Policy
Border:IN:KA:Bangalore:BLD1	Interior:IN:KA:Bangalore:BLD1	Allow/Deny
Border:IN:KA:Bangalore:BLD1	Interior:IN:KA:Bangalore	Allow/Deny
Border:IN:KA:Bangalore:BLD1	Interior:IN:KA	Allow/Deny
Border:IN:KA:Bangalore:BLD1	Interior:IN	Allow/Deny
Border:IN:KA:Bangalore:BLD1	Interior	Allow/Deny
Border:IN:KA:Bangalore	Interior:IN:KA:Bangalore:BLD1	Allow/Deny
Border:IN:KA:Bangalore	Interior:IN:KA:Bangalore	Allow/Deny
Border:IN:KA:Bangalore	Interior:IN:KA	Allow/Deny
Border:IN:KA:Bangalore	Interior:IN	Allow/Deny

GeolocationValueA	GeolocationValueB	Policy
Border:IN:KA:Bangalore	Interior	Allow/Deny
Border:IN:KA	Interior:IN:KA:Bangalore:BLD1	Allow/Deny
Border:IN:KA	Interior:IN:KA:Bangalore	Allow/Deny
Border:IN:KA	Interior:IN:KA	Allow/Deny
Border:IN:KA	Interior:IN	Allow/Deny
Border:IN:KA	Interior	Allow/Deny
Border:IN	Interior:IN:KA:Bangalore:BLD1	Allow/Deny
Border:IN	Interior:IN:KA:Bangalore	Allow/Deny
Border:IN	Interior:IN:KA	Allow/Deny
Border:IN	Interior:IN	Allow/Deny
Border:IN	Interior	Allow/Deny
Border	Interior:IN:KA:Bangalore:BLD1	Allow/Deny
Border	Interior:IN:KA:Bangalore	Allow/Deny
Border	Interior:IN:KA	Allow/Deny
Border	Interior:IN	Allow/Deny
Border	Interior	Allow/Deny

For a given pair of geolocation identifiers, if no configured policy is found, the Logical Partition Default System Policy gets used.

Policy Checking

Policy checking takes place in the following situations:

- Policy checking occurs for all calls that connect a PSTN gateway and a VoIP phone.
- Policy checking occurs for all calls that invoke supplementary services, such as Transfer and Conference, that connect a PSTN gateway and VoIP phones.
- All restricted calls and connections based on policies get denied.

Deny Policy Handling

When calls are denied because of logical partitioning policy, the following handling occurs:

- Basic calls get cleared with a reorder tone that Cisco Unified Communications Manager sends.

  - Q.850-compliant devices (SCCP, H323. MGCP) get cleared by using cause code=63 “Service or option not available.”
  - SIP line or trunk gets cleared by using SIP status code=503 “Service unavailable.”
- Features get handled based on the individual feature
  - If call clearing is involved, the cause code=63 or SIP status code=503 gets used.
  - Feature=based message gets sent to VoIP phones for display on the status line.
  - For analog phones that invoke a feature, Transfer results in both calls getting cleared. Conference clears the secondary call to play reorder tone to the analog phone.

LPSession Infrastructure and Policy Checking

LPSession specifies an infrastructure that enhances the Cisco Unified Communications Manager Resource Reservation Protocol (RSVP) infrastructure to provide a centralized policy-checking infrastructure.

Note The enhancement of the RSVP infrastructure is based on similar paired policy checking behavior for logical partitioning. Logical partitioning has no impact on RSVP policy checking and vice-versa.

The following operations use LPSession infrastructure for policy checking:

- Basic calls
- Redirections (for example, Forwarding, Redirecting features, and Park reversion)
- Split/Join primitive

The commonly used features perform logical partitioning policy checks in the feature layer before Split/Join or Redirection:

- Transfer
- Ad Hoc Conference
- Meet-me Conference
- Pickup
- Call Park and Directed Call Park

Other existing Split/Join features and similar features depend on LPSession infrastructure for Split/Join primitive-level policy checking (for example, MKI for Cisco Unified Mobility).

Logical Partitioning Handling

This section describes logical partitioning handling with a basic call.

Operation

The logical partitioning policy gets checked between the geolocation policy records of the calling device and the called device.

Configuration

The calling device and the called device both associate with a geolocation and geolocation filter.

When

Logical partitioning handling takes place in the following circumstances:

- During a basic call between a VoIP phone and a PSTN gateway, a PSTN gateway and another PSTN gateway, an ICT and a PSTN gateway, or an ICT and another ICT.
- During Post Digit Analysis, which uses configured calling search spaces and partitions for routing the calls.
- Cisco Unified Communications Manager uses the geolocation identifier information that associates with the incoming and outgoing Cisco Unified Communications Manager device to perform logical partitioning policy checking.
- The configured logical partitioning policy returns to an outgoing Cisco Unified Communications Manager device layer, which takes action accordingly.

When Not

Logical partitioning handling does not take place in the following circumstances:

- When both the calling and called devices specify VoIP phones (DevType=Interior).
- When geolocation or geolocation filter is not associated with any device.

Deny Handling

Logical partitioning handles a denied call as follows:

- The call gets denied/rejected with a reorder tone.
- The call does not get extended to a phone, gateway, or intercluster trunk.
- The Number of Basic Call Failures perfmon counter gets incremented.

Logical Partitioning Interaction with Geolocation Conveyance

If logical partitioning applies to a multicluster environment, ensure location conveyance is configured.

Location conveyance configuration entails the same configuration as logical partitioning configuration for a single-cluster environment, but additional configuration must take place for devices that belong to remote clusters.

For the details of configuring logical partitioning for systems that do not require location conveyance, see the Configure Logical Partitioning, on page 795.

To support logical partitioning scenarios that involve participants across clusters requires the following support from SIP trunks and intercluster trunks:

- The geolocation and device type information gets sent from one cluster to another cluster.
- This information gets sent both at call establishment and at midcall joins and redirects.
- The geolocation filter gets configured on the trunk.
    - This configuration allows creation of geolocation identifiers. Based on these geolocation identifiers, policy records may be configured for logical partitioning policy checks.

The geolocation gets sent across clusters if the Send Geolocation Information check box gets checked upon configuration of the SIP trunk or intercluster trunk:

- If geolocation is configured for a device, the geolocation information gets sent in call signaling across the trunk for SIP trunk or intercluster trunk interactions.

Note Location conveyance does not depend on any logical partitioning configuration.

For additional details, see the Geolocation Conveyance Across SIP Trunks and Intercluster Trunks, on page 593.

The Configure Location Conveyance, on page 577 provides a detailed checklist for configuring location conveyance.

Logical Partitioning Handling of a Received Geolocation

If the receiving cluster is enabled for logical partitioning, the receiving cluster uses the received PIDF-LO geolocation information for logical partitioning policy checks with the devices on Cisco Unified Communications Manager.

For additional details, see the Handle a Received Geolocation, on page 594.

Also, see the Interactions, on page 814 for a list of features that use geolocation information for policy checking.

Logical Partitioning Feature Interactions with Midcall Geolocation Change

If logical partitioning is enabled, the following actions take place:

- SIP trunk or intercluster trunk checks the logical partitioning policy and takes an action that is based on the configured policy.
- The feature layer, such as Conference or Meet-me, rechecks the logical partitioning policy based on the updated geolocation information for the trunk device.

For feature interactions that involve a midcall geolocation change, see the Feature Interactions with Midcall Geolocation Change, on page 594.

Also, see the Interactions, on page 814 for a list of features that use geolocation information for policy checking.

Dynamic SIP Trunks

For dynamic SIP trunks, such as Cisco Intercompany Media Engine (IME), Service Advisement Framework (SAF), or Cisco Extension Mobility Cross Cluster (EMCC), the target cluster varies depending on the pointed destination. The device-level geolocation and geolocation filter that can be configured on these trunks may not have the flexibility to vary depending on the destination. Such SIP trunks must be configured appropriately to allow or deny traffic from these trunks. Cisco Systems recommends using location conveyance functionality, which allows the actual geolocation to propagate across clusters and helps in accurate logical partitioning policy checking.

SIP Trunk or Intercluster Trunk Configuration Requirement

A cluster for which logical partitioning is enabled exhibits the following typical behaviors:

1. Traffic between VoIP phones and SIP trunk (or intercluster trunk [ICT]) gets allowed.
2. Traffic between SIP trunk (or ICT) and PSTN gateways gets blocked.
3. VoIP-only traffic between SIP trunk (or ICT) and SIP trunk (or ICT) gets allowed.

Logical partitioning policies must get configured to achieve these behaviors.

Interaction with Non-Location Conveyance Cluster

To achieve behaviors 1 and 3, you need to configure one policy each. If default policy specifies Deny, you do not need any policy for behavior 2.

For behaviors 1 and 3, because no location conveyance exists, a logical partitioning cluster cannot identify whether traffic is VoIP-only or comes from a gateway in a remote cluster. This means that typically, all traffic must be allowed from SIP trunk (or ICT) to VoIP phones or other SIP trunk (or ICT).

Interaction with Location Conveyance Cluster

For behavior 1, the VoIP phone that calls a SIP trunk (or ICT) needs a policy that allows extension of the call on the trunk. This occurs before receipt of location conveyance information from the remote cluster.

For incoming VoIP call from SIP trunk (or ICT), you do not need any policy for calling VoIP phones. If traffic from SIP trunk (or ICT) needs to be allowed to any other ICT or PSTN gateway, you require a corresponding policy.

Example

Ensure the SIP trunk that points from Bangalore to RCDN cluster is configured as follows:

Geolocation = “IN:KA:Bangalore:ICTToRCDN”

Geolocation Filter = “UseCountry, UseA1, UseA3, UseNam”

This configuration specifies the geolocation identifier for SIP trunk as follows:

{“IN:KA:Bangalore:ICTToRCDN”, devType=Border}

Configure logical partitioning policies as follows:

“Border:IN:KA:Bangalore:ICTToRCDN” to Interior = Allow

Result: All VoIP phones in Bangalore cluster can communicate with Richardson.

“Border:IN:KA:Bangalore:ICTToRCDN” to “Border:IN:KA:Bangalore:ICTToRCDN” = Allow Result: ICTs can communicate.

These policies fulfill behavior 1 and 3 requirements.

For location conveyance scenarios, ensure the policies are configured based on geolocation configurations and device type for devices across the cluster.

System Requirements for Logical Partitioning

Logical partitioning requires the following software components:

- Cisco Unified Communications Manager 7.1 or later
- Cisco CallManager service that is running on at least one server in the cluster
- Cisco Unified Communications Manager Locale Installer, that is, if you want to use non-English phone locales or country-specific tones
- Microsoft Internet Explorer 7 or Microsoft Internet Explorer 8 or FireFox 3.x or Safari 4.xr

Interactions and Limitations

This section describes the interactions and restrictions for logical partitioning.

Interactions

This section details the interactions between logical partitioning and the supplementary features and call processing entities that are listed.

Note Configure the Logical Partitioning Default Policy enterprise parameter, and configure a corresponding logical partitioning policy through the **Call Routing** > **Logical Partitioning Policy Configuration** menu option.

Logical partitioning also interacts with the following Cisco Unified Communications Manager components:

- Bulk Administration Tool - For information on how the Bulk Administration Tool (BAT) supports logical partitioning, see the *Cisco Unified Communications Manager Bulk Administration Guide*.
- Call Detail Records - For logical partitioning failures, existing call termination cause codes and new Cisco-specific call termination cause codes get used. For more information on CDRs, see the *Cisco Unified Communications Manager Call Detail Records Administration Guide*.
- Real Time Monitoring Tool - The Real Time Monitoring Tool provides a set of performance monitoring (perfmon) counters for the Cisco Call Restriction object that increment in the event of logical partitioning failures. The Real Time Monitoring Tool also tracks a Logical Partitioning Failures Total counter in the Call Activity window. For more information on the Real Time Monitoring Tool, see the *Cisco Unified Real Time Monitoring Tool Administration Guide*.

- Cisco Unified Reporting - Cisco Unified Reporting generates reports that provide information about logical partitioning policies. For more information on the reports that Cisco Unified Reporting generates, see the *Cisco Unified Reporting Administration Guide*.

Call Forwarding

This section describes the interaction of logical partitioning with the Call Forwarding feature.

Operation

The logical partitioning policy check gets performed between the geolocation identifier of the device from which call is coming and the device to which the call is forwarded.

Configuration

The caller device and a forwarded device associate with a geolocation and geolocation filter.

When

Logical partitioning handling takes place in the following circumstances:

- When an incoming call is received for a device that is call forwarded to another device, the Forwarding feature invocation takes place.
- One of the devices specifies a PSTN participant.
- Cisco Unified Communications Manager uses the geolocation identifier information that associates with the incoming and forwarded Cisco Unified Communications Manager devices for performing logical partitioning policy checking.
- The configured logical partitioning policy returns to the forwarded Cisco Unified Communications Manager device, which takes action accordingly.
- This handling applies to all variations of call forwarding; for example, Call Forward All (CFwdAll), Call Forward No Answer (CFNA), and Call Forward Busy (CFB).

When Not

Logical partitioning handling does not take place in the following circumstances:

- When both the caller and forwarded devices are VoIP phones (DevType=Interior).
- When geolocation or geolocation filter does not associate with any device.

Deny Handling

Logical partitioning handles a denied call as follows:

- The calling device receives a reorder tone from Cisco Unified Communications Manager.
    - Q.850-compliant devices (phone that is running SCCP, H323, or MGCP device) get cleared by using cause code=63 “Service or option not available.”
    - SIP line or trunk gets cleared by using SIP status code=503 “Service unavailable.”

Call Transfer

This section describes the interaction of logical partitioning with the Call Transfer feature.

Operation

The logical partitioning policy check gets 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.

Configuration

The transferred device and a transferred destination device associate with a geolocation and geolocation filter.

When

Logical partitioning handling takes place in the following circumstances:

- When a phone uses a Transfer softkey to transfer the call, the second Transfer key press results in Transfer feature invocation and processing.
- Similarly, other mechanisms (for example, Direct Transfer, OnHook Transfer, Hook Flash Transfer, CTI-application-initiated Transfer) that result in Transfer feature invocation get included.
- The transferred or/and transferred destination specifies a PSTN participant.
- Cisco Unified Communications Manager uses the geolocation identifier information that associates with the transferred and transferred destination Cisco Unified Communications Manager device to perform logical partitioning policy checking.
- This handling normally gets performed before splitting of the primary and secondary calls and before joining.

When Not

Logical partitioning handling does not take place in the following circumstances:

- When both the Transferred and Transferred Destination devices are VoIP phones (DevType=Interior).
- When geolocation or geolocation filter does not associate with any device.

Deny Handling

Logical partitioning handles a denied call as follows:

- Sends External Transfer Restricted message to the VoIP phone.
- Normal Transfer - For phone that is running SCCP, the primary call remains on hold, and consultation call remains active. For phone that is running SIP, both primary and consultation calls remain on hold and need to be resumed manually after the failure.
- Onhook, HookFlash and Analog-Phone-Initiated Transfer - Both the primary and secondary calls get cleared by using cause code=63 “Service or option not available” with a reorder tone from Cisco Unified Communications Manager.
- The Number of Transfer Failures perfmon counter gets incremented.

Interaction with Block OffNet to OffNet Transfer Service Parameter

The Block OffNet to OffNet Transfer service parameter allows the Transfer feature to block the transfer operation when both Transferred and Transferred Destinations specify offnet calls.

See the Set the Block OffNet to OffNet Transfer Service Parameter, on page 572 in the External Call Transfer Restrictions, on page 567 chapter of this guide for more information about this service parameter.

The Cisco Unified Communications Manager cluster or system that is disabled for logical partitioning retains the expected behavior that this service parameter specifies.

Logical Partitioning-Enabled Cluster or System

In a logical partitioning-enabled Cisco Unified Communications Manager cluster, or system, you can configure the system to allow multiple Voice Gateway (PSTN) participants that use the GeolocationPolicy, GLPolicyX, in a supplementary feature by configuring a policy such as the following one:

GLPolicyX Border GLPolicyX Border Allow

After Cisco Unified Communications Manager configures such a policy, be aware that all features (such as Forwarding, Transfer, Ad Hoc Conference, and so forth) are allowed between participants that use GeolocationPolicy, GLPolicyX Border. For example, forwarding a call that comes from a party that uses GLPolicyX Border to another party that uses GLPolicyX Border gets allowed.

Assume that Cisco Unified Communications Manager deployment requires that all supplementary features except the Transfer feature function for such participants. If so, the Block OffNet to OffNet Transfer service parameter can block transfer between offnet devices even if the logical partitioning policy is allowed.

This service parameter controls only the blocking of offnet-to-offnet transfers and does not impact any other supplementary features. Thus, the following details highlight scenarios that involve voice-gateway-to-voice-gateway transfers.

Details

1. Border-to-Border Logical Partitioning Policy Specifies Deny

   For Transfer operation between parties that use this geolocation policy, Cisco Unified Communications Manager denies the transfer. The “External Transfer Restricted” message displays to the transferring party.

   The Cisco Unified Communications Manager setting (either True or False) for the Block OffNet to OffNet Transfer service parameter does not affect the Transfer operation.

   The logical partitioning Deny policy takes precedence, and Cisco Unified Communications Manager follows the policy strictly.

2. Border-to-Border Logical Partitioning Policy Specifies Allow

   For Transfer operation between parties that use this geolocation policy, Cisco Unified Communications Manager checks the allow policy and also checks the setting of the Block OffNet to OffNet Transfer service parameter. This service parameter thus affects the transfer between offnet participants.

3. Block OffNet to OffNet Transfer service parameter specifies True - Cisco Unified Communications Manager checks whether both parties (transferred and transferred destination) are offnet. If so, the transfer of such calls gets denied, and the “External Transfer Restricted” message displays to the transferring party.

   Because transfer gets blocked due to the service parameter, the serviceability Perfmon counter for Logical Partitioning Transfer Failures does not increment.

4. Block OffNet to OffNet Transfer service parameter specifies False - Transfer succeeds.

Offnet/Onnet Behavior for a Device

For outgoing calls, the Call Classification setting in the Route Pattern Configuration window determines the offnet or onnet value. The Call Classification value in the Route Pattern Configuration window overrides the device-level configuration or the corresponding value of the Call Classification service parameter.

For incoming calls, the device-level configuration or the corresponding Call Classification service parameter value determines the offnet or onnet value.

Ad Hoc Conference, Join, Join Across Lines (JAL)

This section describes the interaction of logical partitioning with the Ad Hoc Conference, Join, and JAL features.

Operation

Establishing Conference - The logical partitioning policies get checked between the geolocation identifiers of the devices that are invited to an ad hoc conference.

Established Conference - The logical partitioning policies get checked between the geolocation identifiers of each of the devices that are already in the conference and the device that is invited to the conference.

Configuration

The participant devices associate with a geolocation and a geolocation filter.

The conference bridge does not need to associate with geolocation or geolocation filter; only participants associate, and policy checks get performed for the participants.

When

Logical partitioning handling takes place in the following circumstances:

- A phone uses a Conference softkey to establish or extend an ad hoc conference or a CTI application initiates ad hoc conference.
- The second Conference key press results in conference feature invocation and processing.
- Cisco Unified Communications Manager uses participant geolocation identifier information for policy checking.
- In an established conference, policy checking occurs again, based on changed participant geolocation identifier information for midcall updates. For example, policy checking occurs during call state change, such as Alerting to Answer, Hold/Remote-Resume, Transfer, Call Park Retrieval, Redirection, and so forth.
- PSTN participants are involved.

When Not

Logical partitioning handling does not take place in the following circumstances:

- When all participants are VoIP phones (DevType=Interior).
- When geolocation or geolocation filter does not associate with a device, no policy check takes place for that device.

Deny Handling

Logical partitioning handles a denied conference as follows:

- For the establishing-conference case, the CFB does not get allocated.
- For phones that are running SCCP or phones that are running SIP, the primary call leg gets put on hold and the consultation call remains active. If the primary call leg needs to resume, resumption must take place manually.
- The Conference is Unavailable message gets sent to the VoIP phone that initiates the conference.
- When an analog phone initiates the conference, the secondary call gets cleared by using cause code=63 "Service or option not available" with a reorder tone from Cisco Unified Communications Manager.
- The Number of Adhoc Conference Failures perfmon counter increments.

Meet-Me Conference

This section describes the interaction of logical partitioning with the Meet-Me Conference feature.

Operation

The logical partitioning policies get checked between the geolocation identifiers of each of the devices that are already in the meet-me conference and the device that is attempting to join the conference.

Configuration

The participant devices associate with a geolocation and a geolocation filter.

Be aware that the conference bridge is not required to be associated with a geolocation or geolocation filter; only participants get associated, and policy checks get performed for the participants.

When

Logical partitioning handling takes place in the following circumstances:

- Requirement exists for PSTN participant involvement.
- Policy checks get supported during joining of participants. When a participant dials the meet-me number to join in a meet-me conference, the participant geolocation gets used for policy checking before the new participant is allowed to join the meet-me conference.
- In an established meet-me conference, the updated policy of the participant gets used for policy checking during midcall updates (such as Hold-Resume, Transfer, Barge, cBarge, Call Park Retrieval, and so forth).

When Not

Logical partitioning handling does not take place in the following circumstances:

- When all participants are VoIP phones (DevType=Interior), handling does not occur.
- When geolocation or geolocation filter does not associate with a device, no policy check takes place for that device.

Deny Handling

Logical partitioning handles a denied call as follows:

- The MeetMe is Unavailable message gets sent to the VoIP phone.
- The existing conference does not get affected.
- The call gets cleared with reorder tone from Cisco Unified Communications Manager.
    - Q.850-compliant devices (phone that is running SCCP, H323, or MGCP device) get cleared by using cause code=63 “Service or option not available.”
    - SIP line or trunk gets cleared by using SIP status code=503 “Service unavailable.”
- The Number of Meet-Me Conference Failures perfmon counter increments.

Call Pickup

This section describes the interaction of logical partitioning with the Call Pickup feature.

Operation

The logical partitioning policies get checked between the geolocation identifiers of the calling device and that of the device that picks up the call.

Configuration

The calling device and the device that attempts pickup associate with a geolocation and a geolocation filter.

When

Logical partitioning handling takes place in the following circumstances:

- A PSTN device calls a VoIP phone (A) to which another VoIP phone (B) has a Pickup group relation (for example, both phones belong to the same pickup group).
- When phone B attempts pickup by pressing either Pickup, OPickup, Group Pickup, or BLF Pickup button, the Pickup feature gets invoked.
- Cisco Unified Communications Manager uses geolocation identifier information of the calling device and of device picking up call for policy checking.
- When only one alerting call occurs, the corresponding logical partitioning policy gets treated as final.
- When multiple alerting calls occur, the logical partitioning policy gets checked for each alerting call, starting from the longest alerting call until logical partitioning policy is allowed and call is picked up. If last processed alerting call has logical partitioning Deny policy and no more alerting calls occur, deny handling action takes place.

When Not

Logical partitioning handling does not take place in the following circumstances:

- When the caller consists of a VoIP phone (DevType=Interior), handling does not occur.
- When geolocation or geolocation filter does not associate with devices, no policy check occurs.

Deny Handling

Logical partitioning handles a denied pickup as follows:

- PickUp is Unavailable message gets sent to the VoIP phone that attempts pickup.
- The alerting call does not get affected.
- For multiple alerting calls (mixture of Allowed and Deny policy), if a call with deny policy fails for pickup first, Cisco Unified Communications Manager proceeds by picking up the next alerting call.
- Cisco Unified Communications Manager sends reorder tone to the phone that attempts the pickup.
  - Q.850-compliant devices (phone that is running SCCP) get cleared by using cause code=63 “Service or option not available.”
  - SIP phone gets cleared by using SIP status code=503 “Service unavailable.”
- The Number of Pickup Failures perfmon counter increments.

Call Park and Directed Call Park

This section describes the interaction of logical partitioning with the Call Park and Directed Call Park features.

Operation

The logical partitioning policies get checked between the geolocation identifier of the device that is retrieving the call and the geolocation identifier of the parked party

Configuration

For Retrieval - The parked party and the device that attempts park retrieval associate with a geolocation and geolocation filter.

For Reversion - The parked party and device to which reversion happens associate with a geolocation and geolocation filter.

When

Logical partitioning handling takes place in the following circumstances:

- When a parked call exists and a device attempts a park retrieval, the Park retrieval feature gets invoked.
- When a parked call exists and the reversion timer expires, the Park reversion feature gets invoked.
- One party must be a PSTN participant.
- For Park retrieval, Cisco Unified Communications Manager uses geolocation identifier information of the parked device and of the device that performs park retrieval for policy checking.
- For Park reversion, Cisco Unified Communications Manager uses geolocation identifier information of the parked device and of the device to which call is redirected for policy checking.

When Not

Logical partitioning handling does not take place in the following circumstances:

- When the involved devices are VoIP phones (DevType=Interior), handling does not occur.
- When geolocation or geolocation filter does not associate with devices, no policy check occurs.

Deny Handling

Logical partitioning handles a denied retrieval/reversion as follows:

- For retrieval, Cannot Retrieve Parked Call message gets sent to the VoIP phone.
- Cisco Unified Communications Manager sends reorder tone to the phone that is attempting retrieval.
    - Q.850-compliant devices (phone that is running SCCP, H323, or MGCP device) get cleared by using cause code=63 “Service or option not available.”
    - Phone that is running SIP or SIP trunk gets cleared by using SIP status code=503 “Service unavailable.”
- For reversion, the parked call gets cleared with reorder tone.
- The Number of Park Retrieval Failures perfmon counter gets incremented (for both Call Park and Directed Call Park retrievals that get denied).

Cisco Extension Mobility

This section describes the interaction of logical partitioning with the Cisco Extension Mobility feature.

Operation

A user logs on to a VoIP phone by using Cisco Extension Mobility within the same Cisco Unified Communications Manager cluster. The incoming or outgoing calls from the phone get logical partitioning policy checked.

Configuration

The VoIP phone that is logged on to Cisco Extension Mobility and the PSTN access device both associate with a geolocation and geolocation filter.

When

Logical partitioning handling takes place in the following circumstances:

- A user logs on, by using Cisco Extension Mobility, to a device in a different geolocation as the device profile, and the user makes a PSTN call by using a gateway in the user home site, or the user receives an incoming PSTN call.
- Cisco Unified Communications Manager uses geolocation identifier information of the Cisco Extension Mobility logged-on device and the PSTN gateway device for policy checking.
- The configured logical partitioning policy returns to an outgoing Cisco Unified Communications Manager device layer, which takes action accordingly.

When Not

Logical partitioning handling does not take place in the following circumstances:

- Geolocation or geolocation filter does not associate with a VoIP phone that is logged on to Cisco Extension Mobility nor with the calling party nor called party device.
- The VoIP phone that is logged on to Cisco Extension Mobility calls or receives a call from a VoIP phone (DevType=Interior).

Deny Handling

Logical partitioning handles a denied call as follows:

- If the VoIP phone that is logged in to Cisco Extension Mobility places a PSTN call that should be denied per logical partitioning, the call gets rejected with a reorder tone.
- If the VoIP phone that is logged in to Cisco Extension Mobility receives a PSTN call that should be denied per logical partitioning, the call gets rejected with a reorder tone.

Cisco Unified Mobility

This section describes the interaction of logical partitioning with the Cisco Unified Mobility feature. These interactions apply to calls that involve Cisco Unified Mobility or Mobile Voice Access.

Operation

Logical partitioning interacts with Cisco Unified Mobility as follows:

- Single-Number-Reach (SNR) Call - The SNR call gets logical partitioning policy checked between a calling device and a PSTN gateway that connects the mobile device.
- Cell Pickup - The Cell Pickup operation from a desktop phone attempts to join the already connected call with a PSTN gateway that connects the remote destination mobile device. The logical partitioning policy gets checked before joining the call by using the geolocation identifiers for the involved devices.
- Mobile Voice Access - The logical partitioning policy gets checked between the geolocation identifier of the incoming gateway and the geolocation identifier of the called party device.

Configuration

The involved devices and the PSTN access gateway must associate with a geolocation and geolocation filter.

When

Logical partitioning handling takes place in the following circumstances:

- Single-Number-Reach (SNR) Call

  Cisco Unified Mobility gets configured for an enterprise extension, and a call is received for SNR from a VoIP phone or another PSTN gateway.

  Cisco Unified Communications Manager uses the geolocation identifier information that associates with calling and called Cisco Unified Communications Manager device to perform logical partitioning policy checking.

  The configured logical partitioning policy returns to the called Cisco Unified Communications Manager device layer, which takes action accordingly.

- Cell Pickup

Cisco Unified Mobility gets configured for an enterprise extension, and a call is active between a VoIP phone (SNR) and another VoIP phone or a PSTN gateway (termed the connected party).

The VoIP phone (SNR) performs Cell Pickup to Mobile, which tries to join the connected party with the PSTN gateway that was used to reach the mobile phone.

Cisco Unified Communications Manager uses the geolocation identifier information that associates with the PSTN gateway and the connected party for performing logical partitioning policy checking.

The configured logical partitioning policy decides whether the Cell Pickup operation succeeds or fails.

- Mobile Voice Access

  Cisco Unified Mobility gets configured for an enterprise extension, and a mobile phone calls from a PSTN gateway to an enterprise VoIP phone.

  Cisco Unified Communications Manager uses the geolocation identifier information that associates with the calling PSTN gateway and called VoIP phone to perform logical partitioning policy checking.

  The configured logical partitioning policy returns to the called Cisco Unified Communications Manager device layer, which takes action accordingly.

When Not

Logical partitioning handling does not take place in the following circumstances:

- Geolocation or geolocation filter does not associate with the involved devices.
- No logical partitioning support exists when a dual-mode phone is used.

Deny Handling

Logical partitioning handles a denied call as follows:

- For SNR and Mobile Voice Access, the call is cleared or rejected with a reorder tone.
- For cell pickup, the original call between connected party and VoIP phone (SNR) gets restored, and the Cannot Send Call to Mobile message displays on the VoIP phone.

Shared Line

This section describes the interaction of logical partitioning with the Shared Line feature.

Operation

The call to or from a shared line uses the same processing for logical partitioning checks as a basic call.

The shared-line device on Cisco Unified Communications Manager performs logical partitioning policy checks for displaying remote-in-use (RIU) information. The policy gets checked between the geolocation identifier for the connected party and the shared-line device that shows RIU information.

Configuration

The shared-line devices and the PSTN access device (a VoIP gateway) associate with a geolocation and geolocation filter.

When

Logical partitioning handling takes place in the following circumstances for a basic call:

- A shared line exists for the VoIP phones that span different geolocations, and one of the VoIP phones makes or receives a PSTN call through its local PSTN gateway.
- For completing the call from a shared line to a PSTN gateway, Cisco Unified Communications Manager uses the geolocation identifier information that associates with the calling shared-line phone and with the called PSTN gateway to perform logical partitioning policy checking.
- For completing the call from a PSTN gateway to a shared line, Cisco Unified Communications Manager uses the geolocation identifier information that associates with the calling PSTN gateway and with each of the called shared-line phones to perform logical partitioning policy checking.
- The configured logical partitioning policy gets returned to the called Cisco Unified Communications Manager device layer, which takes action accordingly.
- For determining whether to display the remote-in-use (RIU) information, Cisco Unified Communications Manager uses the geolocation identifier information of each device that associates with the shared line and that of the connected party (calling or called) to perform logical partitioning policy checking.

When Not

Logical partitioning handling does not take place in the following circumstances:

- When both the caller and the callee devices are VoIP phones (DevType=Interior), no handling occurs.
- When geolocation or geolocation filter does not associate with any device, no handling occurs.

Deny Handling

Logical partitioning handles a denied call as follows:

- Cisco Unified Communications Manager drops the call (or does not extend the call) to the called shared-line devices that are in unauthorized geolocations for the calling device.
- The call instance information does not display on the shared-line device in the remote-in-use state.

Barge cBarge and Remote Resume

This section describes the interaction of logical partitioning with the Barge, cBarge, and Remote Resume features.

Operation

The Barge, cBarge, or Remote-Resume operations on a shared line depend on the availability of call instance information in the remote-in-use (RIU) state.

The same logical partitioning policy checks that apply to shared-line interactions determine the availability of RIU information.

For logical partitioning deny cases, the RIU call instance gets withdrawn on a restricted shared line.

Configuration

The shared-line devices and the PSTN access device associate with a geolocation and geolocation filter.

When

Logical partitioning handling takes place in the following circumstances:

- A shared line exists for the VoIP phones that span different geolocations and one VoIP phone makes or receives a PSTN call through its local PSTN gateway.
- The display of remote-in-use (RIU) information gets handled as in the shared-line call scenario.
- During Hold for an active call by a shared-line device, no Remote Resume button is available.
- Because Barge and cBarge buttons are not available, these scenarios remain impossible.

When Not

Logical partitioning handling does not take place in the following circumstances:

- When both the caller and the callee devices are VoIP phones (DevType=Interior), logical partitioning policy checks get ignored.
- When geolocation or geolocation filter does not associate with any device, no handling occurs.
- When the connected party is a conference bridge due to an active feature, such as Conference or Meet-Me, and an active shared-line device associates with a geolocation that is allowed for all the devices in the conference, the remote-in-use shared-line device shows call instance information. In this case, the remote-in-use phone can always perform the cBarge/Barge feature even if a disallowed participant participates in the conference. For the participants in cBarge/Barge, no logical partitioning policy checking exists, and you cannot prevent logical-partitioning-denied scenarios.

Deny Handling

Logical partitioning handles a denied call as follows:

- The call instance information does not display.

Route Lists and Hunt Pilots

This section describes the interaction of logical partitioning with route lists and hunt pilots.

Operation

For route lists, the call from a device to gateways or MGCP ports that belong to route lists and route groups gets checked for logical partitioning policy by using the geolocation identifier of the involved calling party and called party devices as a basis.

For hunt pilots, the call from a PSTN device to a line device that belongs to a hunt list or hunt group gets checked for logical partitioning policy by using the geolocation identifier of the involved calling party and called party devices as a basis.

Configuration

The calling party and called party devices associate with a geolocation and geolocation filter.

When

Logical partitioning handling takes place in the following circumstances:

- A basic call takes place from a VoIP phone or a PSTN gateway through a route list to a PSTN gateway.
- A basic call takes place from a PSTN gateway through a hunt list to a set of VoIP phones.
- Cisco Unified Communications Manager uses the geolocation identifier information that associates with the incoming and outgoing Cisco Unified Communications Manager devices to perform logical partitioning policy checking.
- The configured logical partitioning policy returns to an outgoing Cisco Unified Communications Manager device layer, which takes action accordingly.

When Not

Logical partitioning handling does not take place in the following circumstances:

- When both the calling party and called party devices specify VoIP phones (DevType=Interior), handling does not occur.
- All devices must associate with both a geolocation and geolocation filter. If any device does not associate with both geolocation and geolocation filter, handling does not occur.

Deny Handling

Logical partitioning handles a denied call as follows:

- The call gets cleared or rejected with a reorder tone from Cisco Unified Communications Manager.

CTI Handling

This section describes the CTI interaction of logical partitioning with all features that perform Join or Redirects.

Operation

All the operations involving calls, joins, or redirects to a PSTN gateway get logical partitioning policy checked, and a CTI error gets generated for logical partitioning failures in the following instances:

- Basic call
- Transfer
- Conference
- Park retrieval and similar functions

Configuration

The involved devices associate with a geolocation and geolocation filter.

When

Logical partitioning handling takes place in the following circumstances:

- One of the devices specifies a PSTN participant.
- The logical partitioning policy gets checked in the context of an operation.

When Not

Logical partitioning handling does not take place in the following circumstances:

- When a geolocation or geolocation filter does not associate with any device, handling does not occur.
- When all the involved devices specify VoIP phones (DevType=Interior), handling does not occur.

Deny Handling

Logical partitioning handles a denied call by generating an operation-based CTI cause code as follows:

- Basic call - CTICCMSIP503SERVICENOTAVAILABL.
- Redirection - CTIERR_REDIRECT_CALL_PARTITIONING_POLICY.
- Join, Transfer, Conference, and others. - CTIERR_FEATURE_NOT_AVAILABLE.

Limitations

The following limitations apply to logical partitioning:

- SIP trunk User Agent Server (UAS) location conveyance in UPDATE

  The UAS uses UPDATE request to communicate geolocation of the called party to the User Agent Client (UAC). This normally happens after 180 Ringing.

  The logical partitioning policy checks in logical partitioning-aware cluster that receives this geolocation may CANCEL the call if policy gets denied. A convenient end user experience may not occur.

- The logical partitioning checks do not get supported for participants across conferences in conference chaining.

  For example, meet-me and ad hoc chained conferences can have participants that are logical partitioning denied.

- Limitation with QSIG intercluster trunk (ICT)

  Be aware that the ICT with Q.SIG protocol is not allowed to communicate geolocation info for the caller or callee device. The ICT configuration for “Send Geolocation Information” gets disabled when the Q.SIG tunneled protocol gets selected.

- Shared Line Active Call Info

  For logical partitioning restricted scenario, the shared line drops the active call information for the duration of the call, even if some feature moves the shared-line call to allowed category.

- cBarge/Barge

  Barge/cBarge does not occur because it gets prevented by not allowing shared lines to attempt these features based on logical partitioning deny policy with the connected party (the call instance gets dropped).

  However, when the connected party is a conference bridge due to an active feature, such as Conference or Meet-Me, and an active shared-line device associates with a geolocation that is allowed for all the devices in the conference, the remote-in-use shared-line device shows call instance information. In this case, the remote-in-use phone can always perform the cBarge/Barge feature even if a disallowed participant participates in the conference. For the participants in cBarge/Barge, no logical partitioning policy checking exists, and you cannot prevent logical-partitioning-denied scenarios.

- Cisco Unified Communications Manager does not communicate geolocation info to H.323 or MGCP gateway.

  Communication to a SIP gateway can get disabled from a SIP trunk check box.

- Cisco Unified Communications Manager does not communicate geolocation information over a H.225 gatekeeper-controlled trunk.

  Scenario: Cisco Unified Communications Manager 1 remains logical partitioning enabled, but Cisco Unified Communications Manager 2 stays logical partitioning disabled.

  Phone A on CCM1 calls Phone B on CCM2 (using ICT or SIP trunk).

  Phone B presses conference and invites PSTN to conference.

  Limitation: The conference gets established.

  After phone B goes on hook, the call between phone A and the PSTN on Cisco Unified Communications Manager 2 gets cleared with a reorder tone.

- Mobility Cell Pickup: Logical partitioning Deny handling takes place after call gets answered on the mobile phone.

  The logical partitioning policy check does not happen before the call gets placed to the mobile phone (as it happens for a basic SNR call). The current design checks logical partitioning policy only after SsJoinReq processing, which takes place after the mobile phone answers the call.

- Cisco Extension Mobility logs in to a phone in a different geolocation

  Outgoing PSTN calls can occur when Local Route Groups are configured.

  Incoming PSTN calls do not get placed to the phone but receive a reorder tone.

- BLF SD or BLF Pickup Presence notifications do not get checked for logical partitioning policy.

  Currently, no logical partitioning infrastructure gets added for notifications.

  For forwarding failures, the RTMT Number of Forwarding Failures performance monitor counter does not increment. Instead, the Number of Basic Call Failures performance monitor counter increments.

- No reorder tone is provided on IOS H.323 and SIP gateways upon release of connected calls due to logical partitioning policies during supplementary features.

  Example

  Remote destination (RD) phone behind IOS SIP or H.323 gateway calls VoIP phone A.

  After authentication completes, RD phone makes a call to phone C, but the call gets denied due to logical partitioning restricted policy.

  Call gets cleared to RD phone with cause 63 (Service or option not available), but no reorder tone gets played to the RD phone.

Note

This cause code is common to all logical partitioning failure cases.

This behavior occurs due to a design limitation on the IOS gateway side, which does not play reorder tone after the CONNECT state. The only tones that play after the CONNECT state specify 17 (Busy) or 44 (No Circuit Available).

Similar limitations apply for Hook Flash, Onhook Transfer, and other supplementary features.

- No configuration exists for forwarding the call to voice mail for logical partitioning failures.
- No announcements occur for logical partitioning deny failures.
- Cisco Unified Communications Manager does not support the logical partitioning feature for calls that involve Cisco Unified MeetingPlace or Cisco Unified MeetingPlace Express.

Logical Partitioning Configuration

This section describes how to configure logical partitioning.

Tip

Before you configure logical partitioning, review the configuration summary task for this feature.

Related Topics

Configure Logical Partitioning, on page 795

Geolocation Configuration

Use the **System** > **Geolocation Configuration** menu option in Cisco Unified Communications Manager Administration to configure geolocations.

For details of geolocation configuration, see the Geolocation Configuration, on page 582.

Geolocation Filter Configuration

Use the **System** > **Geolocation Filter** menu option in Cisco Unified Communications Manager Administration to configure geolocation filters.

For details of geolocation filter configuration, see the Geolocation Filter Configuration, on page 588.

Logical Partitioning Policy Configuration

This section provides information to configure logical partitioning policies. Use the **Call Routing** > **Logical Partitioning Policy Configuration** menu option in Cisco Unified Communications Manager Administration to configure logical partitioning policies.

Find a Logical Partitioning Policy

Because you might have multiple logical partitioning policies in your network, Cisco Unified Communications Manager lets you search for logical partitioning policies on the basis of specified criteria. Follow these steps to search for a specific logical partitioning policy in the Cisco Unified Communications Manager database.

Note During your work in a browser session, Cisco Unified Communications Manager Administration retains your logical partitioning policy search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your logical partitioning policy search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Call Routing** > **Logical Partitioning Policy Configuration**.

The Find and List Policies window displays. Records from an active (prior) query may also display in the window.

Step 2 To filter or search records

a) From the first drop-down list box, choose a search parameter.
b) From the second drop-down list box, choose a search pattern.
c) Specify the appropriate search text, if applicable.

Note To add additional search criteria, click the **+** button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the **–** button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

Step 3 To find all records in the database, ensure the dialog box is empty, click **Find.**

All matching records display. You can change the number of items that display by choosing a different value from the Rows per Page drop-down list box.

Note You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking **Delete Selected**. You can delete all configurable records for this selection by clicking **Select All** and then clicking **Delete Selected**.

Step 4 From the list of records that display, click the link for the record that you want to view.

Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Configure a Logical Partitioning Policy

Perform the following procedure to add or update a logical partitioning policy.

Procedure

Step 1 Choose **Call Routing** > **Logical Partitioning Policy Configuration**.

The Find and List Policies window displays.

Step 2 Perform one of the following tasks:

a) To add a new logical partitioning policy, click **Add New**.

The Logical Partitioning Policy Configuration window displays.

b) To update a logical partitioning policy, locate a specific logical partitioning policy as described in the Find a Logical Partitioning Policy, on page 831.

Step 3 Enter the appropriate settings as described in Logical Partitioning Policy Configuration, on page 833.

Step 4 Click **Save.**

If you added a logical partitioning policy, the list box at the bottom of the window now includes the new logical partitioning policy.

Delete a Logical Partitioning Policy Record

Perform the following procedure to delete an existing logical partitioning policy record.

Procedure

Step 1 Choose **Call Routing** > **Logical Partitioning Policy Configuration**.

The Find and List Policies window displays.

Step 2 To locate a specific logical partitioning policy, enter search criteria and click **Find.**

A list of geolocation filter logical partitioning policies that match the search criteria displays.

Step 3 Perform one of the following actions:

a) Check the check boxes next to the logical partitioning policies that you want to delete and click **Delete Selected**.

b) Delete all logical partitioning policies in the window by clicking **Select All** and then clicking **Delete Selected**.

c) From the list, choose the name of the logical partitioning policy that you want to delete and click **Delete.**

A confirmation dialog displays.

Step 4 Click **OK.**

The specified logical partitioning policy and all pair policies for this record get deleted.

Delete a Logical Partitioning Policy Pair Configuration

In this case, select a logical partitioning policy record and display the configuration window of that record.

The policies are currently configured in pairs. For example,

GLP-1 Border GLP-2 Interior Allow

GLP-1 Border GLP-3 Interior Allow

If the second policy needs to be deleted, choose the second policy and select the Use Default Policy setting.

After you save, the corresponding pair of policies gets deleted from the matrix of policies.

Note that no change is made in the GLP-1 record.

Update a Logical Partitioning Policy Pair Configuration

In this case, select a logical partitioning policy record and display the configuration window of that record.

The policies are currently configured in pairs. For example,

GLP-1 Border GLP-2 Interior Allow

GLP-1 Border GLP-3 Interior Allow

If the second policy needs to be updated, choose the second policy and specify either Allow or Deny in the Policy setting.

After you save, the corresponding pair of policies gets updated from the matrix of policies.

Logical Partitioning Policy Configuration

Ensure logical partitioning policies are configured for the required interconnection behavior between the following entities:

- Between PSTN gateways and VoIP phones
- Between PSTN gateway and PSTN gateway
- Between an intercluster trunk (ICT) and a VoIP phone
- Between an ICT and a VoIP gateway

The System Default Policy enterprise parameter (Default value=DENY) represents the default policy when no configured policy is found.

In the Logical Partitioning Policy Configuration window (**Call Routing** > **Logical Partitioning Policy Configuration** menu option in Cisco Unified Communications Manager Administration), the administrator must create geolocation policy records from a subset of the fields that are configured for geolocations.

Configure logical partitioning policies between pairs of geolocation policy records and device types.

Ensure Allow and Deny policies are configured. See the Logical Partitioning Feature, on page 796 for configuration details.

See the Logical Partitioning Policies, on page 803 for more information about logical partitioning policies, including examples.

The following table describes the configuration settings that are used for configuring logical partitioning policies.

Table 92: Logical Partitioning Policy Configuration Settings

Field	Description
Logical Partitioning Policy Configuration	
Name	Enter a unique name (between 1 and 50 characters) for this logical partitioning policy. You may use all characters except quotes ("), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).
Description	Enter a description for this logical partitioning policy.
Country	From the drop-down list box, choose a country for this logical partitioning policy. You can leave the <None> value if you do not want to specify this field for this logical partitioning policy.
A1	From the drop-down list box, choose an A1 value for this logical partitioning policy. You can leave the <None> value if you do not want to specify this field for this logical partitioning policy.
A2	From the drop-down list box, choose an A2 value for this logical partitioning policy. You can leave the <None> value if you do not want to specify this field for this logical partitioning policy.
A3	From the drop-down list box, choose an A3 value for this logical partitioning policy. You can leave the <None> value if you do not want to specify this field for this logical partitioning policy.
A4	From the drop-down list box, choose an A4 value for this logical partitioning policy. You can leave the <None> value if you do not want to specify this field for this logical partitioning policy.
A5	From the drop-down list box, choose an A5 value for this logical partitioning policy. You can leave the <None> value if you do not want to specify this field for this logical partitioning policy.
A6	From the drop-down list box, choose an A6 value for this logical partitioning policy. You can leave the <None> value if you do not want to specify this field for this logical partitioning policy.
PRD	From the drop-down list box, choose a PRD value for this logical partitioning policy. You can leave the <None> value if you do not want to specify this field for this logical partitioning policy.

Field	Description
POD	From the drop-down list box, choose a POD value for this logical partitioning policy. You can leave the <None> value if you do not want to specify this field for this logical partitioning policy.
STS	From the drop-down list box, choose an STS value for this logical partitioning policy. You can leave the <None> value if you do not want to specify this field for this logical partitioning policy.
HNO	From the drop-down list box, choose an HNO value for this logical partitioning policy. You can leave the <None> value if you do not want to specify this field for this logical partitioning policy.
HNS	From the drop-down list box, choose an HNS value for this logical partitioning policy. You can leave the <None> value if you do not want to specify this field for this logical partitioning policy.
LMK	From the drop-down list box, choose an LMK value for this logical partitioning policy. You can leave the <None> value if you do not want to specify this field for this logical partitioning policy.
LOC	From the drop-down list box, choose a LOC value for this logical partitioning policy. You can leave the <None> value if you do not want to specify this field for this logical partitioning policy.
FLR	From the drop-down list box, choose a FLR value for this logical partitioning policy. You can leave the <None> value if you do not want to specify this field for this logical partitioning policy.
NAM	From the drop-down list box, choose an NAM value for this logical partitioning policy. You can leave the <None> value if you do not want to specify this field for this logical partitioning policy.
PC	From the drop-down list box, choose a PC value for this logical partitioning policy. You can leave the <None> value if you do not want to specify this field for this logical partitioning policy.
Configured Policies	

Field	Description
Device Type	After you configure a relationship between this logical partitioning policy and another (or the same) logical partitioning policy, a new row displays in this pane for the configured relationship. This column displays the device type of the current logical partitioning policy for this relationship. **Note** Only relationships that do not specify Use Default Policy display in this pane.
Geolocation Policy	After you configure a relationship between this logical partitioning policy and another (or the same) logical partitioning policy, a new row displays in this pane for the configured relationship. This column displays the other geolocation policy for this relationship. **Note** Only relationships that do not specify Use Default Policy display in this pane.
Other Device Type	After you configure a relationship between this logical partitioning policy and another (or the same) logical partitioning policy, a new row displays in this pane for the configured relationship. This column displays the device type of the other logical partitioning policy for this relationship. **Note** Only relationships that do not specify Use Default Policy display in this pane.
Policy	After you configure a relationship between this logical partitioning policy and another (or the same) logical partitioning policy, a new row displays in this pane for the configured relationship. This column displays the configured logical partitioning policy value for this relationship. **Note** Only relationships that do not specify Use Default Policy display in this pane.
Configure Relationship to Other Geolocation Policies	

Field	Description
Device Type	From the drop-down list box, choose one of the following values to configure the relationship of this logical partitioning policy to other geolocation policies: • Border - Choose this device type for devices that specify PSTN trunks, gateways, and MGCP ports. • Interior - Choose this device type for devices that specify VoIP phones or internal endpoints. **Note** See Logical Partitioning Feature, on page 796 for a listing of which Cisco Unified Communications Manager devices can be associated with each device type (border or interior).
Geolocation Policy	In this pane, choose the name of another geolocation policy to configure the relationship between this logical partitioning policy and that geolocation policy.
Other Device Type	From the drop-down list box, choose the device type of the other geolocation policy that you selected in the Geolocation Policy column. Choose one of the following values: • Border - Choose this device type for devices that specify PSTN trunks, gateways, and MGCP ports. • Interior - Choose this device type for devices that specify VoIP phones or internal endpoints. **Note** See Logical Partitioning Feature, on page 796 for a listing of which Cisco Unified Communications Manager devices can be associated with each device type (border or interior).

Field	Description
Policy	From the drop-down list box, choose the policy to apply between this logical partitioning policy and the geolocation policy that you selected in the Geolocation Policy column. Choose one of the following values: • Use Default Policy - Choose this value to apply the default policy that the Logical Partitioning Default Policy enterprise parameter specifies. • Allow - Choose this value to specify a policy of Allow between this logical partitioning policy and the other geolocation policy. • Deny - Choose this value to specify a policy of Deny between this logical partitioning policy and the other geolocation policy.

Logical Partitioning Configuration After Upgrade

During upgrade of Cisco Unified Communications Manager from a release that preceded Release 7.1(2), the following values get assigned for the entities that associate with logical partitioning configuration:

- Enable Logical Partitioning enterprise parameter specifies False.
- Logical Partitioning Default Policy enterprise parameter specifies Deny.
- Geolocation
  - No configured geolocation records exists in the geolocation table.
  - Default Geolocation enterprise parameter specifies Unspecified.
  - Device pools specify Geolocation value None.
  - Devices specify Geolocation value Default.
- Geolocation filter
  - No configured geolocation filter records exist in geolocation filter table.
  - Logical Partitioning Default Filter enterprise parameter specifies None.
  - Device pools specify Geolocation Filter value None.
  - Devices specify Geolocation Filter value None.
- Logical partitioning policy
  - No configured GeolocationPolicy records and policies exist in geolocationpolicy and geolocationpolicymatrix tables.

Troubleshooting Logical Partitioning

For information on troubleshooting logical partitioning, see the Troubleshooting Guide for Cisco Unified Communications Manager.

CHAPTER 37

Malicious Call Identification

This chapter provides information about the Malicious Call Identification feature.

Configure Malicious Call ID

The malicious call identification (MCID) feature allows a user to report a call of a malicious nature by requesting that Cisco Unified Communications Manager identify and register the source of an incoming call in the network.

Malicious call identification (MCID), an internetwork service, allows users to initiate a sequence of events when they receive calls with a malicious intent. The user who receives a disturbing call can invoke the MCID feature by using a softkey or feature button while the user is connected to the call. The MCID service immediately flags the call as a malicious call with an alarm notification to the Cisco Unified Communications Manager administrator. The MCID service flags the call detail record (CDR) with the MCID notice and sends a notification to the off-net PSTN that a malicious call is in progress.

Perform the following steps to configure malicious call identification. For additional information on malicious call identification, see the Malicious Call Identification Feature, on page 842 and the Malicious Call Identification, on page 841.

Procedure

Step 1 Configure the CDR service parameter.

Step 2 Configure the alarm.

Step 3 If users will access MCID by using a softkey, configure a softkey template with the Toggle Malicious Call Trace (MCID) softkey.

Note The Cisco Unified IP Phones 8900 and 9900 series support MCID with feature button only.

Step 4 Assign the MCID softkey template to an IP phone.

Step 5 If users will access MCID by using a feature button, configure a phone button template with the Malicious Call Identification feature.

Step 6 Assign the MCID phone button template to an IP phone.

Step 7 Notify users that the Malicious Call Identification feature is available.

Related Topics

Set Malicious Call ID Service Parameter, on page 846
Configure Malicious Call ID Alarms, on page 846
Configure a Softkey Template for Malicious Call Identification, on page 847
Associate a Softkey Template with a Phone, on page 848
Configure Malicious Call ID Phone Button Template, on page 848

Malicious Call Identification Feature

The Malicious Call Identification (MCID) supplementary service allows you to report a call of a malicious nature by requesting that Cisco Unified Communications Manager identify and register the source of an incoming call in the network.

Malicious Call Identification (MCID), an internetwork service, allows users to initiate a sequence of events when they receive calls with a malicious intent. The user who receives a disturbing call can invoke the MCID feature by using a softkey or feature code while the user is connected to the call. The MCID service immediately flags the call as a malicious call with an alarm notification to the Cisco Unified Communications Manager administrator. The MCID service flags the call detail record (CDR) with the MCID notice and sends a notification to the off-net PSTN that a malicious call is in progress.

The system supports the MCID service, which is an ISDN PRI service, when it is using PRI connections to the PSTN. The MCID service includes two components:

- MCID-O - An originating component that invokes the feature upon the user request and sends the invocation request to the connected network.
- MCID-T - A terminating component that receives the invocation request from the connected network and responds with a success or failure message that indicates whether the service can be performed.

Note Cisco Unified Communications Manager supports only the originating component.

Use the Malicious Call ID Feature with CUCM

The MCID feature provides a useful method for tracking troublesome or threatening calls. When a user receives this type of call, the Cisco Unified Communications Manager system administrator can assign a new softkey template that adds the Malicious Call softkey to the user phone. For POTS phones that are connected to a SCCP gateway, users can use a hookflash and enter a feature code of *39 to invoke the MCID feature.

When the MCID feature is used, the following actions take place:

1. The user receives a threatening call and presses Malicious Call (or enters the feature code *39).

2. Cisco Unified Communications Manager sends the user a confirmation tone if the device can play a tone - and a text message on a phone that has a display - to acknowledge receiving the MCID notification.
3. Cisco Unified Communications Manager updates the 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 has 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.

System Requirements for Malicious Call ID

Malicious Call ID service requires Cisco Unified Communications Manager 5.0 or later to operate.

The following gateways and connections support MCID service:

- PRI gateways that use the MGCP PRI backhaul interface for T1 (NI2) and E1 (ETSI) connections
- H.323 trunks and gateways

The Cisco ATA 186 analog phone ports support MCID by using the feature code (*39).

To determine which IP Phones support the MCID feature, see the Determine Device Support for Malicious Call Identification, on page 843.

Determine Device Support for Malicious Call Identification

Use the Cisco Unified Reporting application to generate a complete list of IP Phones that support MCID. To do so, follow these steps:

Procedure

Step 1 Start Cisco Unified Reporting by using any of the methods that follow. The system uses the Cisco Tomcat service to authenticate users before allowing access to the web application. You can access the application

- by choosing **Cisco Unified Reporting** in the **Navigation** menu in Cisco Unified Communications Manager Administration and clicking **Go.**
- by choosing **File** > **Cisco Unified Reporting** at the Cisco Unified **Real Time Monitoring Tool** (RTMT) menu.
- by entering `https://<server name or IP address>:8443/cucreports/` and then entering your authorized username and password.

Step 2 Click **System Reports** in the navigation bar.

Step 3 In the list of reports that displays in the left column, click the **Unified CM Phone Feature List** option.

Step 4 Click the **Generate a new report** link to generate a new report, or click the **Unified CM Phone Feature List** link if a report already exists.

Step 5 To generate a report of all IP Phones that support MCID, choose these settings from the respective drop-down list boxes and click the **Submit** button:

Product: All

Feature: Malicious Call Identification

The List Features pane displays a list of all devices that support the MCID feature. You can click on the Up and Down arrows next to the column headers (Product or Protocol) to sort the list.

For additional information about the Cisco Unified Reporting application, see the *Cisco Unified Reporting Administration Guide*.

Interactions and Restrictions

This section describes the interactions and restrictions for Malicious Call Identification.

Interactions

This section describes how Malicious Call Identification interacts with Cisco Unified Communications Manager applications and call processing features.

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.

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 featured 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

See the *Cisco Unified Serviceability Administration Guide* for more information about alarms and traces.

Restrictions

The following restrictions apply to Malicious Call Identification:

- 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.
- MCID does not work across intercluster trunks because Cisco Unified Communications Manager does not support the MCID-T function.
- Cisco MGCP FXS gateways do not support MCID. No mechanism exists for accepting the hookflash and collecting the feature code in MGCP.
- MCID does not work over QSIG trunks because MCID is not a QSIG standard.
- The Cisco VG248 Analog Phone Gateway does not support MCID.
- Skinny Client Control Protocol (SCCP) IP phones use a softkey to invoke the MCID feature.
- MCID does not support SIP trunks.

See the Configure Malicious Call ID, on page 846 for configuration details.

Install Malicious Call ID

Malicious Call Identification, which is a system feature, comes standard with Cisco Unified Communications Manager software. MCID does not require special installation or activation.

Configure Malicious Call ID

This section provides information to configure Malicious Call ID.

Tip Before you configure Malicious Call Identification, review the configuration summary task for this feature.

Related Topics

Configure Malicious Call ID, on page 841

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 846

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 846

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 846

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 Phone

To provide the MCID feature to users, you must assign the MCID softkey template to their IP phone.

Note For users whose phones do not have a softkeys, provide them the feature code information and instructions on how to invoke the feature.

Before you begin

Configure a Softkey Template for Malicious Call Identification, on page 847

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.

Remove the Malicious Call Identification Feature from a User

To remove the MCID feature from a user, you must assign another softkey template to their IP phone.

Procedure

Step 1 From **Cisco Unified CM Administration**, choose **Device** > **Phone**.
The **Find and List Phones** window displays.

Step 2 To locate the phone configuration, enter phone search information and click **Find**.

Step 3 Choose the phone that you want to update.

Step 4 Locate the **Softkey Template** field and choose a softkey template without MCID from the drop-down list.

Step 5 To save the changes in the database, click **Save**.

Step 6 To activate the changes on the phone, click **Reset**.

Step 7 Notify the user that the Malicious Call Identification feature is no longer available.

Configure Malicious Call ID Phone Button Template

Before you begin

Configure Malicious Call ID Alarms, on page 846

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 848

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 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 38

Monitoring and Recording

This chapter provides information about Silent Call Monitoring and Call Recording.

Call centers need to be able to guarantee the quality of customer service that an agent in a call center provides. To protect themselves from legal liability, call centers need to be able to archive agent-customer conversations.

The Silent Call Monitoring feature allows a supervisor to eavesdrop on a conversation between an agent and a customer; neither the agent nor the customer can hear the supervisor voice.

The Call Recording feature allows system administrators or authorized personnel to archive conversations between the agent and the customer.

Cisco Unified Communications Manager supports Silent Call Monitoring ionly within a single cluster. Call Recording is supported within multi-cluster environments.

Silent call monitoring specifies one of the three call monitoring modes.(The other modes specify whisper call monitoring and active call monitoring.) In whisper monitoring mode, the supervisor can listen to the conversation between an agent and a customer and can talk to the agent without making the customer aware of the presence of the supervisor. In active monitoring mode, the supervisor can participate fully in the conversation between the agent and the customer.

The Silent Monitoring and Call Recording features specify generic features in Cisco Unified Communications Manager. Cisco makes these features available to any deployment or installation where monitoring- and recording-enabled applications are available. Descriptions in this document use terms such as supervisor, agent, and customer to see the parties that participate in call monitoring and recording sessions.

Silent Monitoring

Customers need to guarantee the quality of customer service provided by their employees who service their customers, such as call center agents. Customers also need to meet compliance, guidelines and protect themselves from legal liability. These requirements are satisfied by monitoring and recording agent-customer conversations.

The silent call monitoring feature allows a supervisor to eavesdrop on any conversation; neither of the call participants can hear the supervisor voice.

Terminology

This document uses the following terms to discuss call monitoring:

Agent

The call party that is monitored.

Customer

Any call participant other than the agent or the supervisor.

Local stream

The media stream from agent to customer.

Remote stream

The media stream from customer to agent.

Supervisor

The person who is silently monitoring the call.

Supervisor desktop application

A silent monitoring-enabled application that is used to invoke a monitoring session.

Silent monitoring

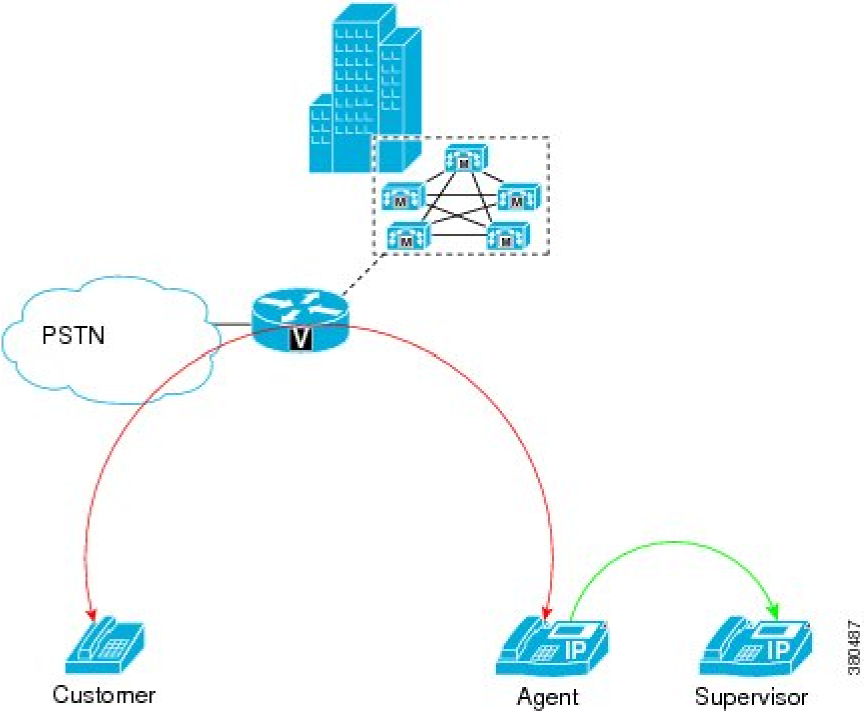
The feature which allows a monitoring party (a supervisor) to listen to a conversation between a near-end party (an agent) and a far-end party (a customer); neither the agent nor the customer hears the monitoring party voice.

Introduction

With silent call monitoring, the supervisor can listen in on any call for quality control and performance evaluation. By default, the agent is not aware of the monitoring session. In IP phone-based silent call monitoring, the monitoring stream comprises a mix of the customer voice and the agent voice. Only a CTI application can trigger a silent monitoring session.

Figure 75: Silent Call Monitoring Session

The following figure shows a typical monitoring session.

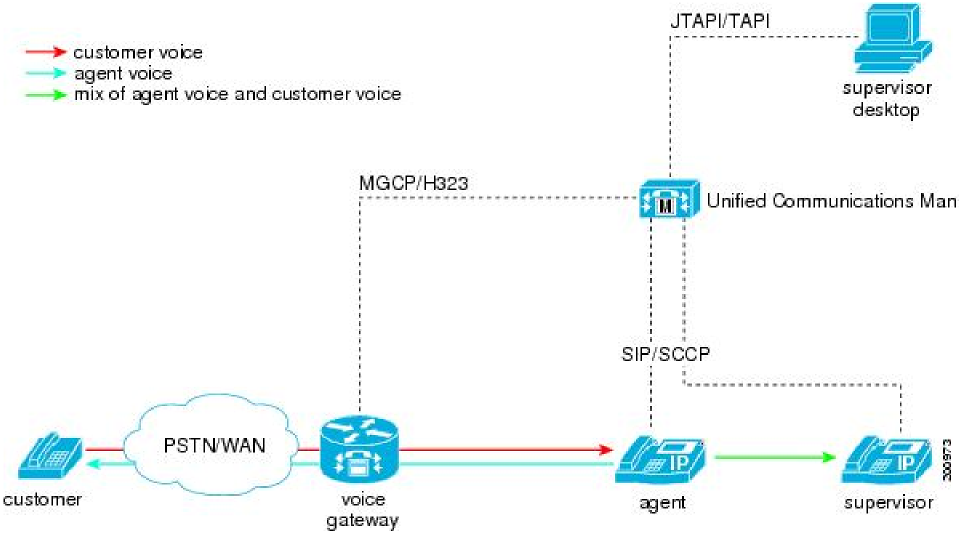


Architecture

Cisco Unified Communications Manager uses an IP phone-based architecture to provide call monitoring whereby the agent phone mixes the agent voice with the customer voice and sends a single, combined, or mixed stream of both voices to the supervisor phone.

Figure 76: IP Phone-Based Architecture for Monitoring

The following figure illustrates the IP phone-based architecture for monitoring. In the figure, the blue lines indicate the agent voice stream, the red lines indicate the customer voice stream, and the green line indicates the mix of customer and agent voice streams that gets sent to the supervisor.



Applications can initiate monitoring 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 the silent monitoring feature.

Monitoring exhibits the following characteristics:

- Silent monitoring is call based; the supervisor selects a specific call on a line appearance of an agent phone to be monitored.
- The start-monitoring request from the application triggers the supervisor phone to go off hook automatically to make a special monitoring call to the agent.
- The agent phone automatically answers the monitoring call. The monitoring call is not presented to the agent.

The following requirements apply:

- The CTI application user needs to be a member of the Standard CTI Allow Call Monitoring user group.
- The agent device needs to be in the CTI application user's controlled device list.

For a monitoring call, the supervisor phone displays “From Monitoring [agent username/DN]”.

One-Way Media

A monitoring call comprises one-way media from an agent phone to a supervisor phone.

Monitoring calls go through normal call admission control.

Network Address Translation (NAT) separating agent and supervisor or customer remains transparent within the limitations of Cisco Unified Communications Manager.

Firewall Considerations

Firewall software needs to know the destination IP address and destination port as well as the source IP address to allow the RTP streams.

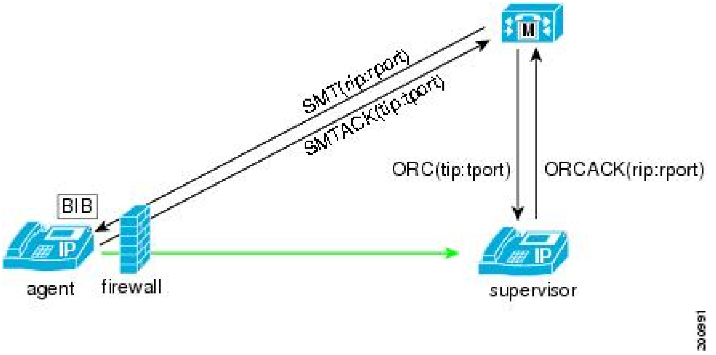
Be aware that SCCP messages for media are not symmetric; SIP is acceptable.

The SCCP version 12 enhancement for one-way media provides the following additions:

- New StartMediaTransmissionAck (SMTACK) message with transmission IP and port
- OpenReceiveChannel (ORC) with additional transmission IP and port

Figure 77: One-Way Media and Firewall

The following figure illustrates one-way media and a firewall.



Codec Selection

The agent phone and the supervisor phone negotiate the codec for the monitoring call using Cisco Unified Communications Manager region settings.

Call Preservation

If the agent call that is being monitored goes to call preservation, Cisco Unified Communications Manager puts the monitoring call into call preservation mode.

The agent call is not affected if the monitoring call goes to call preservation mode.

Notification Tones

In certain jurisdictions, a notification tone must be played to either the agent, customer, or both indicating the call is being monitored.

Use the following service parameters to set the default notification-tone options:

- Play Monitoring Notification Tone To Observed Target (agent)
- Play Monitoring Notification Tone To Observed Connected Parties (customer)

CTI applications can specify the notification tone option in the monitoring request.

Play Tone Behavior

The following table specifies the behavior of tones during a monitoring session.

Table 93: Play Tone Behavior

Play To	Agent Hears	Customer Hears	Supervisor Hears
None	Nothing	Nothing	Nothing
Agent	Tone	Nothing	Nothing
Customer	Nothing	Tone	Nothing
Both	Tone	Tone	Nothing

Silent Monitoring Usage Scenarios

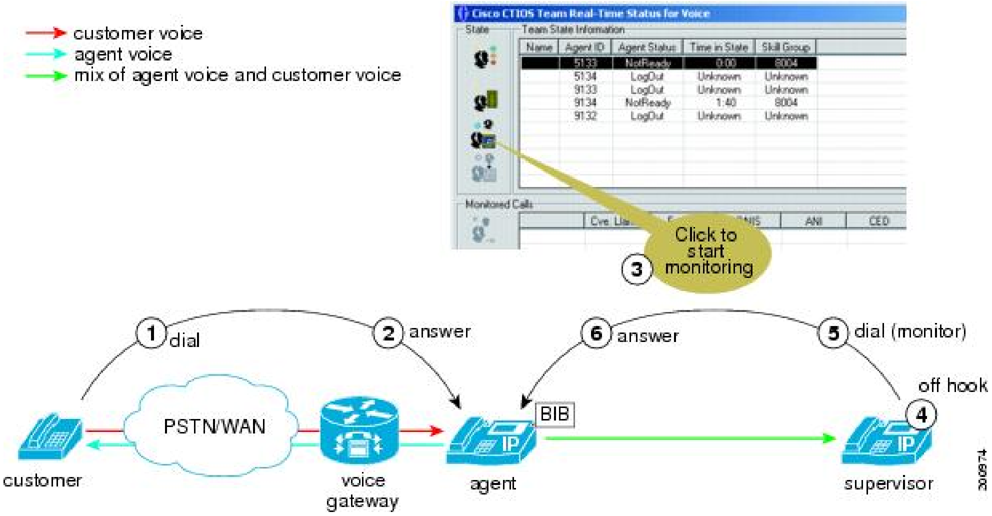
The following section provides usage scenarios for Call Monitoring.

Invocation of a Silent Monitoring Session

A supervisor can initiate a silent monitoring session by using a desktop application after the agent answers a call.

The following figure illustrates a silent monitoring session.

Figure 78: Silent Monitoring Session



Cisco CTIOS Team Real-Time Status for Voice

Team State Information

Name	Agent ID	Agent Status	Time in State	Skill Group
	5133	NotReady	0:00	8004
	5134	LogOut	Unknown	Unknown
	9133	LogOut	Unknown	Unknown
	9134	NotReady	1:40	8004
	9132	LogOut	Unknown	Unknown

When the supervisor initiates a monitoring session, the following steps take place:

1. The customer calls into the call center. The call gets routed to the agent.
2. The agent answers the call. A two-way media stream is set up between the agent IP phone and the customer.
3. The supervisor selects the agent from the desktop application, and then clicks Monitoring.
4. The supervisor phone automatically goes off hook.
5. The supervisor phone makes a monitoring call to the agent.

6. The built-in bridge (BIB) of the agent phone automatically accepts the monitoring call. The agent phone starts to mix media of the agent voice and the customer voice and sends the mix to the supervisor phone.

The supervisor can transfer the monitoring call anywhere after the monitoring call is initiated.

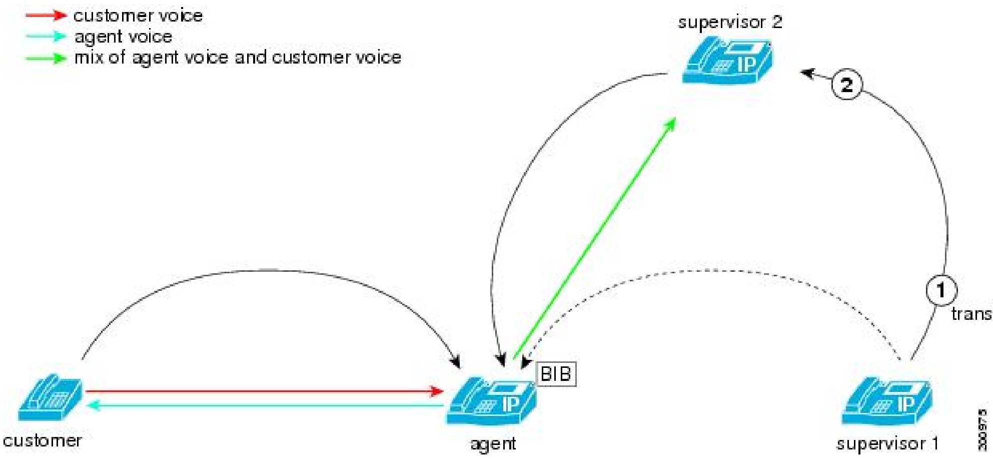
The supervisor can stop monitoring the call anytime after the call starts, either through the application or simply by hanging up.

The supervisor can put the monitoring call on hold (no MOH gets inserted) and resume the monitoring call from the same or a different device.

Supervisor Transfers the Monitoring Call

The following figure illustrates the supervisor transfer of a monitoring call.

Figure 79: Supervisor Transfers the Monitoring Call



During a monitoring call, the supervisor transfers the monitoring call, and the following steps take place:

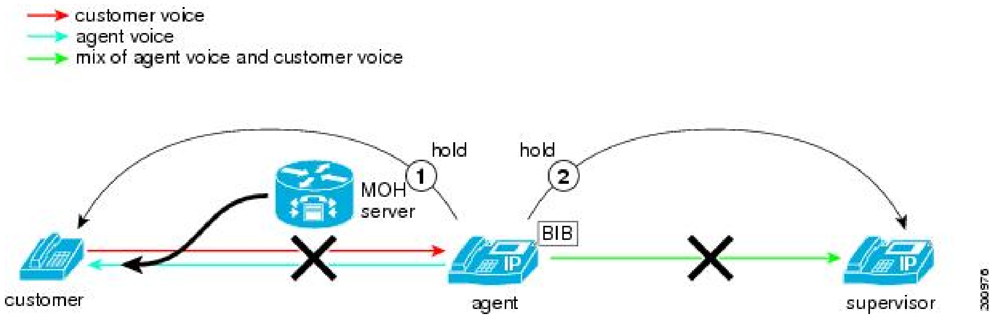
1. Supervisor 1 presses the Transfer softkey and dials the phone number of supervisor 2.
2. Supervisor 2 answers the call.
3. Supervisor 1 completes the transfer by pressing the Transfer softkey again.
4. The monitoring call transfers to supervisor 2. Supervisor 2 starts to receive the mix of the agent voice and the customer voice.

Agent Cannot Control a Monitoring Call

The agent does not have direct control over the monitoring call; however, the agent action on the primary call causes a corresponding action for the monitoring call.

The following figure illustrates the scenario where the agent puts the customer on hold while the supervisor is monitoring the agent.

Figure 80: Agent Does Not Control the Monitoring Call



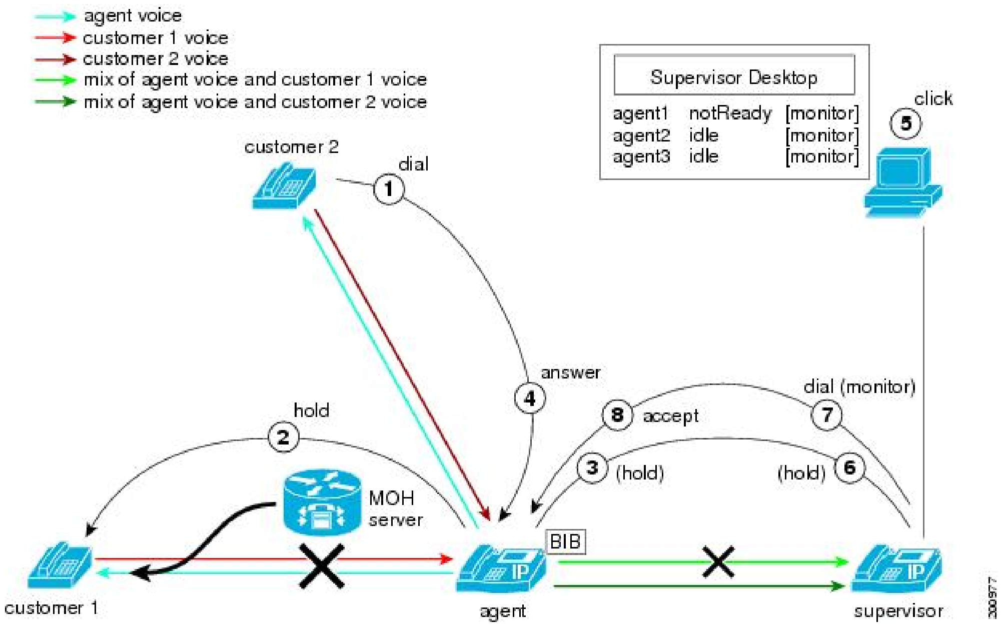
While an agent is being monitored, the agent puts the customer on hold, and the following steps take place:

1. The agent puts the customer on hold. MOH gets inserted and played to the customer.
2. Cisco Unified Communications Manager automatically puts the supervisor on hold. No MOH gets inserted to the supervisor.

Multiple Monitoring Sessions

The following figure illustrates the call flows during multiple monitoring sessions.

Figure 81: Multiple Monitoring Sessions



agent1	notReady	[monitor]
agent2	idle	[monitor]
agent3	idle	[monitor]

During multiple monitoring sessions, the following steps take place:

1. Customer 2 calls the agent while the agent is in a call with customer 1 and supervisor is monitoring the agent call with customer 1.
2. The agent puts customer 1 on hold; MOH gets inserted to customer 1.
3. Cisco Unified Communications Manager puts the supervisor on hold. No MOH gets inserted to the supervisor.

4. The agent answers the call from customer 2.
5. The supervisor initiates a second monitoring request for the agent call with customer 2.
6. The supervisor phone goes off hook and makes the second monitoring call to the agent.
7. The agent IP phone (BIB of the agent IP phone) automatically accepts the monitoring call. The mix of agent voice and customer 2 voice gets sent to the supervisor phone.

Barging or Monitoring an Agent Call

If the agent call is being monitored, the barge-in call from a shared line fails.

If the agent call has already been barged, the monitoring request gets rejected with a No Resource Available error.

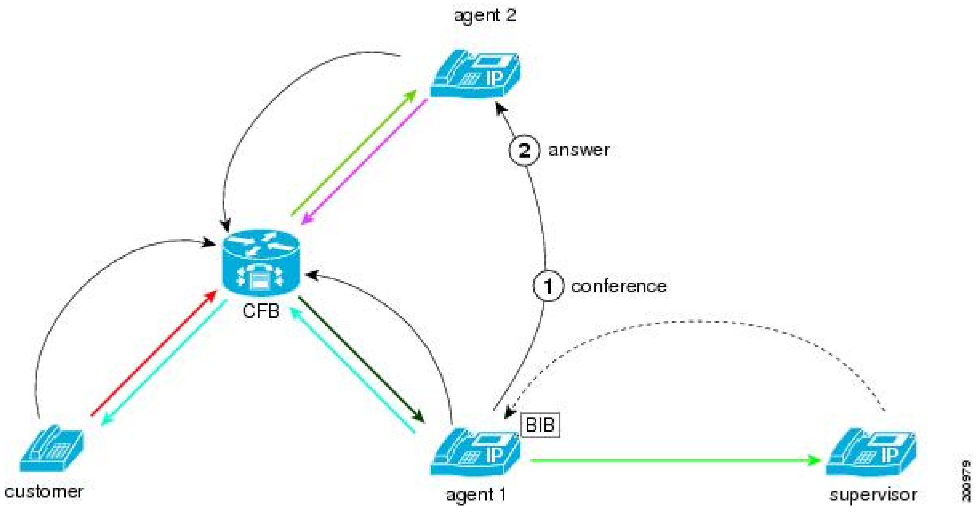
Monitoring an Agent in a Conference

An agent in a call center sometime needs to bring in another party into the conversation with the customer.

The following figure illustrates a case where agent 1 starts an ad hoc conference to include agent 2 in the conversation with the customer. The supervisor for agent 1 monitors the original call with the customer.

During the setting-up process, the media of the monitoring call briefly disconnect. After the conference completes, the supervisor can hear all the parties that are included in the conference.

Figure 82: Monitoring an Agent in a Conference



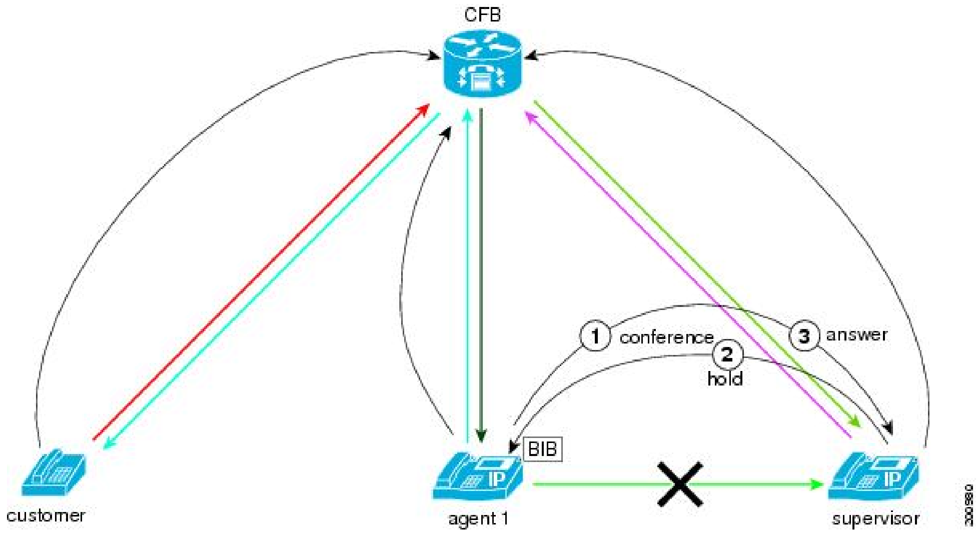
Agent Conferences in the Supervisor

The agent may create a conference with the supervisor while that supervisor is monitoring that agent.

The supervisor must put the monitoring call on hold before joining the conference.

This figure shows the final connection when the supervisor puts the monitoring call on hold and joins the conference. The monitoring session remains in the Hold state while the supervisor participates in the conference. After the supervisor leaves the conference, the supervisor can then resume the monitoring session.

Figure 83: Agent Conferences in the Supervisor

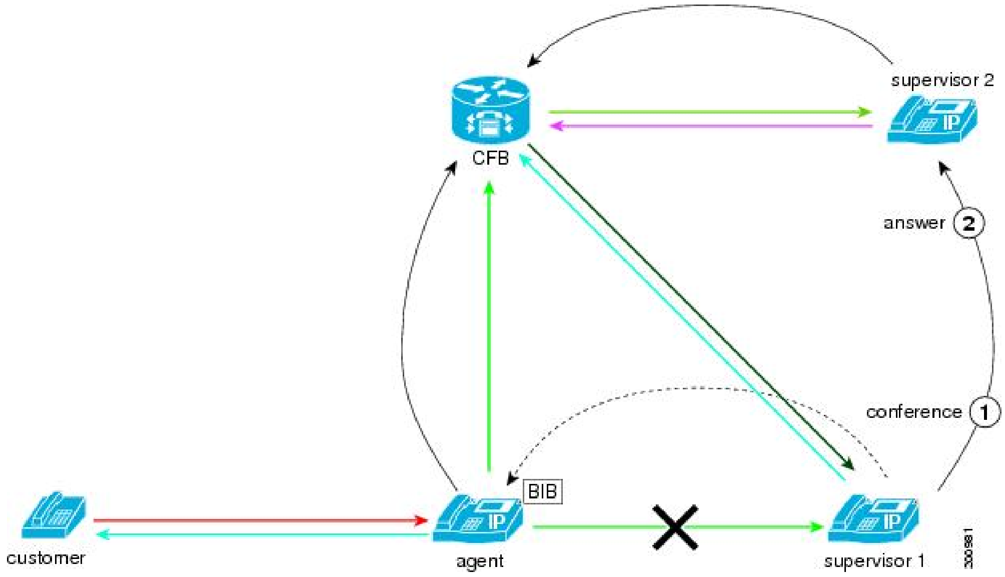


Supervisor Conferences In Another Supervisor

A supervisor can conference in another supervisor for the monitoring session.

The following figure illustrates this scenario.

Figure 84: Supervisor Conferences In Another Supervisor



In the example shown, supervisor 1, who started a monitoring call to the agent, conferences in supervisor 2 to the monitoring call. The customer and agent can still hear each other and are not aware of either of the monitoring supervisors. Both supervisor 1 and the supervisor 2 can hear the conversation of the agent with the customer. The two supervisors can hear each other.

Whisper Coaching

Whisper coaching allows supervisors to talk to agents during a monitoring session. To start a whisper coaching session, a monitoring session must already be in progress. A whisper coaching session is initiated by any CTI application (JTAPI/TAPI), such as Cisco Unified Contact Center Enterprise or Cisco Unified Contact Center Express.

Supervisors can toggle between monitoring and whisper coaching sessions as needed using a CTI application.

To enable whisper coaching, follow the instructions to enable monitoring. No additional configuration is needed for whisper coaching.

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 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 enabled, then the supervisor phone must have encryption enabled to silently monitor agent calls. If the agent phone has encryption enabled, but the supervisor phone does not, then requests to monitor the agent are rejected.

Secure Silent Monitoring and Transcoders

Cisco Unified Communications Manager transcoders do not support encrypted media. If a transcoder is required to establish the secure silent monitoring session between supervisor and agent, and the agent's phone is enabled for encrypted media, the monitoring session is not allowed. A tone is played to the supervisor and cause code 57 (Bearer capability not authorized) is used to disconnect the call. The CTI application notifies the supervisor that the monitoring session was disconnected.

Secure Silent Monitoring Icons

The following table describes the secure icons.

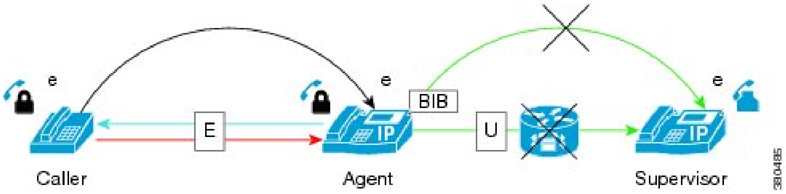


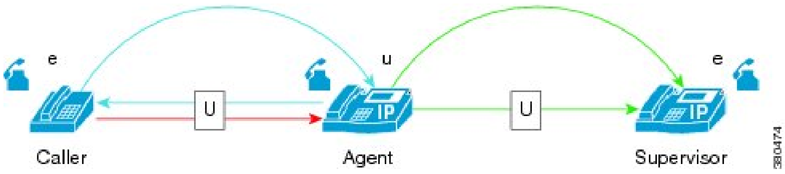
Table 94: Secure Silent Monitoring Icon Definitions

Icon	Description
e	Indicates that both devices can make and receive secure calls.
E	Indicates that the call media is encrypted using sRTP.
Lock Symbol	Indicates that the call is secure.

Secure Silent Monitoring Usage Scenarios

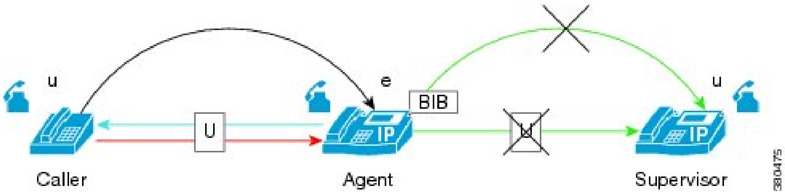
Unsecure Silent Monitoring Call

Supervisor’s phone is enabled for secure media, but the agent is not, so the silent monitoring call is unsecure.



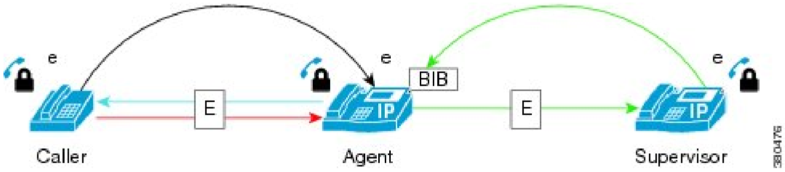
Secure Silent Monitoring Call

Supervisor's phone is not enabled for secure media, but the agent phone is enabled for secure media, so the silent monitoring call is rejected. Supervisor's phone does not meet or exceed security capabilities of agent device.



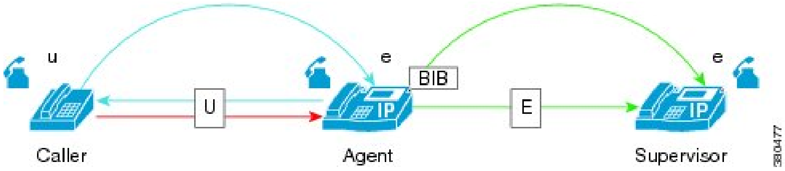
Encrypted Silent Monitoring Call

All phones support secure media, so all calls are encrypted.



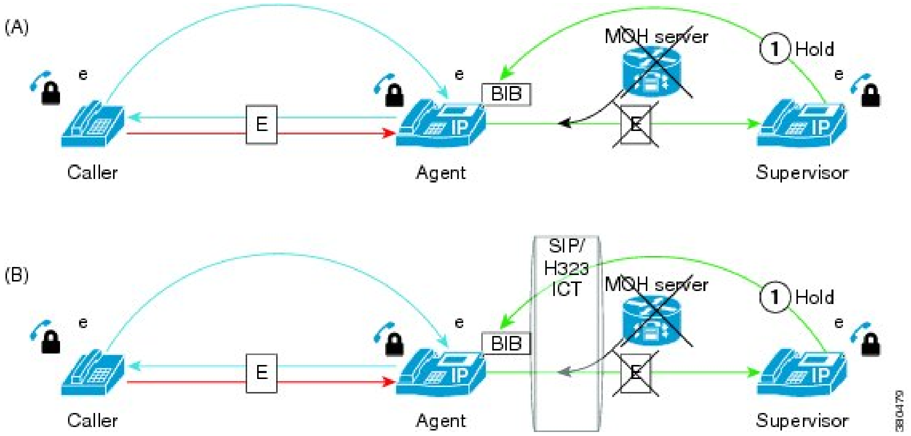
Unencrypted Silent Monitoring Call

Agent and supervisor phones both support secure media, so the silent monitoring call is encrypted, while the customer-agent call is unencrypted.



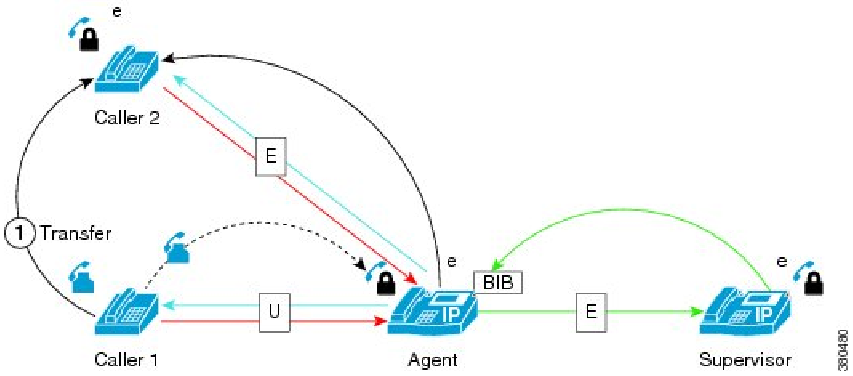
Supervisor Places Monitoring Call On Hold

Supervisor placing the monitoring call on hold has no affect on the caller-agent call. Monitoring session resumes when the supervisor resumes the call.



Call Security Upgrades as a Result of the Caller Transfer

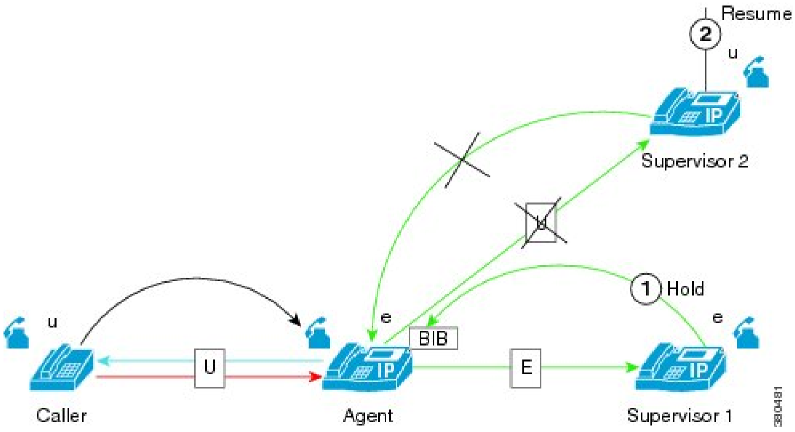
Cisco Unified Communications Manager determines if a call should be secured by examining the device capabilities of call-participants. When all call participant devices support sRTP, Cisco Unified Communications Manager automatically secures the call. When one or more call participant devices are not enabled for secure media using Secure Real Time Transfer Protocol (sRTP), the call is unsecure. If the agent device is enabled for sRTP, the Supervisor device must also be enabled for sRTP to establish a monitoring session. When caller 1 transfers to caller 2, the security of the call upgrades to secure media because caller 2’s phone is enabled for sRTP. The Secure Icons appear on the agent and caller 2 phones. The monitoring call is not affected as the supervisor’s phone is enabled for sRTP. The same scenario applies when the caller i-diverts to another destination or if caller 2 resumes the call via a shared line.



Transfer A Secure Monitoring Session to a Nonsecure Device

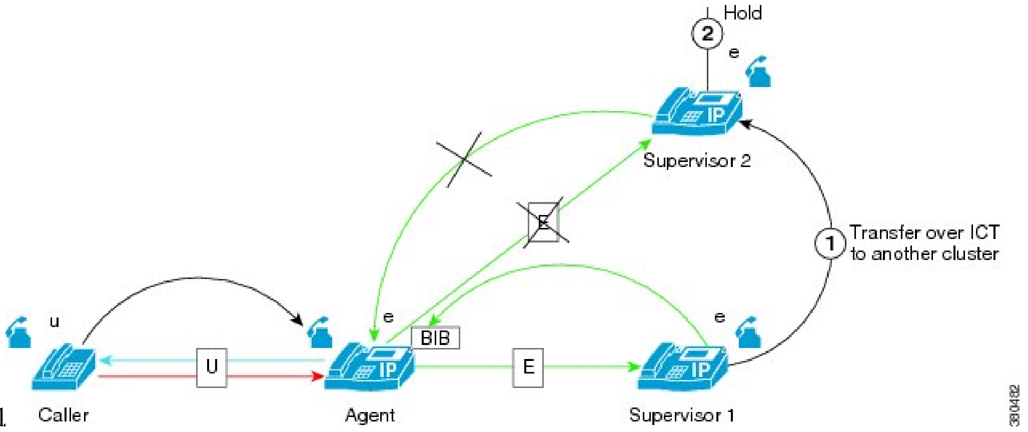
- Supervisor 1 monitors the agent in a secure monitoring session
- Supervisor 1 then transfers the monitoring call to supervisor 2
- Since supervisor 2’s device is not enabled for encrypted media, the monitoring call is disconnected.
- Tone is played to supervisor 2 and cause code 57 (Bearer capability not authorized) is used to disconnect this call.
- CTI notifies the application connected to the original supervisor who started the monitoring session (supervisor1) that the monitoring session was disconnected.

- If the monitoring call is held, then resumed using a shared line on another phone not enabled for encryption, the same behavior results



Supervisor Transfers Monitoring Call Across Inter-Cluster Trunk

Cisco Unified Communications Manager does not support transferring secure monitoring calls over an Inter-Cluster trunk. The secure monitoring call is



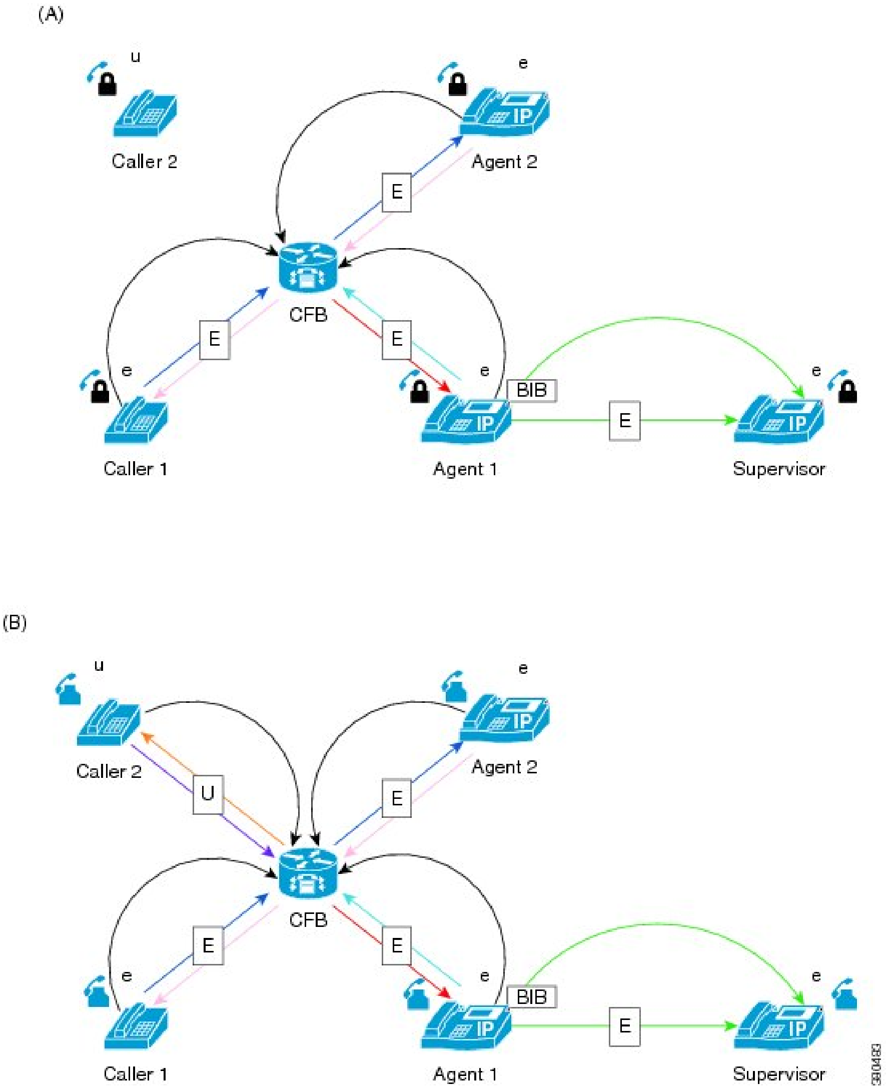
disconnected call.

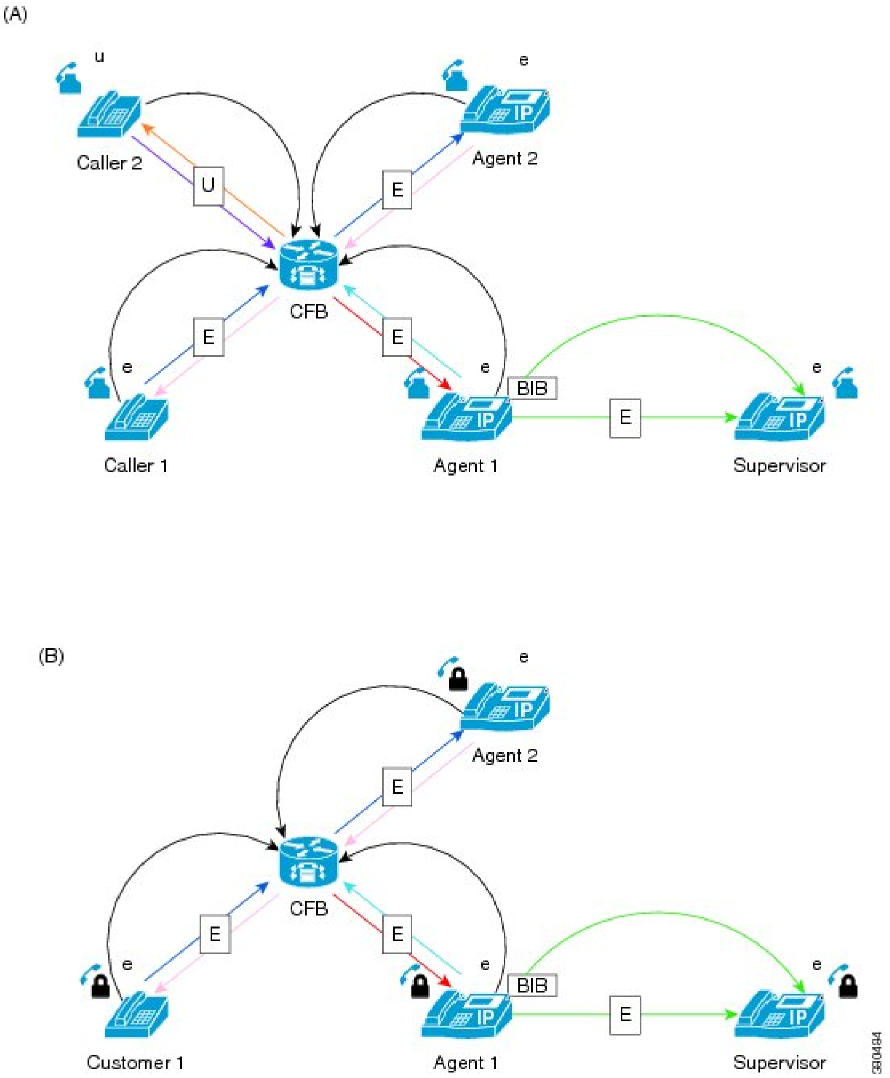
Secure Monitoring a Conference Call

1. Caller 1 and agent 1 are engaged in a secure call
2. Supervisor establishes a secure monitoring session
3. Caller 2 joins the call from a non-secure device, so call security is downgraded to unsecure.

   The secure silent monitoring session remains “encrypted” because agent 1 and supervisor both support encrypted media
4. Caller 2 leaves the call

   All remaining participants support encryption, so call security is upgraded automatically to use encrypted media
5. The original silent monitoring session was established as a secure call, so it remains unaffected

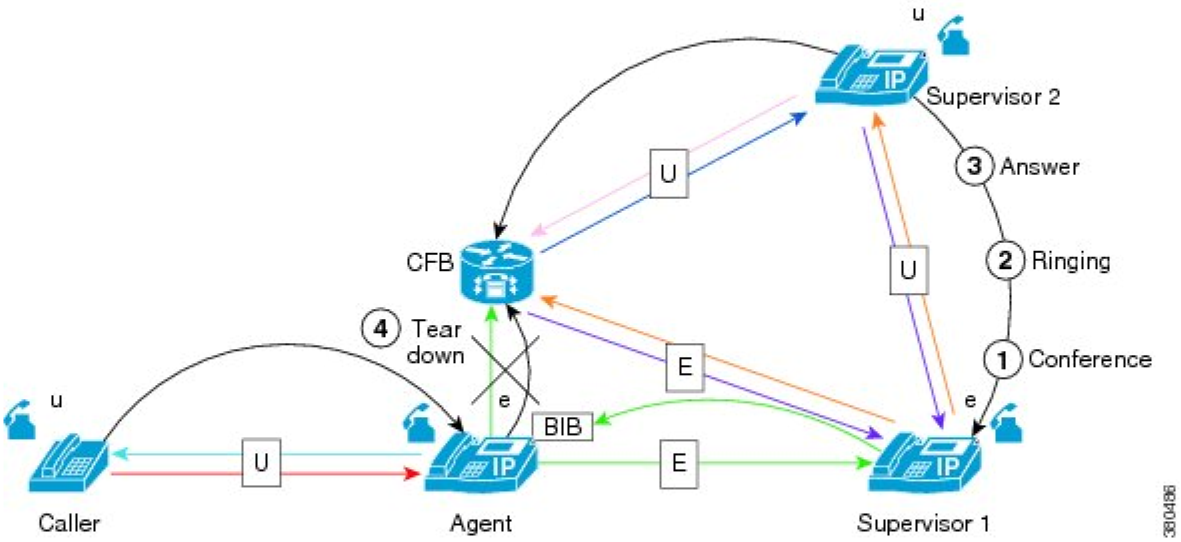

(A)
u
Caller 2
e
Agent 2
E
CFB
E
E
e
Caller 1
e
BIB
E
Agent 1
e
Supervisor
(B)
u
Caller 2
U
e
Agent 2
E
CFB
E
E
e
Caller 1
e
BIB
E
Agent 1
e
Supervisor
390483



Transfer Secure Silent Monitoring Calls

Supervisors can conference and transfer secure silent monitoring calls. Transfer of secure silent monitoring is possible if the transfer participant phone meets or exceeds the security capabilities of the Agent being monitored.

- Supervisor 1 is monitoring Agent in a secure monitoring session.
- Supervisor 1 transfers the call to Supervisor 2, whose phone is not enabled for encryption. When the call is transferred, the secure monitoring session call is disconnected.
- No tones are played to Supervisor 2. Supervisor 1 receives a CTI notification that the monitoring session was disconnected.



System Requirements

The following section provides the system requirements for monitoring.

Supported Devices

For more information about verification of agent phone models that are supported for call monitoring, see http://developer.cisco.com/web/sip/wikidocs/-/wiki/Main/Unified+CM+Silent+Monitoring+Recording+Supported+Device+Matrix

CTI Requirements

Computer Telephony Integration (CTI) provides the ability for applications to monitor calls on a per-call basis. Cisco defines the monitor target as the party that is monitored (agent) and the monitor initiator as the monitoring party (supervisor).

If a single CTI application monitors both the agent and supervisor phones, that application receives the call events that are necessary for silent monitoring. If different CTI applications monitor the agent and supervisor phones, the CTI application that monitors the agent phone must provide the call information to the application that observes the supervisor phone.

CTI applications that monitor calls must have the corresponding monitoring privileges enabled for the application-user or end-user account.

Configuration

This section provides the steps that are necessary to configure monitoring.

Turn on IP Phone Built-In-Bridge to Allow Monitoring

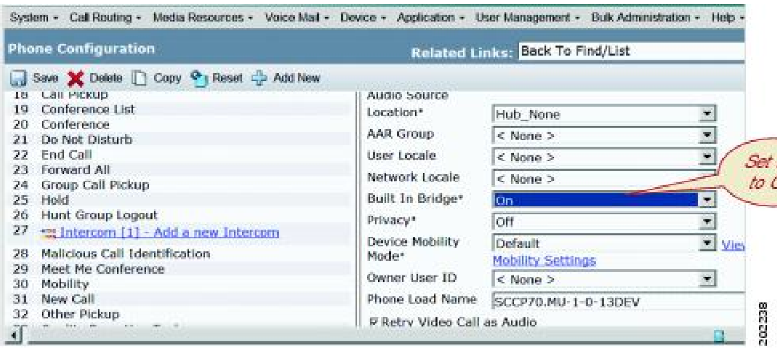
The built-in bridge (BIB) of the agent phone must be set to **On** to allow its calls to be monitored.

You can also set the **Built-in Bridge Enable** service parameter to **On** and leave the **Built-in Bridge in the Phone Configuration** window set to **Default**.

Use the **Device** > **Phone** menu option in Cisco Unified Communications Manager Administration to perform the necessary configuration.

Figure 85: Setting the Phone Built In Bridge to On

The following figure illustrates turning on the IP phone BIB to allow monitoring.


System ▾ Call Routing ▾ Media Resources ▾ Voice Mail ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾
Phone Configuration
Related Links: Back To Find/List
Save
Delete
Copy
Reset
Add New
Vie
Mobility Settings
202238

18 Call Pickup
19 Conference List
20 Conference
21 Do Not Disturb
22 End Call
23 Forward All
24 Group Call Pickup
25 Hold
26 Hunt Group Logout
27 Intercom [1] - Add a new Intercom
28 Malicious Call Identification
29 Meet Me Conference
30 Mobility
31 New Call
32 Other Pickup

Audio Source	
Location*	Hub_None
AAR Group	< None >
User Locale	< None >
Network Locale	< None >
Built In Bridge*	On
Privacy*	Off
Device Mobility Mode*	Default
Owner User ID	< None >
Phone Load Name	SCCP70.MU-1-0-13DEV

☑ Retry Video Call as Audio

Set BIB to On.

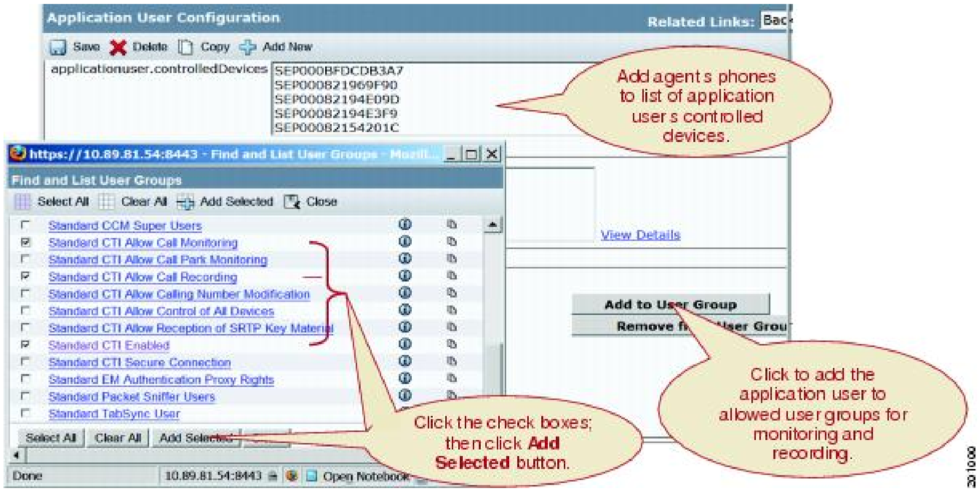
Add Supervisor to Groups That Allow Monitoring

Add the supervisor to the user groups: **Standard CTI Allow Call Monitoring user group** and the **Standard CTI Enabled user group**.

Use the **User Management** menu option in Cisco Unified Communications Manager Administration to perform the necessary configuration.

Figure 86: Adding Supervisors to Groups That Allow Monitoring

The following figure illustrates adding the user to these user groups.



applicationuser.controlledDevices
SEP000BFDCDB3A7
SEP000821969F90
SEP00082194E09D
SEP00082194E3F9
SEP00082154201C

□ Standard CCM Super Users
☑ Standard CTI Allow Call Monitoring
□ Standard CTI Allow Call Park Monitoring
☑ Standard CTI Allow Call Recording
□ Standard CTI Allow Calling Number Modification
□ Standard CTI Allow Control of All Devices
□ Standard CTI Allow Reception of SRTP Key Material
☑ Standard CTI Enabled
□ Standard CTI Secure Connection
□ Standard EM Authentication Proxy Rights
□ Standard Packet Sniffer Users
□ Standard TabSync User

Add agent s phones to list of application user s controlled devices.

Click the check boxes; then click **Add Selected** button.

Click to add the application user to allowed user groups for monitoring and recording.

Configure Monitoring Calling Search Space

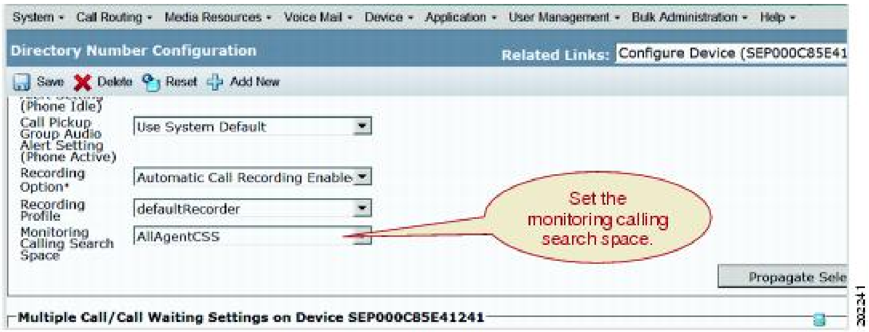
The monitoring calling search space of the supervisor line appearance must include the agent line or device partition.

Set the monitoring calling search space in the supervisor line appearance window.

Use the **Device** > **Phone** menu option in Cisco Unified Communications Manager Administration to perform the necessary configuration. When you display the Phone Configuration window for a phone, click on a line, such as Line [1], in the Association Information pane. (You can choose either a DN that is already associated with this phone or you can add a new DN to associate with this phone.) In the Directory Number Configuration window that displays, configure the Monitoring Calling Search Space field for the chosen line on this phone.

Figure 87: Configuring DN for Monitoring Calling Search Space

The following figure illustrates how to configure the monitoring calling search space.


System ▾ Call Routing ▾ Media Resources ▾ Voice Mail ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾
Directory Number Configuration
Related Links: Configure Device (SEP000C85E41
Save Delete Reset Add New
Propagate Sele
202341

(Phone Idle)

Call Pickup Group Audio Alert Setting (Phone Active): Use System Default

Recording Option*: Automatic Call Recording Enable

Recording Profile: defaultRecorder

Monitoring Calling Search Space: AllAgentCSS

Set the monitoring calling search space.

Multiple Call/Call Waiting Settings on Device SEP000C85E41241

Configure Notification Tones for Monitoring

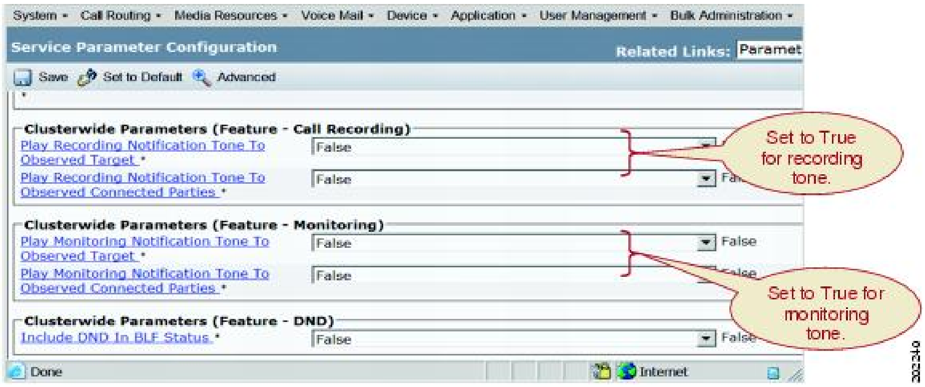
Set the service parameters for playing tone to **True** to allow tones to be played to the agent, the customer, or both.

CTI applications that initiate monitoring can also pass the play tone option to Cisco Unified Communications Manager. The monitoring tone plays when either the service parameter or the CTI application specifies the play tone option.

Use the **System** > **Service Parameters** menu option in Cisco Unified Communications Manager Administration to configure notification tones for monitoring.

Figure 88: Using Service Parameters to Configure Tones

The following figure illustrates how to use service parameters to configure tones.


System ▾ Call Routing ▾ Media Resources ▾ Voice Mail ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾
Service Parameter Configuration
Related Links: Paramet
Save Set to Default Advanced
Done
Internet
202340

Clusterwide Parameters (Feature - Call Recording)

Play Recording Notification Tone To Observed Target *: False

Play Recording Notification Tone To Observed Connected Parties *: False

Set to True for recording tone.

Clusterwide Parameters (Feature - Monitoring)

Play Monitoring Notification Tone To Observed Target *: False (False)

Play Monitoring Notification Tone To Observed Connected Parties *: False

Set to True for monitoring tone.

Clusterwide Parameters (Feature - DND)

Include DND In BLF Status *: False (False)

Set the Monitoring Service Parameters

This section describes the service parameters that are related to the silent monitoring feature.

Notification

The following service parameters affect the playing of notification tones to the parties that are monitored by the call monitoring feature:

Clusterwide Parameters (Feature - Monitoring)

- Play Monitoring Notification Tone To Observed Target
- Play Monitoring Notification Tone To Observed Connected Parties

The default value for these service parameters is **False**. You must change the value of each parameter to **True** to enable the particular notification tone to play.

Built-In-Bridge

The following service parameter enables or disables the built-in bridge on phones:

Clusterwide Parameters (Device - Phone)

Built-in Bridge Enable

For more information about this service parameter, see "Turn on IP phone BIB to allow Monitoring".

Secure Silent Monitoring Provisioning Phone Configuration

To configure the phone for secure silent monitoring, follow these steps:

Procedure

Step 1 Create a security profile for the Supervisor's phone type.

Step 2 Set the **Device Security Mode** in the security profile to **Encrypted**.

Step 3 Apply the device security profile to the Supervisor's device.

Recording

Call recording is a Cisco Unified Communications Manager feature that enables a recording server to archive agent conversations.

Terminology

The following terminology is used to describe recording:

Calling party
The person initiating the call; also referred to as the Customer.

Called party
The person answering the call; also referred to as the Agent.

Recorder
The application responsible for capturing and storing conversation media.

Built-in-Bridge (BiB)
Cisco IP Phone resources used to copy and forward the media streams of the Calling and Called parties to the Recorder.

Gateway

Cisco Voice Gateways and Unified Border Elements used to copy and forward the media streams of the Calling and Called parties to the Recorder.

Recording Media Source

The phone or gateway selected to copy and forward the media streams to the recorder.

Unified CM Recording Features

Call recording is one of the essential features in call centers, financial institutions and other enterprises. The recording feature sends copies of the agent and customer call media streams to the recorder. Each media stream is sent separately in an effort to best support a wide range of voice analytic applications.

Cisco Unified Communications Manager offers the following recording features:

- Allows conversations to be captured and stored for review, analysis, and/or legal compliance.
- Designed to use a combination of IP Phone and network (e.g. Gateway) resources to ensure conversations are recorded
- Mobility and off-network conversations can be captured using Network-recording; available in Unified Communications Manager release 10 or later
- Network topology friendly
- Does not require SPAN
- Provides Call Admission Control, Bandwidth Reservation, and Codec Negotiation

  Provides notification tones when legal compliance is required
- Supports Secure (sRTP) Media in Unified CM 8.0(1)
- Any conversation may be recorded; does not require contact center software

Network Based Recording

Network based recording is available as of Cisco Unified Communications Manager, Release 10.0(1). Network based recording allows you to use the gateway to record calls.

Network based recording offers the following benefits:

- Allows Cisco Unified Communications Manager to route recording calls, regardless of device, location, or geography.
- Centralizes recording policy control.
- Captures calls that are extended off the enterprise network to mobile and home office phones.
- Cisco Unified Communications Manager selects dynamically the right media source based on the call flow and call participants.
- Enhanced SIP Header and CTI metadata enables applications to track recorded calls in both single and multi-cluster environments.
- Recording Serviceability counters and alarms help compliance officers ensure that calls are recorded by monitoring the real-time status and historical performance of the feature.

Architecture

Cisco Unified Communications Manager uses either IP phone-based or network-based recording architecture to provide call recording.

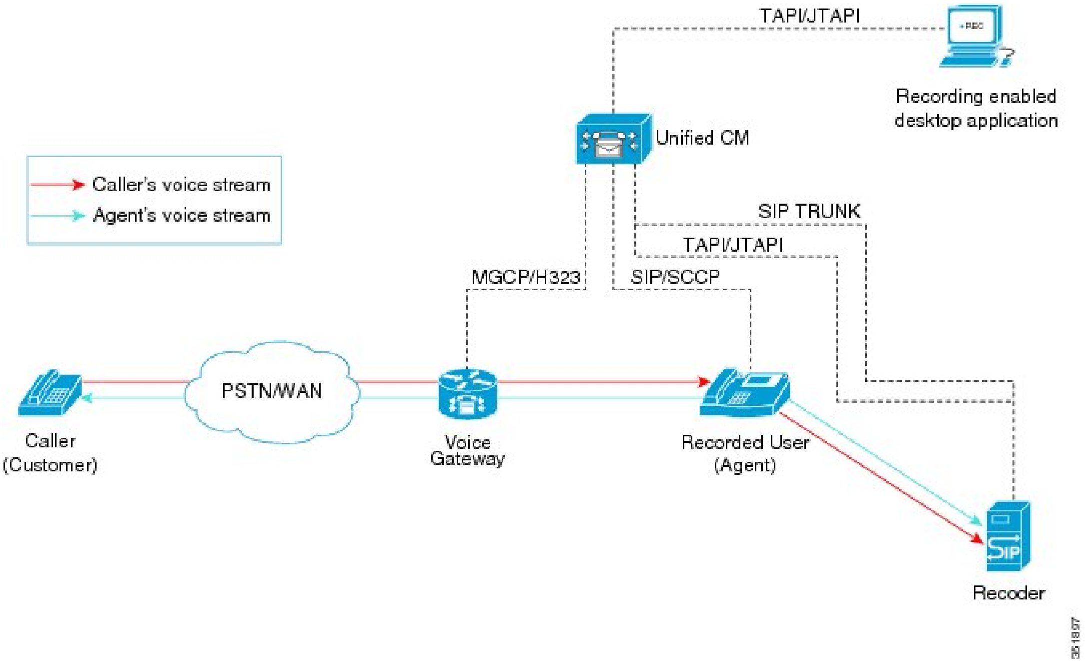
In IP phone based recording, recording media is sourced from the IP phones. The phone forks two media streams to the recording server where the media streams represent the two media streams in the call.

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 Cisco Unified Communications Manager over a SIP trunk.

IP Phone-Based Recording Architecture

The following figure illustrates the phone based approach for recording. In the illustration, the agent phone relays two independent media streams (the agent and the customer) to the recorder.

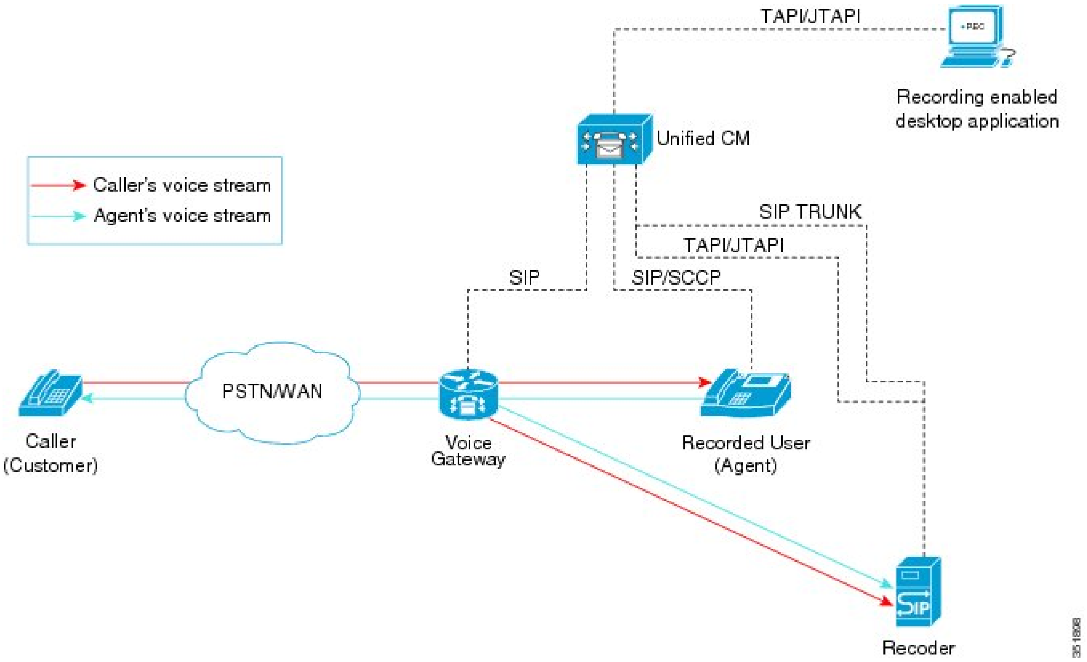
Figure 89: IP Phone-Based Recording Session



Network-Based Recording Architecture

The following diagram illustrates the network based approach for recording. In the illustration, the gateway relays two independent media streams (the agent and the customer) to the recorder.

Figure 90: Network-Based Recording Session



IP Phone Based Recording - How It Works

In IP phone based call recording, Cisco Unified Communications Manager forks media from an IP phone over to a recording servers. IP Phone based recording supports the following recording modes: Automatic, Selective Silent, and Selective User.

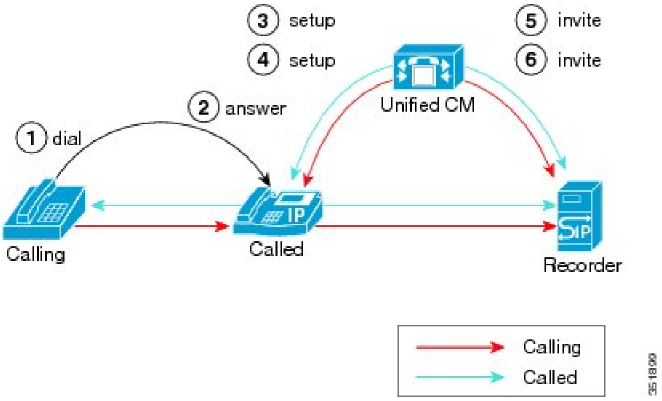
The following describes a typical call flow for IP phone based recording. In this example, call recording is configured to happen automatically.

- A call is received and answered on a line that is configured for automatic recording.
- Cisco Unified Communications Manager automatically sends two call setup messages to the BiB (Called) device. The first setup message is for the called party stream. The second setup message is for the calling party stream.
- Cisco Unified Communications Manager INVITES the recorder to both calls via SIP Trunk.
- The recorder accepts both calls.
- The phone BiB forks two call media streams to the recorder.

Note An optional recording tone can be configured to play to either the calling party, called party, or both. when a call is being monitored and recorded simultaneously, the recording tone settings override the monitoring tone settings

The following figure illustrates an IP phone based recording session that is configured for automatic recording.

Figure 91: IP Phone Based Recording



Network Based Recording - How it Works

With network based recording call recording media can be sourced from either the IP phone or from a gateway that is connected to Cisco Unified Communications Manager over a SIP trunk. Network based recording supports the following recording modes: Automatic, Selective Silent, and Selective User.

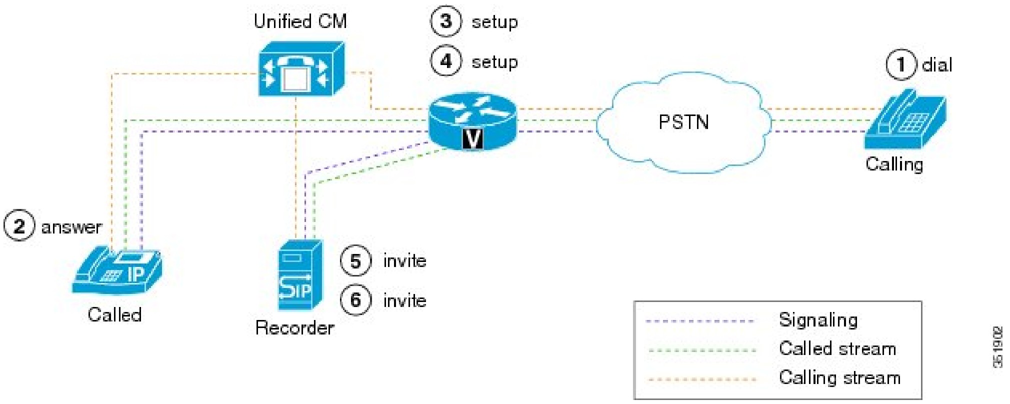
Following is a typical call flow for network based recording:

- A call is received and answered on a line that is configured for automatic silent recording where the gateway is selected as the recording media source.
- Cisco Unified Communications Manager automatically sends two call setup messages to the gateway.
- Cisco Unified Communications Manager INVITES the recorder to both calls via SIP Trunk.
- The recorder accepts both calls. and receives two RTP streams from the gateway.
- The gateway forks both media streams to the recorder.

Note An optional recording tone can be configured to play to the Calling, Called, or both parties. When the call is both monitored and recorded, recording tone settings override monitoring tone settings.

The following figure illustrates how network based recording works.

Figure 92: Network Based Recording



Recording Media Source Selection

When configuring recording, you must specify whether you want to use the phone or the gateway as the preferred media source for call recording. In selecting the recording media source, Cisco Unified Communications Manager takes into account the preferred media source that is configured for the user being recorded, the call media type, and whether a gateway is available in the call path.

Selecting the Recording Media Source

The following table summarizes how Cisco Unified Communications Manager selects the recording media source for calls. For example, if the gateway is chosen as the preferred recording media source, the media type is unsecured and there is a gateway in the call path, Cisco Unified Communications Manager will attempt to use the first gateway in the call path to record the media.

Note If the selected recording media source is unavailable, Cisco Unified Communications Manager will attempt to use an alternate source.

Table 95: Recording Media Source Selection

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

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

* Administrator chooses phone, phone is in the call path, phone is used for recording.

** Administrator chooses gateway, gateway is in call flow, gateway is used for recording.

*** Administrator selects gateway, but gateway is not in call flow, phone is used for recording.

**** Administrator selects gateway, gateway is in call flow, but media is secure, phone is used for recording.

Alternate Recording Source Selection

The following table displays the order that Cisco Unified Communications Manager follows when selecting an alternate source for the selected recording media in the event that the selected recording media source is unavailable. For example, if gateway is the selected media source, Cisco Unified Communications Manager will attempt to use the first gateway in the call path for recording. If that option fails, Cisco Unified Communications Manager will attempt to use the last gateway in the call path. Else, Cisco Unified Communications Manager will use the phone for call recording.

Table 96: Alternate Recording Media Source

Recording Source Selection	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

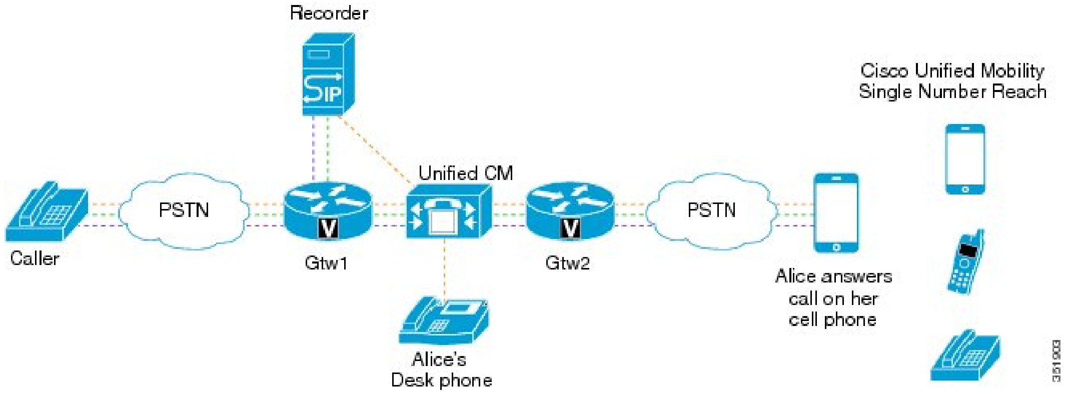
Gateway Selection

When you select the gateway as the preferred source, Cisco Unified Communications Manager attempts to use the first gateway in the call path for recording source media. This gateway may be the ingress or the egress gateway.

Single Number Reach Example

An external caller phones over the PSTN and Gateway 1 to Alice's desk phone. However, Alice is not in the office and has Single Number Reach configured on her desk phone so that Cisco Unified Communications Manager extends the call out of the enterprise network and back out across the PSTN to Alice's mobile phone. Because the gateway between the external caller and Cisco Unified Communications Manager is the first gateway in the call path, recording media is sourced from that gateway.

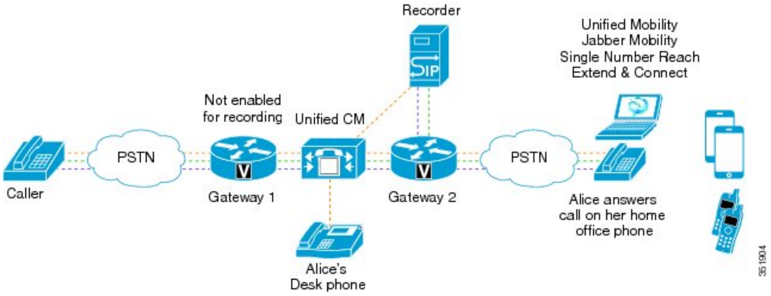
Figure 93: Single Number Reach Example



Cisco Extend & Connect Example

Bob and Alice both work for company X. Bob uses his Cisco IP Phone to call Alice's desk phone. However, Alice is working from home and has Cisco Jabber Extend & Connect configured. Cisco Unified Communications Manager extends the call off-network to Alice's home office phone and Alice answers the call on her home phone. Since Gateway 1 is not enabled for recording, Gateway 2 is used.

Figure 94: Cisco Extend & Connect Example



Recording Operation Modes

The following types of call recording modes exists:

Automatic silent recording

Automatic silent recording records all calls on a line appearance. Cisco Unified Communications Manager invokes the recording session automatically with no visual indication on the phone that an active recording session is established.

Selective silent call recording

Selective silent recording allows calls to be recorded as needed. 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. In Selective silent call recording, there is no visual indication on the phone that an active recording session is established.

For the two types of selective recording, selective silent recording is the default recording mode.

Selective user call recording

Selective user call recording allows calls to be recorded as needed. An agent can choose which calls to record and invoke the recording session via CTI-enabled desktop, or by a Softkey/Programmable Line Key. When selective user call recording is used, the Cisco IP phone displays recording session status messages. This feature is available in Cisco Unified Communications Manager 9.0(1) or later.

As of Release 10.0(1), mobility users can start or stop a recording session via DTMF (*86).

Regardless of the recording mode, each recording session delivers two unmodified RTP streams to the recording server over a SIP trunk. The independent media streams allow contact centers to take better advantage of speech analytic technologies that look for speech patterns, key words, and vocal behaviours that might indicate a problem during the call.

Note Silent selective and user selective call recording sessions can not be run simultaneously. When you try to invoke one of the selective recording modes while the other is already in use, the phone or CTI application displays a "Recording already started" message.

Automatic Silent Recording

In automatic call recording, Cisco Unified Communications Manager establishes the recording session automatically when the call connects. The following describes the call flow:

- A call is received and answered on a line that is configured for automatic silent recording.
- Cisco Unified Communications Manager automatically sends two call setup messages to the BiB (Called) device. The first setup message is for the called party stream. The second setup message is for the calling party stream.
- Cisco Unified Communications Manager INVITES the recorder to both calls via SIP Trunk.
- The recorder accepts both calls and receives two RTP streams from the phone BiB.

Note An optional recording tone can be configured to play to either the calling party, called party, or both. when a call is being monitored and recorded simultaneously, the recording tone settings override the monitoring tone settings

For an illustration of automatic silent recording, see the example in IP Phone Based Recording - How It Works, on page 873.

Selective Silent Recording

Selective silent recording is typically used in a call center environment to allow a supervisor to record an agent call. In selective silent recording mode, a CTI-enabled application running on a supervisor desktop is typically used to start and stop call recording for selected agent-customer calls. The call recording status does not display on the Cisco IP phone.

A typical call flow for selective silent recording is as follows:

- A call is received and answered on a line that is configured for selective recording.
- A supervisor working from a CTI-enabled desktop initiates the recording session. Alternatively, a recording server based on predetermined business rules.

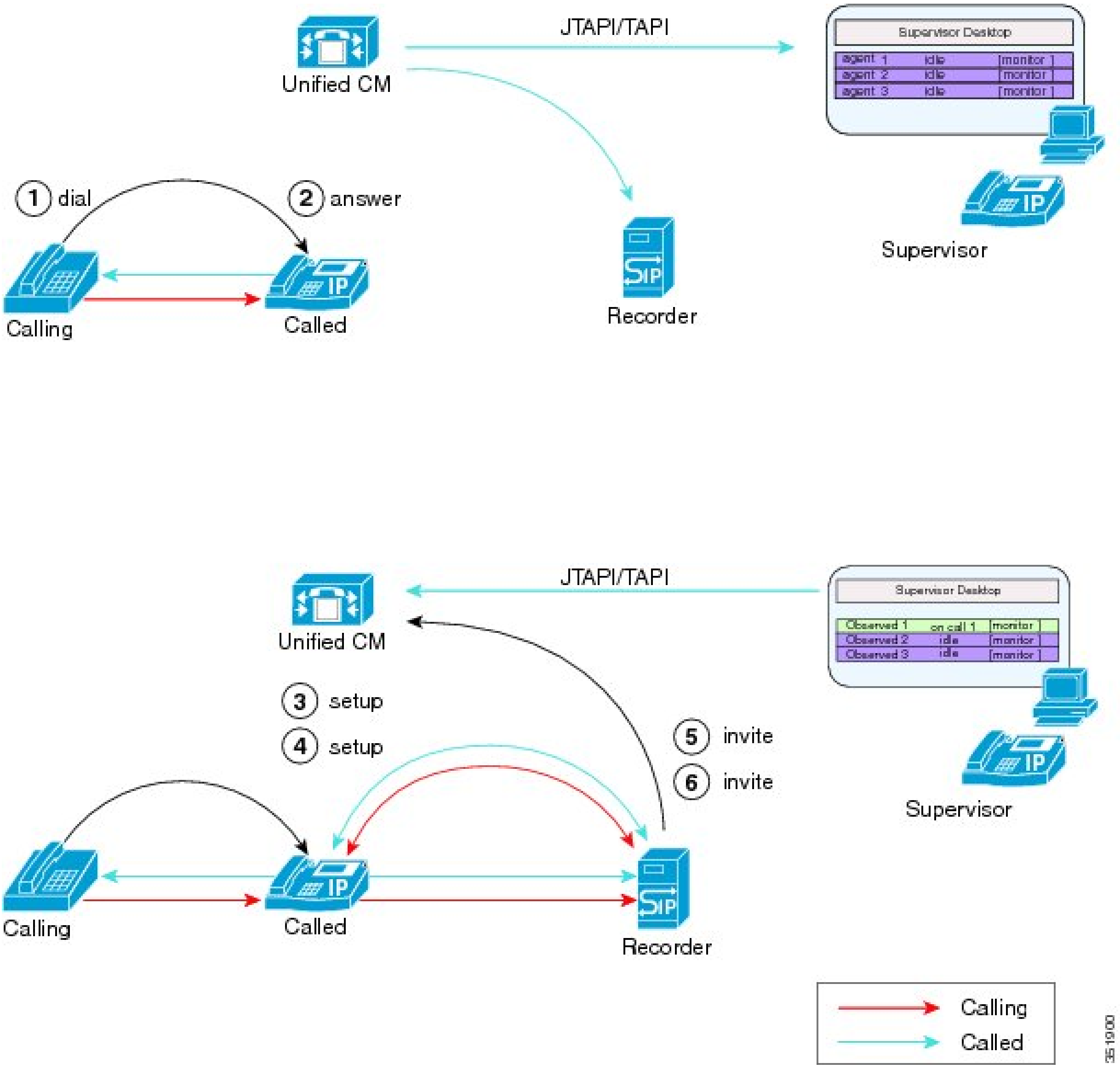
- Cisco Unified Communications Manager automatically sends two call setup messages to the BiB (Called) device: one for the called party media stream and one for the calling party media stream.
- Cisco Unified Communications Manager INVITES the recorder to both calls via SIP trunk.
- The recorder accepts both calls and receives two RTP streams from the device BiB.

Note An optional recording tone can be configured to play to the Calling, Called, or both parties. When the call is being monitored and recorded simultaneously, the recording tone settings override the monitoring tone settings.

In this example, the supervisor manages the recording session from a CTI-enabled desktop.

The following figure illustrates a selective silent call recording session.

Figure 95: Silent Selective Call Recording Mode



Selective User Recording

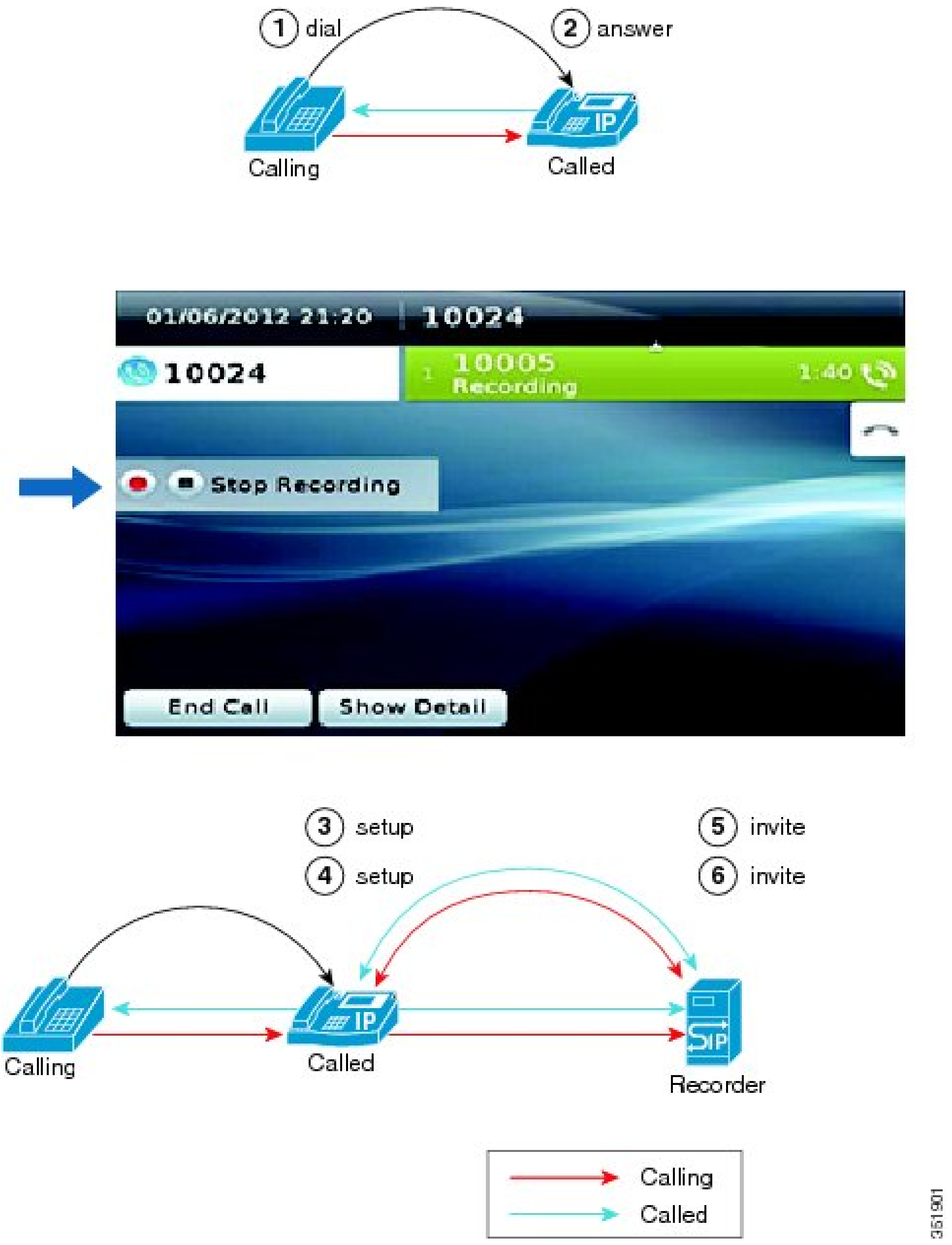
In selective user recording, an agent may start or stop a recording session using a softkey, programmable line key, or CTI-enabled application running on the desktop. In selective user recording, the call recording status displays on the Cisco IP phone.

Following is a typical call flow for selective user recording:

- A call is received and answered on a line configured for selective recording.
- The called party starts the recording session by pressing the ‘Record’ softkey or programmable linke key.
- Cisco Unified Communications Manager automatically sends two call setup messages to the BiB (Called) device: one to set up the media stream from the called party and the second to set up the media stream from the calling party.
- Cisco Unified Communications Manager sends an INVITE to the recorder via SIP trunk for both calls.
- The recorder accepts both calls and receives two RTP streams from the device BiB.
- The phone displays the status of the recording session. The Record key toggles to Stop Recording.

Note An optional recording tone can be configured to play to the Calling, Called, or both parties. When the call is being monitored and recorded, the recording tone settings override the monitoring tone settings.

Figure 96: Selective User Recording



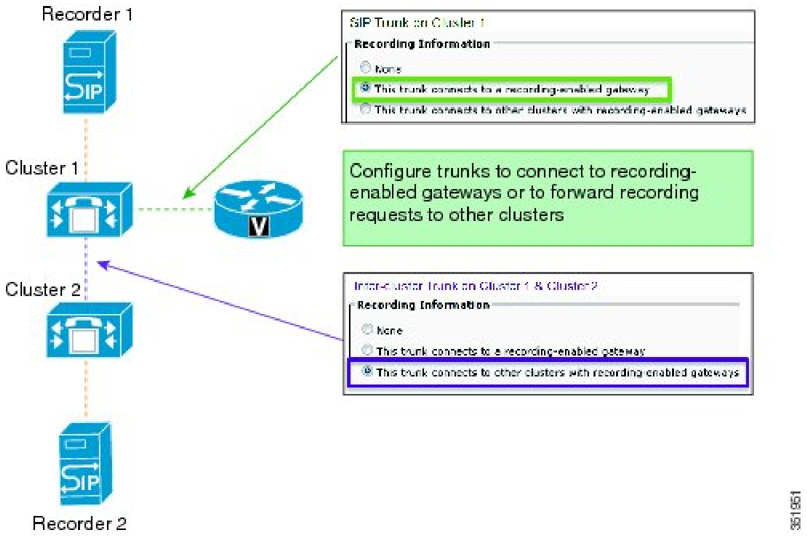
Recording In Multi-Cluster Environments

You can configure recording for multi-cluster networks. Your phones, gateways, and recorders can be connected to any cluster for recording to work. Cisco Unified Communications Manager can communicate recording requests between clusters so that recording can be centralized in a multi-cluster environment.

SIP Trunk Configuration

When you are configuring call recording in multi-cluster networks, you must set up the recording information for the trunks in your network. In Cisco Unified Communications Manager Administration, you can classify your trunks as either being connected to a recording-enabled gateway or being connected to other clusters that connect to recording-enabled gateways. If your trunks are classified as connecting to other clusters that connect to recording-enabled gateways, Cisco Unified Communications Manager forwards recording INVITES to the other clusters that connect to recording-enabled gateways. This allows you to centralize call recording in networks that span multiple clusters and to save on WAN bandwidth. You can set these details in the Recording Information section of the Trunk Configuration window.

Figure 97: Trunk Configuration for Multi-Cluster Recording



SIP Trunk on Cluster 1

Recording Information

○ None
● This trunk connects to a recording-enabled gateway
○ This trunk connects to other clusters with recording-enabled gateways

Configure trunks to connect to recording-enabled gateways or to forward recording requests to other clusters

Inter-cluster Trunk on Cluster 1 & Cluster 2

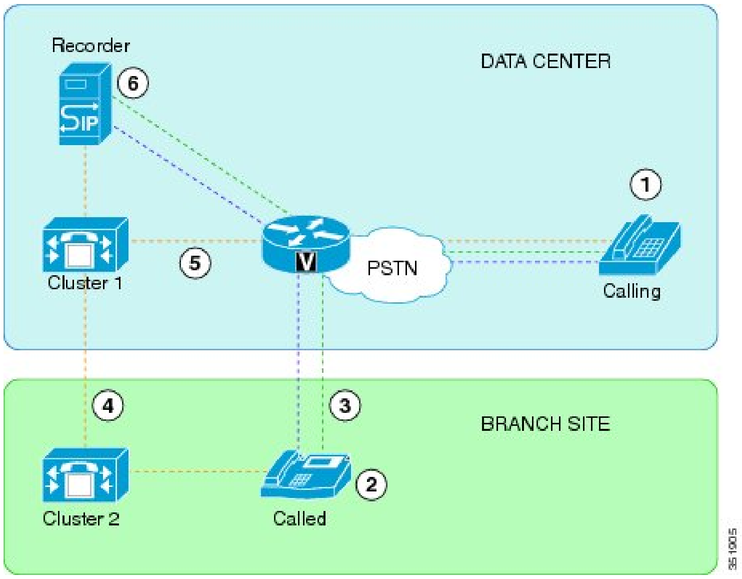
Recording Information

○ None
○ This trunk connects to a recording-enabled gateway
● This trunk connects to other clusters with recording enabled gateways

Multi-Cluster Recording Examples

The following example illustrates a multi-site internal company that has implemented gateway recording. In this example, the gateway that is used for recording depends on whether call recording is initiated from the calling party or from the called party. In this example, the calling party starts recording so Gateway 1 from Cluster 1 is used as the recording source.

Figure 98: Multi-Cluster Recording Example



Network Recording Use Cases

This section illustrates the following network recording use cases:

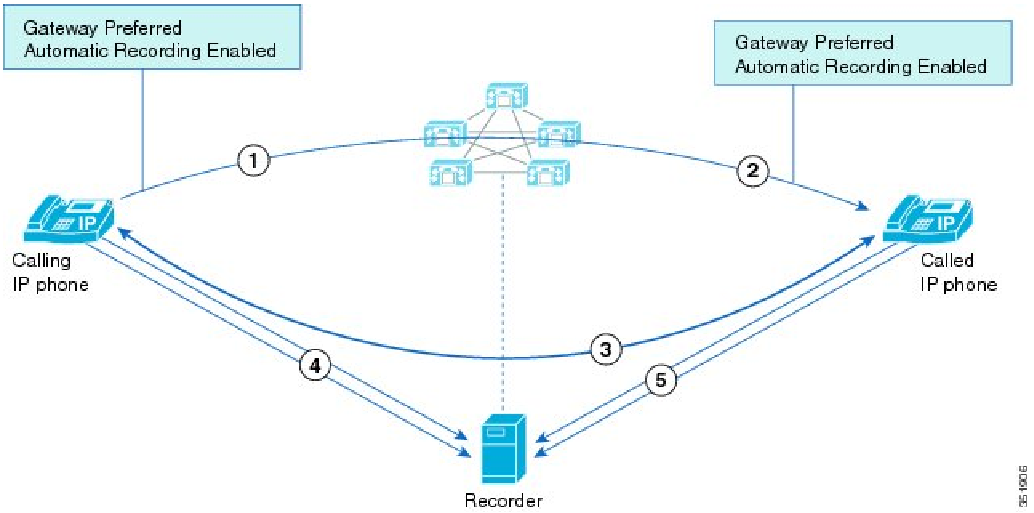
- IP phone to IP Phone both enabled for recording
- External Call to IP phone – Selective Recording
- Mid-Call – Gateway recording session stops when call is held
- Mobility – External Call to Mobile Jabber Client
- Mobility – External Call to Remote Destination Profile
- Extend & Connect – External Call to CTI Remote Device
- Inter-cluster Recording – External call from Cluster 1 to IP Phone on Cluster 2
- Inter-cluster Recording – External call from Cluster 1 is Held by User on Cluster 2

IP Phone to IP Phone Both Enabled for Recording

In this use case, Gateway is preferred, but the phone is selected.

- 1–3. An IP phone calls another IP phone
- 4–5. Two recording sessions are started automatically from both IP phones. The recording media source for both phones is Gateway Preferred. Since the gateway is not in the call flow Cisco Unified Communications Manager selects the IP Phones to fork the media to the recorder.

Figure 99: IP Phone to IP Phone Both Enabled for Recording

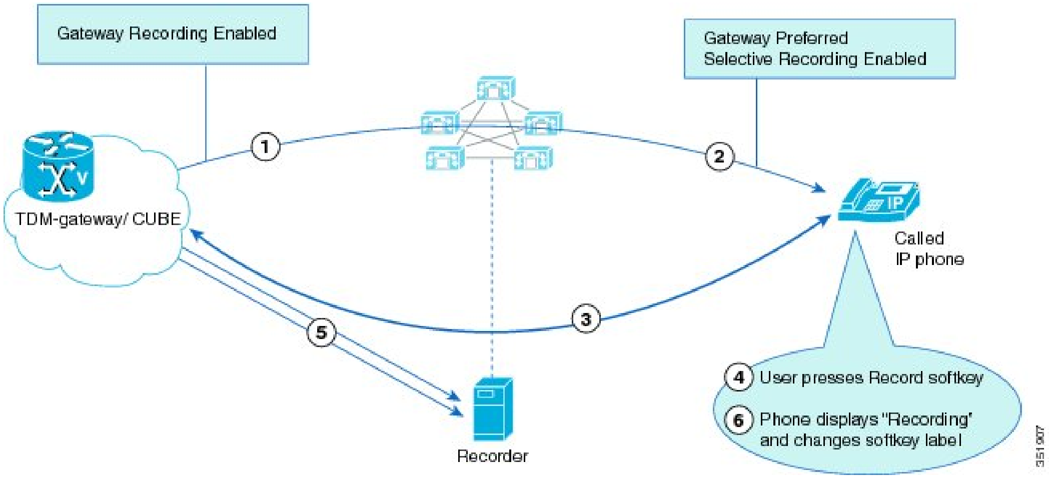


External Call to IP phone – Selective Recording

In this use case, Gateway is preferred and selected.

- 1–3. An external call is answered by a user with a Cisco IP phone.
- 4–5. The Cisco IP phone presses the Record softkey thereby starting a new recording session. The gateway is configured as the preferred recording media source and the gateway is valid for the call flow. Cisco Unified Communications Manager selects the gateway to fork the media to the recorder.
- 6. The Cisco IP phone displays "Recording…" and the softkey label changes to " StopRec".

Figure 100: External Call to IP phone – Selective Recording


Gateway Recording Enabled
Gateway Preferred
Selective Recording Enabled
1
2
TDM-gateway/ CUBE
IP
Called
IP phone
3
5
Recorder
4 User presses Record softkey
6 Phone displays "Recording'
and changes softkey label
351907

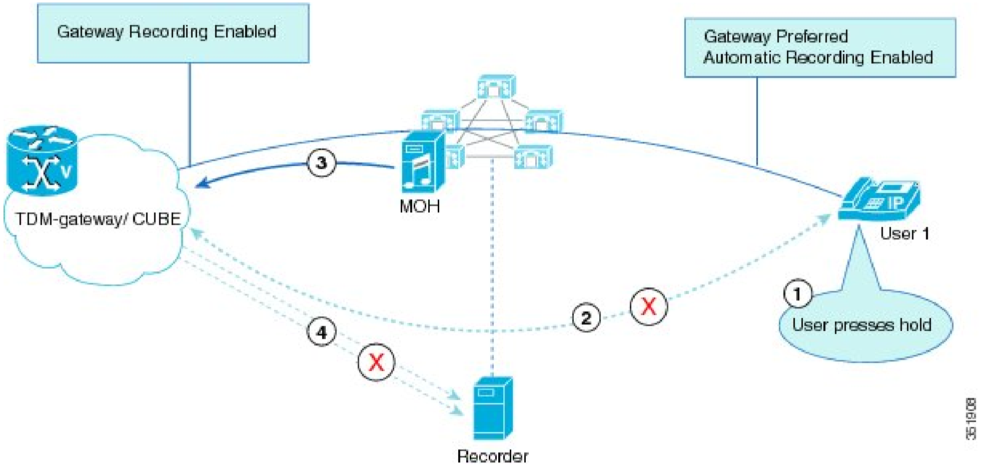
Mid-Call – Gateway Recording Session Stops When Call Is Held

This use case demonstrates the Hold function on the IP phone.

- 1–3. A call is in progress and the gateway is recording the media. User 1 places the call on hold. Cisco Unified Communications Manager plays Music-on-Hold to the caller.

- 4. Cisco Unified Communications Manager instructs the gateway to stop forking media to the recorder.

Figure 101: Mid-Call – Gateway Recording Session Stops When Call Is Held

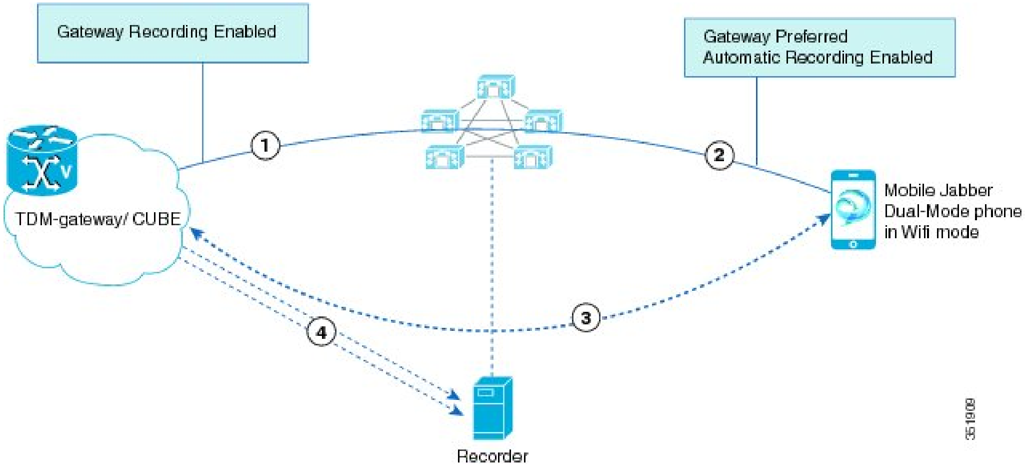


Mobility – External Call to Mobile Jabber Client

In this use case, the gateway is preferred and selected.

- 1–3. An external call is answered on a Mobile phone configured as a Dual-mode device
- 4. The recording session starts automatically for the dual mobile phone. The gateway is configured as the preferred recording source and is valid for the call flow. Cisco Unified Communications Manager selects the gateway to fork the media to the recorder.

Figure 102: Mobility – External Call to Mobile Jabber Client

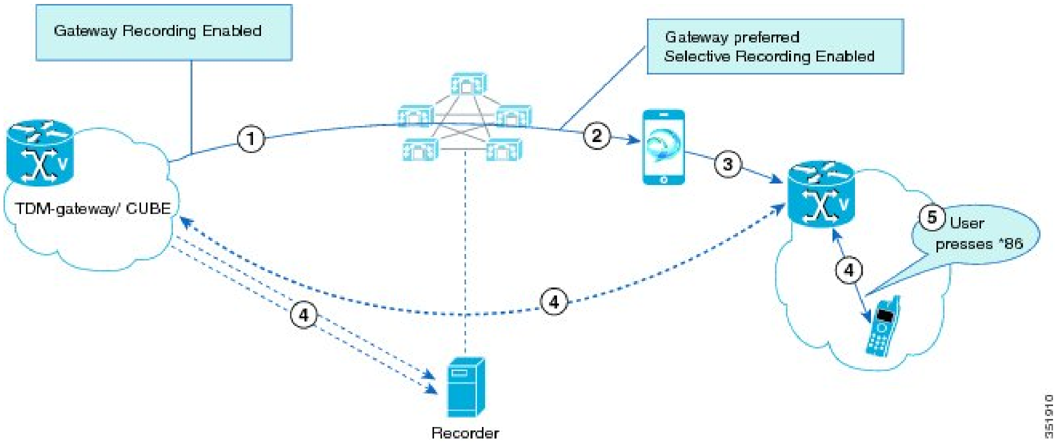


Mobility – External Call to Remote Destination Profile

In this use case, gateway is preferred and selected.

- 1–4. An external call is answered on a mobile phone using a remote destination configured on a Remote Destination Profile.
- 5–6. The mobile presses *86 to use DTMF to start the recording session. Cisco Unified Communications Manager selects the ingress gateway to fork the media to the recorder.

Figure 103: Mobility – External Call to Remote Destination Profile

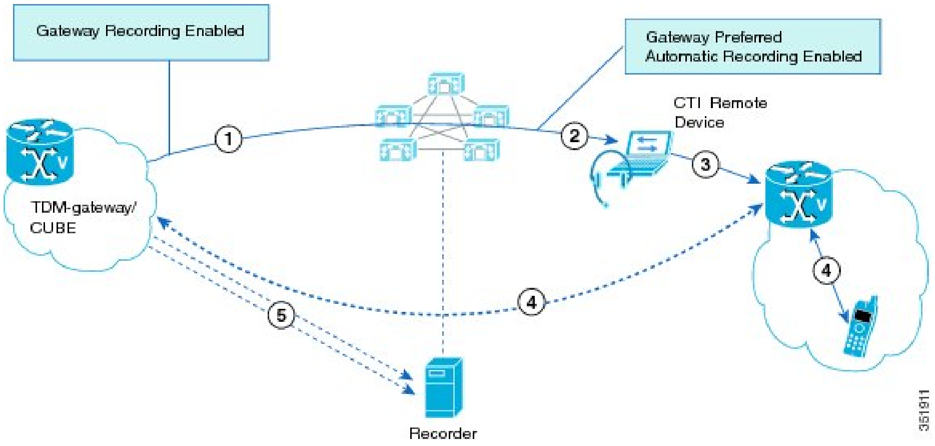


Extend & Connect – External Call to CTI Remote Device

In this use case, gateway is preferred and selected.

- 1–4. An external call is answered on an Extend & Connect remote destination that is configured as a CTI Remote Device.
- 5. The recording session starts from the CTI Remote Device. The gateway is configured as the preferred recording media source and is valid for the call flow. The ingress gateway is the first gateway in the call flow so Cisco Unified Communications Manager selects the ingress gateway to fork recording media to the recorder.

Figure 104: Extend & Connect – External Call to CTI Remote Device

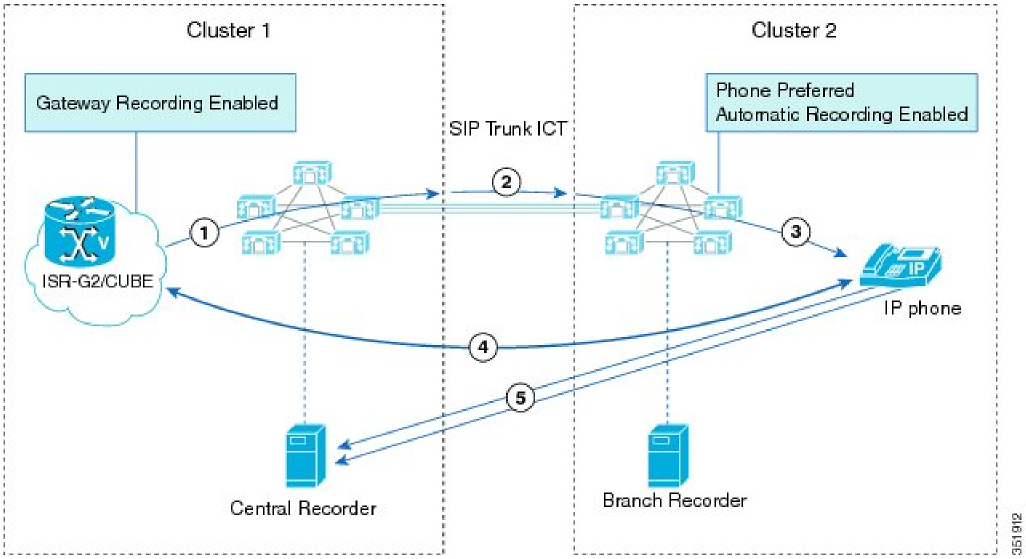


Inter-Cluster Recording – External Call From Cluster 1 to IP Phone on Cluster 2

In this use case, the gateway is selected. The Recording Profile specifies a central recorder.

- 1–4. An external call is received on a gateway in Cluster 1 and is answered by an IP phone in Cluster 2.
- 5. Recording starts automatically for the IP Phone in Cluster 2; the Phone is selected to fork the media. The recording profile assigned to the IP Phone is configured to use a central recorder.

Figure 105: Inter-Cluster Recording – External Call From Cluster 1 to IP Phone on Cluster 2

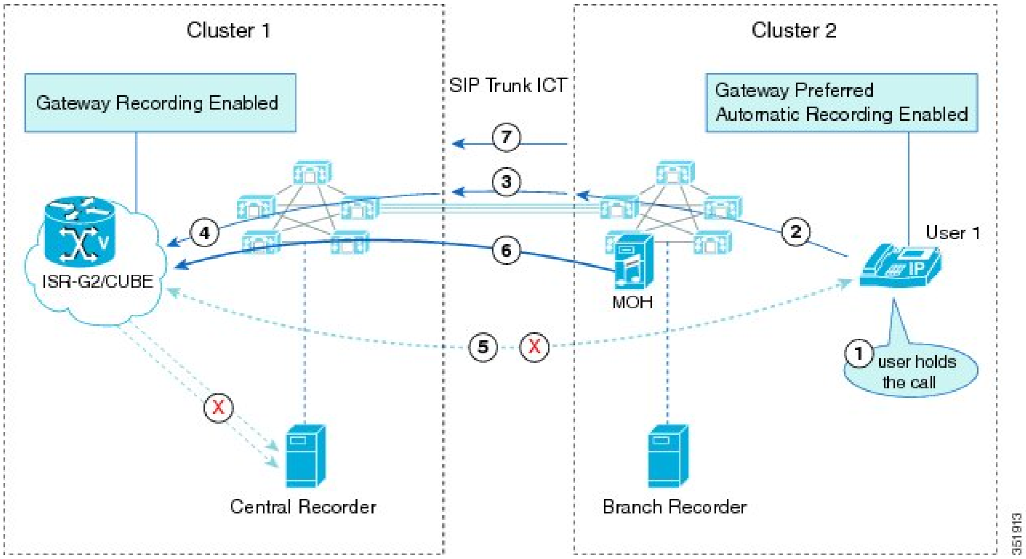


Inter-Cluster Recording – External Call From Cluster 1 Is HELD by User on Cluster 2

This use case demonstrates a mid-call Hold in an inter-cluster call.

- 1–5. An external call is underway to User 1 in Cluster 2. User 1 places the call on hold. The media stream is dropped.
- 6. Cisco Unified Communications Manager in Cluster 2 plays Music On Hold to the external caller.
- 7–8. Cisco Unified Communications Manager in Cluster 2 requests that Cluster 1 stop the recording session. Cluster 1 instructs the gateway to stop the session.

Figure 106: LInter-Cluster Recording – External Call From Cluster 1 Is HELD by User on Cluster 2



Recording Metadata

The SIP header that Cisco Unified Communications Manager sends to the recorder contains metadata that provides information on the media stream, such as device names, directory numbers, and cluster IDs. In addition, you can extract additional caller information with CTI.

You can obtain the following information for call participants from the SIP INVITE header or using CTI:

- Caller IDs
- Device names
- Directory numbers
- Cluster IDs
- Gateway IDs

In addition to the above information, you can use CTI to obtain the following information:

- Recorder profile directory number
- Recorder profile partition
- Recorder SIP trunk device name
- Near-end and far-end partitions
- Recording media source device type
- Recording media source cluster name
- Recording media source device name

Codec Selection

The rules for codec selection are as follows:

- The recording media sources send media streams with the same codec as the call that is being recorded.
- When Phone is configured as the recording media source, the recording codec is always the same as the original codec for the duration of the call.
- When Gateway is selected as the recording media source, the recording codec can be dynamically re-negotiated if the original conversation codec changes.
- If region settings for the recorder require different codecs, a transcoder is automatically inserted.

Note Some recording vendors transcode again for storage.

Recording Server Redundancy

Cisco Unified Communications Manager provides the following three options for setting up load balancing in order to provide redundancy for the recorder server.

- Option 1 - SIP redirect approach
- Option 2 - Route list approach
- Option 3 - DNS SRV records approach

Load balancing options vary depending on the vendor. Many vendors have implemented a SIP Proxy to provide server redundancy. You can use a route list with two or more SIP trunks to provide multiple SIP proxy and recording server redundancy. Refer to the vendor documentation for details on which options are supported by your recorder.

Option 1 - SIP Redirect Approach

Under this approach, the recorder or SIP Proxy issues a SIP 3XX response to redirect the Cisco Unified Communications Manager INVITE to load-balance multiple recorders.

Option 2 - Route List Approach

Under this approach, you can provide recorder load balancing by assigning multiple recorders to a route list. To do this:

- Configure your SIP trunks for each addressable recorder or recorder proxy.
- Assign your SIP trunks to a recorder route group with an assigned algorithm. The algorithm can be top-down or circular.
- Assign the recorder route group to a route list.
- Use a route pattern to direct traffic to the recorder route list.

Option 3 - DNS SRV Records

You can also use a DNS SRV record tag to populate the SIP trunk destination address. DNS SRV records can be set up with different priorities in order to provide primary and backup targets and provide load balancing across multiple targets.

DNS SRV records contain the service, protocol, domain name, TTL, class, priority, weight, port and target. Multiple SRV records may map to the same SRV record tag (service, protocol, domain name), which allows multiple records to be returned in response to a single DNS SRV query thereby providing redundancy.

Notification Tones

For legal compliance, an explicit notification in the form of a periodic tone can be made audible to Agent, Caller, or both to indicate a recording session is in progress. The tone can also be disabled. Recording tone settings override monitoring tone settings when both are enabled for the same call .

Use the following service parameters to set the default notification tone options:

- Play Recording Notification Tone To Observed Target(agent)
- Play Recording Notification Tone To Observed Connected Parties(customer)

The following figure illustrates the observed connected party and the observed target.

Figure 107: Observed Connected Party and Observed Party

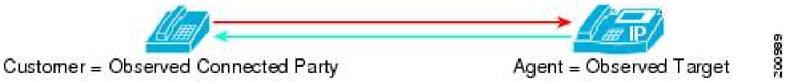


Table 97: Recording Notification Tones

Notification Tone set to play to...	Agent hears tone?	Caller hears tone?	Supervisor hears tone?	Recording stream for agent contains tone?	Recording stream for caller contains tone?
No one	No	No	No	No	No
Agent (Observed Party)	Yes*	No	No***	No	No*****
Customer (Caller)	No	Yes**	No***	Yes****	No*****
Both	Yes*	Yes**	No***	Yes****	No*****

* Agent phone plays the monitoring tone locally; it does not embed the tone into the RTP voice stream sent to the remote (the Caller phone).

** Agent phone embeds a monitoring tone into the RTP voice stream sent to the remote and the remote phone plays the RTP voice stream (with tone).

*** When the remote phone is a non-Cisco Unified Communications Manager device, tones are not generated so none are recorded. If the remote phone is a Cisco Unified Communications Manager device, then it generates a tone, so the tone is included in the recording.

**** The Agent recording stream is a copy of the primary stream sent to the remote The recording is a replica of the Caller's experience, so the tone is part of the recording.

***** When the remote phone is a non-Cisco Unified Communications Manager device, tones are not generated so none are recorded. If the remote phone is a Cisco Unified Communications Manager device, then it generates a tone, so the tone is included in the recording .

Secure Tone Interaction

Secure Tone was introduced in Cisco Unified CM 7.0(1) to provide call participants with an audible indication that the call is secured. The following rules apply to Secure Tones:

- When Secure Tone is enabled, the tone plays once to call participants at the beginning of the call.
- If Secure Tones and Monitoring Tones are both enabled, the Secure Tone plays once followed by Monitoring Tones (if the call is being monitored).
- If Secure Tones and Recording Tones are both enabled, the Secure Tone plays once, followed by Recording Tones (if the call is being recorded).

- If Secure, Monitoring, and Recording Tones are all enabled, the Secure Tone plays once followed by Recording Tones, which always take precedence over Monitoring Tones (if the call is being monitored and recorded).

Recording CDRs

Each call recording session generates one CDR for each media stream. To identify monitoring and recording CDRs, recording CDRs use the onBehalfOf fields to indicate that the calls were redirected by the recording feature. The GCI fields in the recording CDR are the same as the call that was recorded.

The original conversation ID in the recording CDR matches the Observed (Agent's) call leg that was recorded.

Recording Interactions and Limitations

The following interactions and limitations apply to call recording:

- The SIP header delivers recording metadata for each media stream. You can obtain additional metadata by using CTI interfaces for recording sessions that are managed by Cisco Unified Communications Manager.
- Cisco Unified Communications Manager supports multiple recording sessions for the same call when recording is started for both the Calling and Called parties.
- Cisco Customer Voice Portal calls may be recorded using Phone as recording media source.
- The gateway may not be a valid recording source for some call flows between two devices. For these call flows, select Phone as the recording media source. For additional detail, check the recording use cases.
- SIP Proxy servers may not be placed between Cisco Unified Communications Manager and the gateway.
- Each recording session adds two calls to the Busy Hour Call Completion (BHCC) rate with a minimal impact on CTI resources.
- If Multilevel Precedence and Preemption is configured, the **Busy Trigger** setting on the agent phone line must be at least 3.

Performance Counters and Alarms for Recording

Performance Counters

Monitor the health and status of recording media sources and sessions with real-time and historical performance counters. These counters are available in the Cisco Real-time Monitoring Tool under Cisco Call Recording.

The following table summarizes the recording performance counters that are available.

Table 98: Performance Counters Available for Call Recording

Performance Counter	Definition	Type
Recording Gateways In Service	The number of active or successful registrations to a recording-enabled gateway.	Real-time
Recording Gateways Out of Service	The number of configured recording gateways with no active registration.	Real-time
Recording Gateway Registration failures	The number of times registration to a recording-enabled gateway has failed.	Cumulative, Historical
Gateway Recording sessions active	The number of concurrent recording sessions (two streams) from the gateway to recorder.	Real-time
Gateway Recording session failures	The number of times a recording session with two streams from the gateway to the recorder has failed.	Cumulative, Historical
Phone Recording sessions active	The number of concurrent recording sessions with two streams from the phone to the recorder.	Real-time
Phone Recording session failures	The number of times a recording session with two streams from the phone to the recorder has failed.	Cumulative, Historical

Alarms

Recording feature alarms have been added to detect error conditions. The following table displays the recording alarms that are available.

Table 99: Alarms Available for Call Recording

Alarm Name	Description	Alarm Parameters	Severity
Recording Call Setup Fail	Indicates that the recording setup failed.	• Recorded device name • Recorded device DN • Recorded Device Call Leg ID (Origination or destination call leg identifier for the call.) • Gateway GUID (The global unique identifier, it is only available when gateway is recording media source.) • Recording Media Preference (The preference set for the recording resource) • Recording Media Source (The recording resource used for this recording request) • Recording Cluster ID • Reason	Error

Alarm Name	Description	Alarm Parameters	Severity
Recording Resources Not Available	Indicates that the recording request failed due to non-availability of recording resources.	• Recorded device DN • Recorded Device Call Leg ID (Origination or destination call leg identifier for the call.) • Gateway GUID (The global unique identifier, it is only available when gateway is recording media source.) • Recording Media Preference (The preference set for the recording resource) • Recording Media Source (The recording resource used for this recording request) • Recording Cluster ID	Warning

Alarm Name	Description	Alarm Parameters	Severity
Recording Already in Progress	Indicates that the recording request failed due to an existing recording request of the same name.	• Recorded device name • Recorded device DN • Recorded Device Call Leg ID (Origination or destination call leg identifier for the call.) • Gateway GUID (The global unique identifier, it is only available when gateway is recording media source.) • Recording Media Preference (The preference set for the recording resource) • Recording Media Source (The recording resource used for this recording request) • Recording Cluster ID • Reason	

Alarm Name	Description	Alarm Parameters	Severity
Recording Invalid Call State	Indicates that the recording request failed due to internal errors.	• Recorded device name • Recorded device DN • Recorded Device Call Leg ID (Origination or destination call leg identifier for the call.) • Gateway GUID (The global unique identifier, it is only available when gateway is recording media source.) • Recording Media Preference (The preference set for the recording resource) • Recording Media Source (The recording resource used for this recording request) • Recording Cluster ID • Reason	Information

Alarm Name	Description	Alarm Parameters	Severity
Recording Session Terminated Unexpectedly	Indicates that a recording in progress is terminated unexpectedly. The possible causes are trunk connected to recorder is out of service, recorder failed, or the call flow is not supported.	• Recorded device name • Recorded device DN • Recorded Device Call Leg ID (Origination or destination call leg identifier for the call.) • Gateway GUID (The global unique identifier, it is only available when gateway is recording media source.) • Recording Media Preference (The preference set for the recording resource) • Recording Media Source (The recording resource used for this recording request) • Recording Cluster ID • Reason	Error
Recording Gateway Registration Rejected	Registration to recording-enabled gateway rejected after multiple attempts; gateway marked out-of-service	• Gateway Address • Cause	Error
Recording Gateway Registration Timeout	No response from recording-enabled gateway after multiple attempts; timeout occurred; gateway marked out-of-service	• Gateway Address • Cause	Error
Recording Gateway Out Of Service	Recording-enabled gateway closed connection to Cisco Unified Communications Manager	• Gateway Address • Cause	Notice

Alarm Name	Description	Alarm Parameters	Severity
Recording Gateway In Service	Recording gateway status changed from out-of-service to in-service	• Gateway Address	Notice
Recording Gateway Session Failed	Recording gateway closed the recording session unexpectedly	• Gateway Address • Cause • Gateway GUID	Error

System Requirements

The following section provides the system requirements for recording.

Supported Devices

For details on which phone models are supported for call recording, see http://developer.cisco.com/web/sip/wikidocs/-/wiki/Main/Unified+CM+Silent+Monitoring+Recording+Supported+Device+Matrix.

Gateways Supported

- Supports both Voice gateways and Unified Border Elements (CUBE) as long as they interface with Unified CM using SIP and the Router platform supports the UC Services Interface (not supported for H323 or MGCP based calls).
- The word gateway is used interchangeably to refer to both Voice gateways and CUBE devices.
- The gateway has to be directly connected to Cisco Unified Communications Manager using a SIP trunk. Recording is not supported for SIP Proxy servers.
- ISR-Gen2 Gateways (29XX, 39XX Series) running 15.3(3)M train release are supported.
- ASR-100X Gateways running release XE 3.10 or later are supported.
- VG224 is not currently supported.

For additional details on which gateways are supported, see https://developer.cisco.com/web/sip/wiki/-/wiki/Main/Unified+CM+Recording+Gateway+Requirements.

Configuration

Call recording configuration involves:

1. Configure Recording Profile
    a. Configure SIP Profile (optional)
2. Configure Recorder as SIP trunk device
3. Configure route pattern for recorder
4. Configure recorder redundancy (if supported)
5. Enable recording on a line appearance
6. Configure IP Phone as recording media source (optional)
7. Configure Gateway as recording media source (optional)
8. Configure recording notification tones (optional)

Note At least one recording media source must be configured

Configure Recording Profile

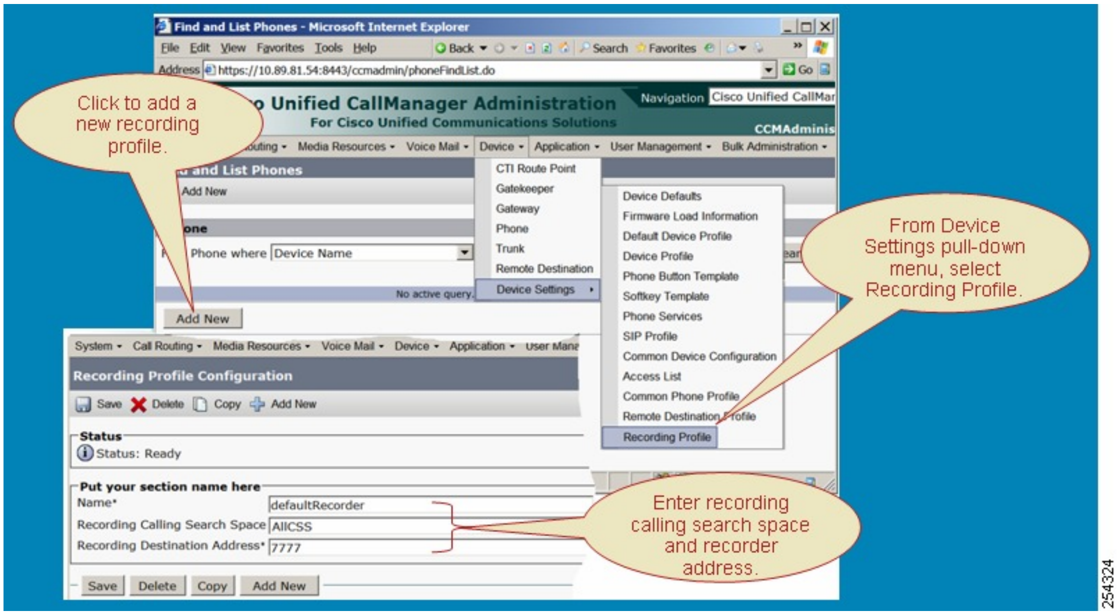
Create a recording profile from the Device Setting pull-down menu.

Enter the recording profile name, recording calling search space, and recording destination address.

Use the **Device** > **Device Settings** > **Recording Profile** menu option in Cisco Unified Communications Manager Administration to perform the necessary configuration.

The following figure illustrates creating a recording profile.

Figure 108: Creating a Recording Profile


Find and List Phones - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://10.89.81.54:8443/ccmadmin/phoneFindList.do
Go
o Unified CallManager Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CallMar
CCMAdminis
outing Media Resources Voice Mail Device Application User Management Bulk Administration
d and List Phones
Add New
one
Phone where Device Name
No active query.
Add New
CTI Route Point
Gatekeeper
Gateway
Phone
Trunk
Remote Destination
Device Settings
Device Defaults
Firmware Load Information
Default Device Profile
Device Profile
Phone Button Template
Softkey Template
Phone Services
SIP Profile
Common Device Configuration
Access List
Common Phone Profile
Remote Destination Profile
Recording Profile
System Call Routing Media Resources Voice Mail Device Application User Mana
Recording Profile Configuration
Save Delete Copy Add New
Status
Status: Ready
Put your section name here
Save Delete Copy Add New
254324

Name* defaultRecorder
Recording Calling Search Space AllCSS
Recording Destination Address* 7777

Click to add a new recording profile.

From Device Settings pull-down menu, select Recording Profile.

Enter recording calling search space and recorder address.

Create SIP Profile for Recorder (Optional)

Create a SIP profile for recording. Use the **Device** > **Device Settings** > **SIP Profile** menu option in Cisco Unified Communications Manager Administration to perform the necessary configuration.

You can check the Deliver Conference Bridge Identifier check box, which delivers additional information (specifically, the b-number that identifies a conference bridge) to the recorder across the SIP trunk. If the check box is left unchecked, the far-end information for the remote conference remains empty.

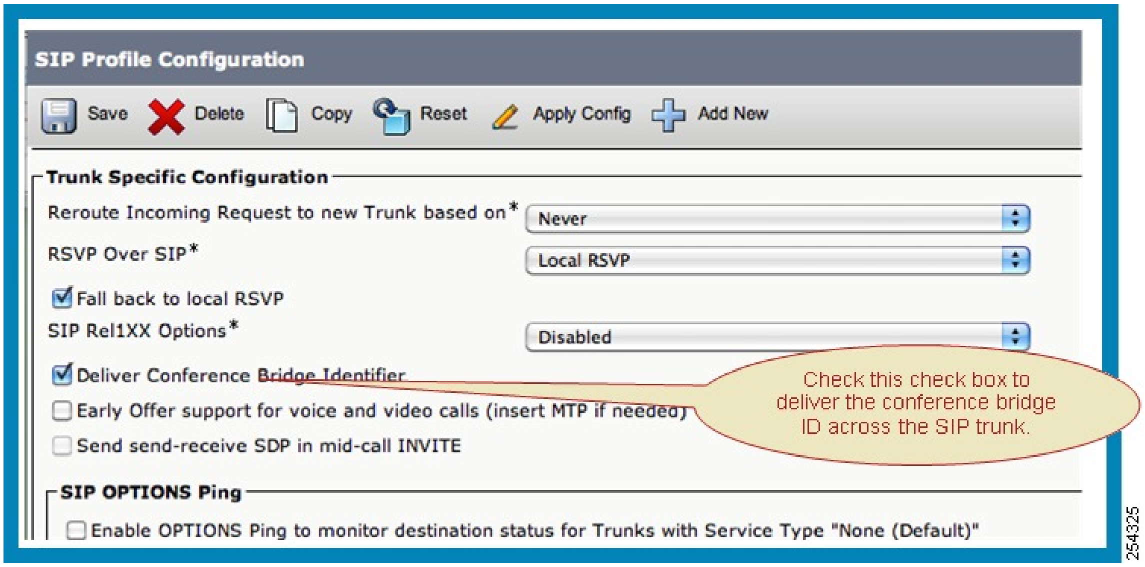
Check the Deliver Conference Bridge Identifier check box on the remote cluster SIP profile as well.

Note Checking this check box is not required for recording, but the conference bridge identifier helps to update the recorder when recording calls that involve a conference bridge. If you do not create a new SIP profile for recording, you can use the Standard SIP Profile.

See the Cisco Unified Communications Manager Administration Guide for details of configuring SIP profiles.

The following figure illustrates creating a SIP profile for recording.

Figure 109: Creating a SIP Profile for Recording



SIP Profile Configuration

Trunk Specific Configuration

Reroute Incoming Request to new Trunk based on* Never

RSVP Over SIP* Local RSVP

☑ Fall back to local RSVP

SIP Rel1XX Options* Disabled

☑ Deliver Conference Bridge Identifier

□ Early Offer support for voice and video calls (insert MTP if needed)

□ Send send-receive SDP in mid-call INVITE

SIP OPTIONS Ping

□ Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"

Check this check box to deliver the conference bridge ID across the SIP trunk.

Configure Recorder as SIP Trunk Device

The SIP trunk points directly to the recorder. Many recorders (such as those from Witness and Nice) consist of proxy, logger or storage and database.

The recorder accepts recording calls from Cisco Unified Communications Manager in SIP.

A directory number gets assigned to the recorder; a route pattern gets configured for the SIP trunk.

Create a SIP Trunk That Points to the Recorder

Create a SIP trunk that points to the recorder.

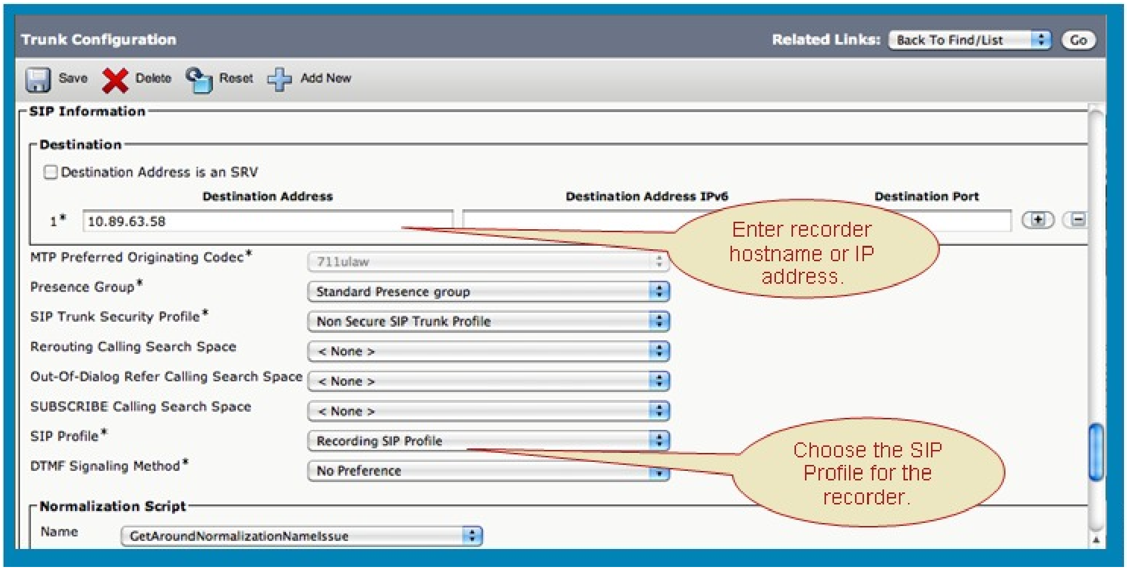
Enter the recorder DN, which must match a route pattern for the SIP trunk or a route list that includes the recorder.

Choose the appropriate SIP profile that you configured for recording.

Use the **Device** > **Trunk** menu option in Cisco Unified Communications Manager Administration to perform the necessary configuration.

The following figure illustrates creating a SIP trunk that points to the recorder.

Figure 110: Creating a SIP Trunk That Points to the Recorder



SIP Information

Destination

☐ Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	10.89.63.58		

MTP Preferred Originating Codec* 711ulaw

Presence Group* Standard Presence group

SIP Trunk Security Profile* Non Secure SIP Trunk Profile

Rerouting Calling Search Space < None >

Out-Of-Dialog Refer Calling Search Space < None >

SUBSCRIBE Calling Search Space < None >

SIP Profile* Recording SIP Profile

DTMF Signaling Method* No Preference

Normalization Script

Name GetAroundNormalizationNameIssue

Enter recorder hostname or IP address.

Choose the SIP Profile for the recorder.

Configure Route Pattern for Recorder

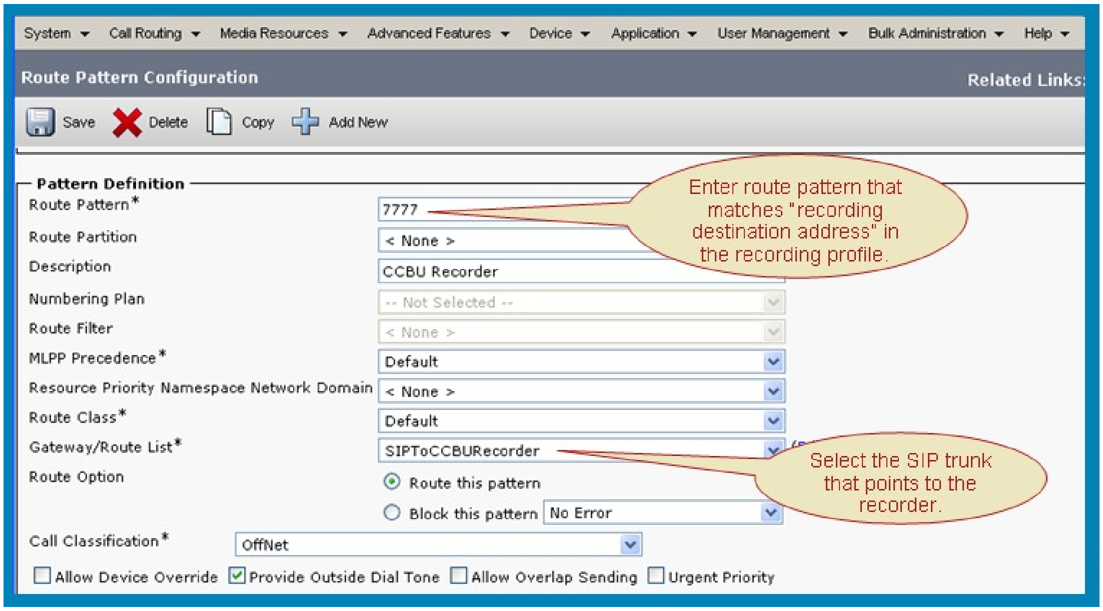
Create a route pattern for the recorder SIP trunk. The Recording Destination Address in the recording profile must match this pattern.

Select the SIP trunk that points to the recorder, or select a route list of which the recorder is a member.

Use the **Call Routing** > **Route/Hunt** > **Route Pattern** menu option in Cisco Unified Communications Manager Administration to perform the necessary configuration.

The following figure illustrates creating a route pattern for the recorder.

Figure 111: Creating a Route Pattern for the Recorder



Pattern Definition

Route Pattern* 7777

Route Partition < None >

Description CCBU Recorder

Numbering Plan -- Not Selected --

Route Filter < None >

MLPP Precedence* Default

Resource Priority Namespace Network Domain < None >

Route Class* Default

Gateway/Route List* SIPToCCBURecorder

Route Option ● Route this pattern

○ Block this pattern No Error

Call Classification* OffNet

☐ Allow Device Override ☑ Provide Outside Dial Tone ☐ Allow Overlap Sending ☐ Urgent Priority

Enter route pattern that matches "recording destination address" in the recording profile.

Select the SIP trunk that points to the recorder.

Configure Recorder Redundancy (If Supported)

Many recorders have built-in proxy and redundancy functionalities, for example, Nice/Witness recorders.

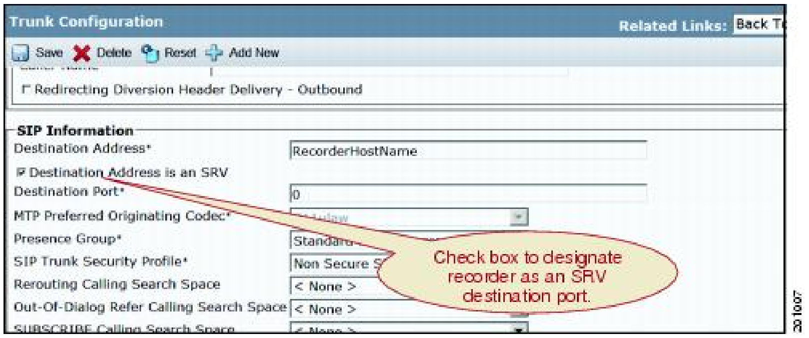
You can also use the following mechanism to achieve recorder redundancy:

- Use the SRV record for the recorder destination address in SIP trunk configuration.
- Use multiple recorders for redundancy and load balance. Create a SIP trunk for each recorder; create a route list to include the route groups that have individual SIP trunks as a member.

Use the **Device** > **Trunk** menu option in Cisco Unified Communications Manager Administration to perform the necessary configuration.

The following figure illustrates enabling SRV for a SIP trunk.

Figure 112: Enabling SRV for a SIP Trunk



□ Redirecting Diversion Header Delivery - Outbound

SIP Information

Destination Address* RecorderHostName

☑ Destination Address is an SRV

Destination Port* 0

MTP Preferred Originating Codec*

Presence Group* Standard

SIP Trunk Security Profile* Non Secure S

Rerouting Calling Search Space < None >

Out-Of-Dialog Refer Calling Search Space < None >

SUBSCRIBE Calling Search Space < None >

Check box to designate recorder as an SRV destination port.

Enable Recording for a Line Appearance

To enable recording of an agent, set the Recording Option in the line appearance of the agent to one of the following options:

- Automatic Call Recording Enabled
- Selective Call Recording Enabled

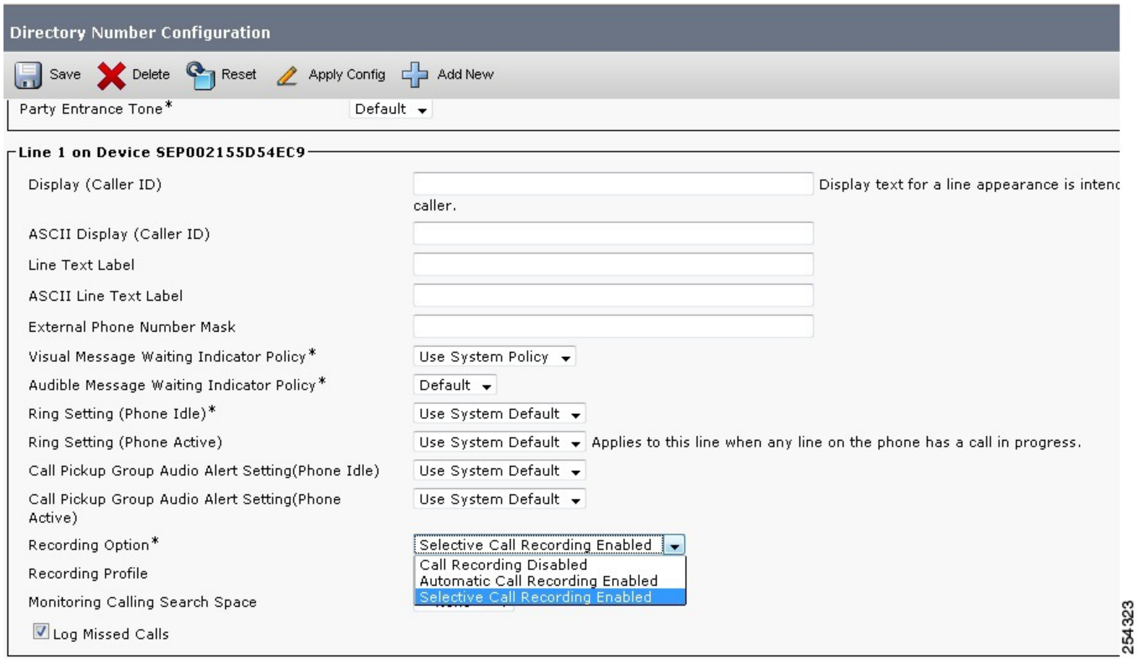
Select a pre-created recording profile from the drop-down list box. (**Use Device** > **Device Settings** > **Recording Profile** to configure a recording profile.)

Use the **Call Routing** > **Directory Number** menu option in Cisco Unified Communications Manager Administration to perform the necessary configuration.

If you also have Multilevel Precedence and Preemption (MLPP) configured, make sure the **Busy Trigger** is set to at least 3.

The following figure illustrates enabling recording for a line appearance.

Figure 113: Enabling Recording for a Line Appearance



Party Entrance Tone* Default

Line 1 on Device SEP002155D54EC9

Display (Caller ID) — Display text for a line appearance is intenc caller.

ASCII Display (Caller ID)

Line Text Label

ASCII Line Text Label

External Phone Number Mask

Visual Message Waiting Indicator Policy* Use System Policy

Audible Message Waiting Indicator Policy* Default

Ring Setting (Phone Idle)* Use System Default

Ring Setting (Phone Active) Use System Default — Applies to this line when any line on the phone has a call in progress.

Call Pickup Group Audio Alert Setting(Phone Idle) Use System Default

Call Pickup Group Audio Alert Setting(Phone Active) Use System Default

Recording Option* Selective Call Recording Enabled

- Call Recording Disabled
- Automatic Call Recording Enabled
- Selective Call Recording Enabled

Recording Profile

Monitoring Calling Search Space

☑ Log Missed Calls

Configure Recording Media Source for a Line Appearance

Add the Record Softkey or Programmable Line Key to the Device Template (Optional)

To enable a user to start and stop recording from a Cisco IP device, add the Record softkey or programmable line key to the device template.

To add the Record softkey, use the **Device** > **Device Settings** > **Softkey Template** menu option in Cisco Unified Communications Manager Administration to create or modify a nonstandard softkey template. Configure the softkey layout for call state *connected* to have the Record softkey in the selected softkeys list.

To add the Record programmable line key, use the **Device** > **Device Settings** > **Phone Button Template** menu option in Cisco Unified Communications Manager Administration. Enter the button template name, feature, and label.

Configure IP Phone as Recording Media Source (Optional)

Turn on IP Phone BIB to allow Recording

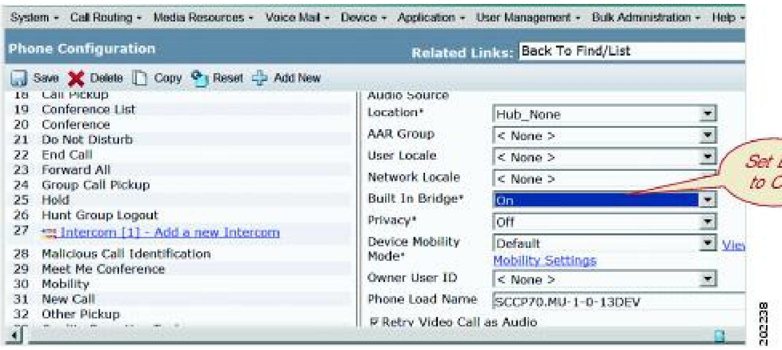
The built-in bridge (BIB) of the agent phone must be set to **On** to allow its calls to be recorded.

You can also set the **Built-in Bridge Enable** service parameter to **On** and leave the **Built-in Bridge in the Phone Configuration** window set to **Default**.

Use the **Device** > **Phone** menu option in Cisco Unified Communications Manager Administration to perform the necessary configuration.

Figure 114: Setting the Phone Built In Bridge to On

The following figure illustrates how to turn on the IP phone BIB to allow recording.


System ▾ Call Routing ▾ Media Resources ▾ Voice Mail ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾
Phone Configuration
Related Links: Back To Find/List
Save
Delete
Copy
Reset
Add New
202238

18 Call Pickup
19 Conference List
20 Conference
21 Do Not Disturb
22 End Call
23 Forward All
24 Group Call Pickup
25 Hold
26 Hunt Group Logout
27 Intercom [1] - Add a new Intercom
28 Malicious Call Identification
29 Meet Me Conference
30 Mobility
31 New Call
32 Other Pickup

Audio Source
Location* Hub_None
AAR Group < None >
User Locale < None >
Network Locale < None >
Built In Bridge* On
Privacy* Off
Device Mobility Mode* Default View
Mobility Settings
Owner User ID < None >
Phone Load Name SCCP70.MU-1-0-13DEV
☑ Retry Video Call as Audio

Set BIB to On.

Configure Recorder as SIP Trunk Device

The administrator needs to enable call recording for a SIP trunk pointing to a recording enabled SIP IOS gateway, in order to use the gateway for the media forking.

Cisco Unified Communications Manager registers with the gateway as a XMF Application at initialization time or when the SIP trunk is reset, after the SIP trunk is enabled for gateway recording. The corresponding settings on the gateway for the XMF provider needs to be configured for Cisco Unified Communications Manager to register with the gateway.

Cisco Unified Communications Manager requests the gateway to start media forking with a XMF media-forking request when the recording is triggered.

Recording related configuration for a SIP trunk is grouped in the **Recording Information** section on the **SIP trunk** page. To enable the SIP trunk for gateway recording, the administrator needs to check the checkbox **This trunk connects to a recording-enabled gateway**. To enable inter-cluster gateway recording for a SIP trunk, the administrator check the checkbox **This trunk connects to other clusters with recording-enabled gateways**.

Configure Recording Notification Tones

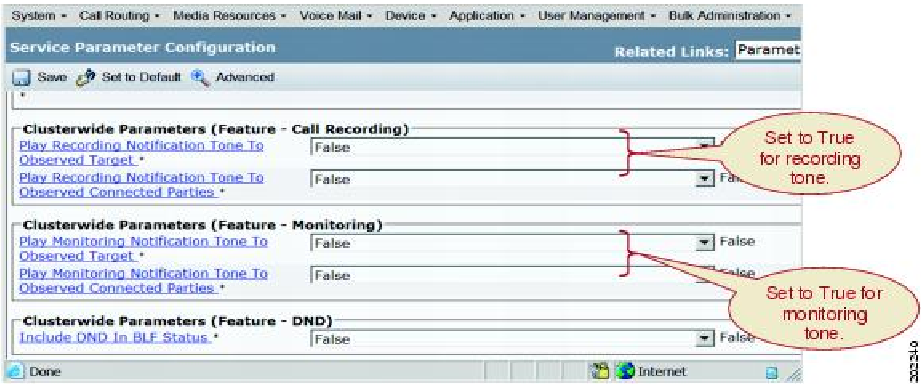
Set the service parameters for playing tone to **True** to allow tones to be played to the agent, the customer, or both.

CTI applications that initiates monitoring can also pass the play tone option to Cisco Unified Communications Manager. The recording tone plays when either the service parameter or the CTI application specifies the play tone option.

Use the **System** > **Service Parameters** menu option in Cisco Unified Communications Manager Administration to perform the necessary configuration.

Figure 115: Using Service Parameters to Configure Tones

The following figure illustrates using service parameters to configure tones.


System ▾ Call Routing ▾ Media Resources ▾ Voice Mail ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾
Service Parameter Configuration
Related Links: Paramet
Save
Set to Default
Advanced
Done
Internet
202340

Clusterwide Parameters (Feature - Call Recording)
Play Recording Notification Tone To Observed Target * False
Play Recording Notification Tone To Observed Connected Parties * False

Clusterwide Parameters (Feature - Monitoring)
Play Monitoring Notification Tone To Observed Target * False
Play Monitoring Notification Tone To Observed Connected Parties * False

Clusterwide Parameters (Feature - DND)
Include DND In BLF Status * False

Set to True for recording tone.

Set to True for monitoring tone.

Set the Recording Service Parameters

This section describes the service parameters that are related to the call recording feature.

Notification

The following service parameters affect the playing of notification tones to the parties in the call being recorded by the call recording feature:

Clusterwide Parameters (Feature - Call Recording)

- Play Recording Notification Tone To Observed Target
- Play Recording Notification Tone To Observed Connected Parties

The default value for these service parameters is **False**. You must change the value of each parameter to **True** to enable the particular notification tone to play.

Built-In-Bridge

The following service parameter enables or disables the built-in bridge on phones:

Clusterwide Parameters (Device - Phone)

Built-in Bridge Enable

For more information about this service parameter, see "Turn on IP phone BIB to allow Monitoring".

Simultaneous Monitoring and Recording

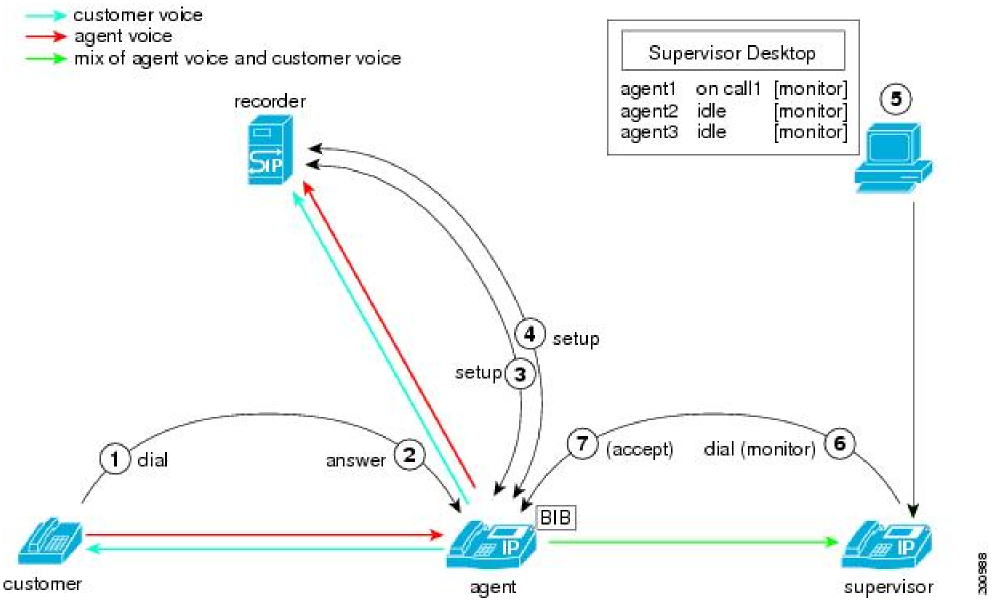
Note Recording a monitored call transferred or redirected across a cluster fails, as the DN information is not passed across the cluster for monitoring.

Recording can take place when the agent call is being monitored.

Recording and monitoring get set up independently from each other

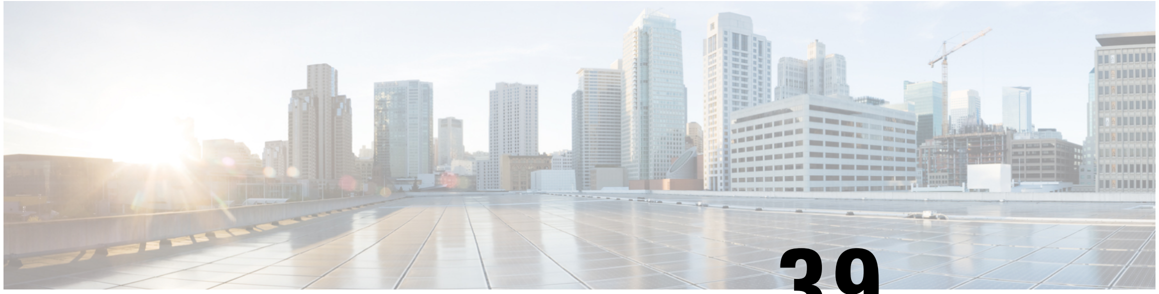
The following figure illustrates simultaneous monitoring and recording.

Figure 116: Simultaneous Monitoring and Recording



In the case of simultaneous monitoring and recording, the following steps take place:

1. A customer calls into the call center.
2. The call routes to agent. Agent answers the call. A two-way media streaming gets set up between agent IP phone and the customer.
3. The recording call for the agent voice gets set up between agent phone and the recorder.
4. The recording call for the customer voice gets set up between agent phone and the recorder.
5. The supervisor desktop application shows that agent has an active call. On his desktop application, the supervisor clicks the monitor button for current active call of agent.
6. The supervisor IP phone gets triggered to go off hook and make a monitoring call toward agent.
7. Agent phone accepts the monitoring call. Agent phone starts to send a stream of mixed voices of the customer and the agent to the supervisor IP phone. Neither the agent nor the customer can hear the supervisor.



CHAPTER 39

Multilevel Precedence and Preemption

This chapter provides information about the Multilevel Precedence and Preemption (MLPP) service which allows properly validated users to place priority calls. If necessary, users can preempt lower priority phone calls.

Precedence designates the priority level that is associated with a call. Preemption designates the process of terminating lower precedence calls that are currently using the target device, so a call of higher precedence can be extended to or through the device.

An authenticated user can preempt calls either to targeted stations or through fully subscribed time-division-multiplexing (TDM) trunks. This capability assures high-ranking personnel of communication to critical organizations and personnel during network stress situations, such as a national emergency or degraded network situations.

Configure MLPP

The Multilevel Precedence and Preemption (MLPP) service allows properly validated users to place priority calls. If necessary, users can preempt lower priority phone calls.

Precedence designates the priority level that is associated with a call. Preemption designates the process of terminating lower precedence calls that are currently using the target device, so a call of higher precedence can be extended to or through the device.

An authenticated user can preempt calls either to targeted stations or through fully subscribed time-division-multiplexing (TDM) trunks. This capability assures high-ranking personnel of communication to critical organizations and personnel during network stress situations, such as a national emergency or degraded network situations.

Perform the following steps to configure MLPP.

Procedure

Step 1 Configure MLPP Domains, Resource Priority Namespace Network Domain, and Resource Priority Namespace Network Domain List.

Step 2 Configure a common device configuration for which associated devices can make MLPP calls.

Step 3 Set enterprise parameters to enable MLPP indication and preemption. If individual devices and devices in common device configurations have MLPP settings of Default, the MLLP-related enterprise parameters apply to these devices and common device configurations.

Step 4 Configure partitions and Calling Search Spaces (CSS) that allow users (calling parties and their associated devices) to place precedence calls that use MLPP.

Not applicable for Assured Services phones

Step 5 Configure route patterns/hunt pilots that specify MLPP precedence level and route options for MLPP calls.

Not applicable for Assured Services phones

Step 6 Configure translation patterns that specify MLPP precedence level and route options for MLPP calls.

Not applicable for Assured Services phones

Step 7 Configure gateways that specify an MLPP domain for MLPP calls. The following gateway types apply:

- Cisco Catalyst 6000 24 port FXS Gateway
- Cisco Catalyst 6000 E1 VoIP Gateway
- Cisco Catalyst 6000 T1 VoIP Gateway
- Cisco DE-30+ Gateway
- Cisco DT-24+ Gateway
- H.323 Gateway

Note Some gateway types allow configuration of MLPP Indication and MLPP Preemption settings.

Step 8 Configure Cisco Unified IP Phones that specify an MLPP domain for MLPP calls.

Note Some phone types allow configuration of MLPP Indication and MLPP Preemption settings.

Step 9 Configure the directory number that will place an MLPP call.

Step 10 Configure the User Device Profile of the user that will make an MLPP call.

Step 11 Configure the Device Profile Default for devices that will make MLPP calls.

Step 12 Notify users that the MLPP service is available.

Related Topics

Multilevel Precedence and Preemption, on page 907

Set the Enterprise Parameters for MLPP, on page 964

MLPP Feature

The Multilevel Precedence and Preemption (MLPP) service allows placement of priority calls. Properly validated users can preempt lower priority phone calls with higher priority calls. An authenticated user can preempt calls either to targeted stations or through fully subscribed TDM trunks. This capability assures high-ranking personnel of communication to critical organizations and personnel during network stress situations, such as a national emergency or degraded network situations.

Note Only SCCP phones support the Multilevel Precedence and Preemption (MLPP) feature. SIP phones do not support MLPP.

MLPP configuration and operation is slightly different for Assured Services SIP (AS-SIP) endpoints than for other MLPP endpoint devices. AS-SIP endpoints deliver the precedence level to the Unified CM via the resource-priority header. Other MLPP endpoints use the dialed number pattern to indicate the precedence level. Many examples throughout this chapter illustrate the use of MLPP using the dialed number to signal precedence. Please refer to the Assured Services SIP Endpoint section for an understanding of how these endpoints differ in their operation and configuration.

Related Topics

MLPP Terminology, on page 910
Precedence, on page 910
Executive Override Precedence Level, on page 911
Preemption, on page 913
Domain, on page 914
Resource Priority Namespace Network Domain, on page 914
Resource Priority Namespace Network Domain List, on page 915
Location-Based MLPP, on page 916
MLPP Over Intercluster Trunks, on page 919
MLPP Precedence Patterns, on page 919
MLPP Indication Enabled, on page 920
Precedence Call Setup, on page 920
Alternate Party Diversion, on page 921
MLPP Preemption Enabled, on page 922
Preemption Details, on page 923
MLPP Announcements, on page 943
MLPP Numbering Plan Access Control for Precedence Patterns, on page 946
MLPP Trunk Selection, on page 947
MLPP Hierarchical Configuration, on page 949
Service Parameter Special Trace Configuration, on page 950
CDR Recording for Precedence Calls, on page 950
Line Feature Interaction, on page 951
Call Preservation, on page 952
Automated Alternate Routing, on page 952
MGCP and PRI Protocol, on page 953
Secure Endpoints and Secure Communications, on page 953
Map MLPP Precedence to DSCP Values, on page 953

MLPP Terminology

The following terms apply to the MLPP service:

- Call - A voice, video, or data connection between two or more users or network entities that is achieved by dialing digits or otherwise routing to a destination according to a predefined dialing plan.
- Precedence - Priority level that is associated with a call.
- Preemption - Process that terminates existing calls of lower precedence and extends a call of higher precedence to or through that target device.
- Precedence call - A call with precedence level that is higher than the lowest level of precedence.
- MLPP call - A call that has a precedence level established and is either being set up (that is, before alerting) or is set up.
- Active call - A call that has the connection established and the calling and called parties are active on the call.
- MLPP domain ID - Specifies the collection of devices and resources that are associated with an MLPP subscriber. When an MLPP subscriber that belongs to a particular domain places a precedence call to another MLPP subscriber that belongs to the same domain, MLPP service can preempt the existing call that the called MLPP subscriber is on for a higher precedence call. MLPP service availability does not go across different domains.
- Resource Priority Namespace Network Domain - Specifies SIP trunk behavior in the case of a precedence call and can preempt an existing call.The Resource Priority Namespace Network Domain in SIP signaling is similar to the ISDN precedence Information Element (IE) and ISDN User Part (ISUP) precedence parameters used in legacy TDM MLPP networks. The Resource Priority Namespace Network Domain is included on outbound calls and based on translation patterns or route patterns directing the call to the SIP trunk. For incoming calls the network domain is validated against the Resource Priority Namespace Network Domain List. If the network domain is not on the list, the call is rejected and a 417 message (unrecognizable) is returned.
- Resource Priority Namespace Network Domain List - Specifies a list of configured Resource Priority Namespace Network Domains for validating incoming calls.
- MLPP Indication Enabled device - In Cisco Unified Communications Manager, a device for which the device and Cisco Unified Communications Manager support precedence and preemption signaling procedures in the device control protocol and that is configured as such in the Cisco Unified Communications Manager system.
- MLPP Preemption Enabled device - In Cisco Unified Communications Manager, a device for which the device and Cisco Unified Communications Manager support preemption signaling procedures in the device control protocol and that is configured as such in the Cisco Unified Communications Manager system. Cisco Unified Communications Manager can initiate preemption on this interface.

Precedence

Precedence indicates the priority level that is associated with a call. Precedence assignment represents an ad hoc action in that the user may choose to apply or not to apply a precedence level to a call attempt. MLPP precedence does not relate to call admission control or enhanced emergency services (E911). Dedicated dial patterns in Cisco Unified Communications Manager Administration allow users to initiate an MLPP request.

Configuration of the calling search space(s) (CSS) that is associated with the calling party (device, line, and so forth) controls the ability of a calling party to dial a precedence pattern to attempt to originate a precedence call.

The Defense Switched Network (DSN) and the Defense Red Switched Network (DRSN) designate the target system for initial MLPP deployment. You generally can apply mechanisms for assigning precedence levels to calls, however, in Cisco Unified Communications Manager Administration to any dial plan by defining precedence dial patterns and calling search spaces that allow or restrict access to these patterns. In the DSN, a dial plan gets defined such that a precedence call is requested by using the string prefix NP, where P specifies the requested precedence level and N specifies the preconfigured MLPP access digit. Precedence priorities are as follows.

- Executive Override
- Flash Override
- Flash
- Immediate
- Priority
- Routine

Without specific invocation of precedence, the system processes a call by using normal call processing and call forwarding.

When a user profile is assigned to a phone, either as a default assignment or through extension mobility, the phone inherits the configuration of the assigned user, including any CSS that is associated with the user. The phone CSS can, however, override the user profile. Cisco Unified Communications Manager assigns the precedence level that is associated with the dialed pattern to the call when a pattern match occurs. The system sets the call request as a precedence call with the assigned precedence level.

When a precedence call is offered to a destination, Cisco Unified Communications Manager provides precedence indications to the source and destination of a precedence call, respectively, if either is MLPP Indication Enabled. For the source, this indication comprises a precedence ringback tone and display of the precedence level/domain of the call, if the device supports display. For the destination, the indication comprises a precedence ringer and display of the precedence level/domain of the call, if the device supports display.

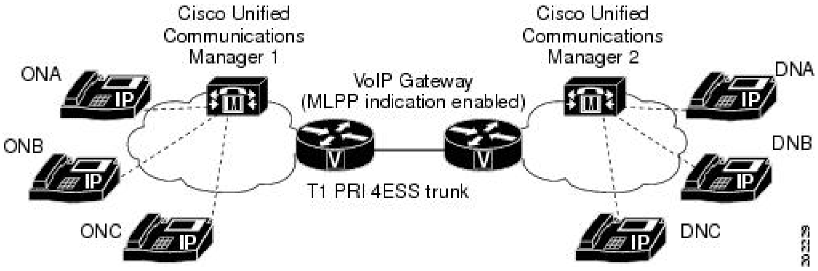
Executive Override Precedence Level

The highest precedence level specifies the Executive Override precedence level. When the Executive Override precedence level preempts a lower precedence call, the Executive Override call can change its precedence level to Flash Override (next highest level), so a subsequent Executive Override call can preempt the first precedence call.

Preempting an Executive Override precedence call requires that the Executive Override Call Preemptable service parameter be set to True. If the service parameter is set to False, an Executive Override precedence call keeps its precedence level and cannot be preempted.

The following figure shows an example of two Executive Override precedence calls, one that can be preempted, and one that cannot be preempted.

Figure 117: Executive Override Precedence Calls Example


Cisco Unified Communications Manager 1
Cisco Unified Communications Manager 2
ONA
ONB
ONC
DNA
DNB
DNC
VoIP Gateway (MLPP indication enabled)
T1 PRI 4ESS trunk
IP
M
V

In the example, in Cisco Unified Communications Manager installation 1, the Executive Override Call Preemptable service parameter specifies False, whereas in Cisco Unified Communications Manager installation 2, the Executive Override Call Preemptable service parameter specifies True.

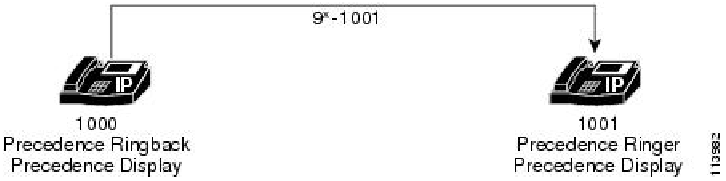
In the example, ONA makes an Executive Override precedence call to DNA from installation 1 to installation 2 through the T1 PRI 4ESS trunk. DNA answers, and the call connects.

In installation 1, if ONB tries to call ONA by placing an Executive Override precedence call, ONB receives a Blocked Precedence Announcement (BPA) because Executive Override calls cannot be preempted in installation 1. If ONB calls DNA by placing an Executive Override precedence call, the call between ONA and DNA gets preempted because Executive Override calls can be preempted in installation 2. Likewise, if DNB calls DNA by placing an Executive Override precedence call, the subsequent Executive Override precedence call preempts the call between ONA and DNA.

Executive Override Precedence Call Setup

The following figure shows an example of the events that take place when an Executive Override precedence call gets placed.

Figure 118: Executive Override Precedence Call Setup



In the example, phone 1000 goes off hook and dials 9*1001. (Route pattern 9*XXXX setting specifies Executive Override.)

For the source, if this precedence call succeeds, Cisco Unified Communications Manager signals Cisco Unified IP Phone to play a ringback tone to the user. If Cisco Unified IP Phone 1000 is MLPP Indication Enabled, precedence ringback tone plays. Otherwise, normal ringback tone plays.

If the precedence call cannot connect, a Blocked Precedence Announcement (BPA) plays if Cisco Unified IP Phone 1000 is MLPP Indication Enabled. Otherwise, a normal reorder tone plays.

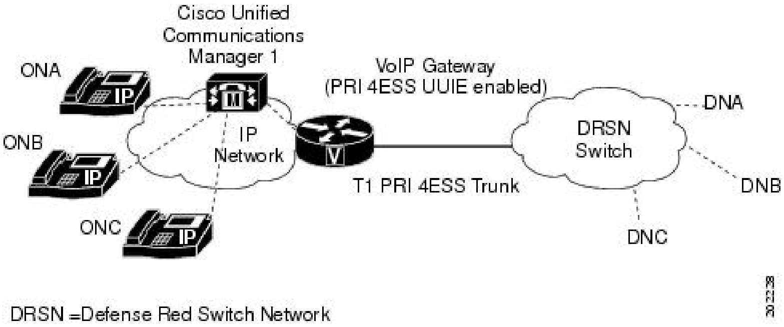
For the destination, if the Executive Override precedence call gets offered to Cisco Unified IP Phone 1001 successfully, Cisco Unified Communications Manager signals the destination to generate an audible ringer at the device. If Cisco Unified IP Phone 1001 is MLPP Indication Enabled, a precedence ring plays. Otherwise, a normal ring plays.

Also, Cisco Unified IP Phone 1001 displays precedence information (such as the Flash Override precedence call icon) if phone 1001 is MLPP Indication Enabled. Otherwise, no precedence information displays.

Executive Override Precedence Calls Across the PRI 4ESS Interface

The following figure shows an example of an Executive Override precedence call across the PRI 4ESS interface.

Figure 119: Executive Override Precedence Call Across the PRI 4ESS Interface


Cisco Unified Communications Manager 1
ONA
ONB
ONC
IP
IP Network
VoIP Gateway (PRI 4ESS UUIE enabled)
V
T1 PRI 4ESS Trunk
DRSN Switch
DNA
DNB
DNC
DRSN =Defense Red Switch Network
202238

Cisco Unified Communications Manager processes Executive Override precedence calls across the PRI 4ESS interface by using the same method that it uses to process other precedence calls, except that the precedence level passes through PRI 4ESS UUIE.

The precedence information through UUIE gets passed only when User-to-User IE Status on the Service Parameter Configuration window is True and Passing Precedence Level Through UUIE gets selected on the Gateway Configuration window.

PRI 4ES UUIE-Based MLPP Interface to DRSN

Cisco Unified Communications Manager now supports passing the MLPP information through the PRI 4ESS UUIE field. A previous release of Cisco Unified Communications Manager offered MLPP for PRI interface that was developed according to the ANSI T1.619a specification to connect with Defense Switched Network (DSN) switches. Defense Red Switch Network (DRSN) switches do not support ANSI T1.619a-based MLPP but do support MLPP over the PRI 4ESS interface by using the UUIE.

Preemption

The preemption process terminates lower precedence calls that are currently using the target device, so a call of higher precedence can be extended to or through the device. Preemption includes the notification and acknowledgement of preempted users and the reservation of shared resources immediately after preemption and prior to call termination. Preemption can take one of the following forms, depending on which method is invoked:

- User Access Channel Preemption - This type of preemption applies to phones and other end-user devices. In this type of preemption, if a called user access channel needs to be preempted, both the called party and the parties to which it is connected receive preemption notification, and the existing MLPP call gets cleared immediately. The called party must acknowledge the preemption before the higher precedence call completes. The called party then gets offered the new MLPP call. If the called party does not acknowledge the preemption, the higher precedence call does proceed after 30 seconds.

- Common Network Facility Preemption - This type of preemption applies to trunks. This type of preemption means that the network resource is busy with calls, some of which are of lower precedence than the call that the calling party requests. One or more of these lower precedence calls gets preempted to complete the higher precedence call.

Note Ensure that all devices that a call uses to preempt an existing call are preemption enabled. Because it is not sufficient for the calling and called devices (phone) to be preemption enable, ensure that the gateways that are used for the call also are preemption enabled.

Domain

An MLPP domain specifies a collection of devices and resources that are associated with an MLPP subscriber. When an MLPP subscriber that belongs to a particular domain places a precedence call to another MLPP subscriber that belongs to the same domain, MLPP service can preempt the existing call that the called MLPP subscriber is on for a higher precedence call. MLPP service availability does not go across different domains.

The MLPP domain subscription of the originating user determines the domain of the call and its connections. Only higher precedence calls in one domain can preempt connections that calls in the same domain are using.

Administrators enter domains in Cisco Unified Communications Manager Administration as hexadecimal values of zero or greater.

Resource Priority Namespace Network Domain

The Resource Priority Namespace Network Domain enables the configuration of namespace domains for a Voice over Secured IP (VoSIP) network that uses SIP trunks. Cisco Unified Communications Manager prioritizes the SIP-signaled resources so that those resources can be used most effectively during emergencies and congestion of telephone circuits, IP bandwidth, and gateways. Endpoints receive the precedence and preemption information. It is based on RFC 4411 and RFC 4412.

The SIP signaling contains a resource-priority header. The resource-priority header is similar to the ISDN precedence Information Element (IE) and ISDN User Part (ISUP) precedence parameters used in legacy TDM MLPP networks. The resource-priority header is related to, but is different from the priority header in RFC 3261, Section 20.26.

The RFC 3261 priority header indicates the importance of SIP requests for the endpoint. For example, the header could indicate decisions about call routing to mobile devices and assistants and about call acceptance when the call destination is busy. The RFC 3261 priority header does not affect the usage of PSTN gateway or proxy resources.

In the RFC 3261 priority header, any value could be asserted but the Resource Priority header field in the namespace network domain is subject to authorization. The Resource Priority header field does not directly influence the forwarding behavior of IP routers or the use of communications resources such as packet forwarding priority.

The RFC 4411 and RFC 4412 resource-priority header in the outbound message is based on the translation or route patterns directing a call to the SIP trunk. Incoming calls are validated against a list of Resource Priority Namespace Network Domains if the calls are terminating to an endpoint configured in the Cisco Unified Communications Manager Administration.

The following messages include the Resource Priority header:

- INVITE
- UPDATE
- REFER

The following is an example of an INVITE message that has an resource priority header that specifies immediate priority (value of 4).

```
INVITE sip:6000@10.18.154.36:5060 SIP/2.0Via: SIP/2.0/TCP 10.18.154.44;
branch=z9hG4bK1636ee4aRemote-Party-ID: “Raleigh - 5001" <sip:5001@10.18.154.44>;
party=calling;screen=yes;privacy=offFrom: “Raleigh - 5001" <sip:5001@10.18.154.44>;
tag=936ad6ec-4d3c-4a42-a812-99ac56d972e1-14875646To: <sip:6000@10.18.154.36>Date: Mon,
21 Mar 2005 14:39:21 GMTCall-ID: 1d13800-23e1dc99-4c-2c9a12ac@172.18.154.44Supported:
100rel,timer,replacesRequire: resource-priorityMin-SE:  1800User-Agent: Cisco-CCM5.0Allow:

INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFYCSeq:
101 INVITEContact: <sip:5001@10.18.154.44:5060;transport=tcp>Expires: 180Allow-Events:
presence, dialog, kpmlCall-Info:<sip:10.18.154.44:5060>;
method=”NOTIFY;Event=telephone-event;Duration=500”Resource-Priority:
namespace.4Max-Forwards: 70Content-Type: application/sdpContent-Length:
269v=0o=CiscoSystemsCCM-SIP 2000 1 IN IP4 10.18.154.44s=SIP Callc=IN IP4 10.18.154.45t=0
0m=audio 19580 RTP/AVP 0 101a=rtpmap:0 PCMU/8000a=ptime:20a=rtpmap:
101 telephone-event/8000a=fmtp:101 0-15
```

You can also add a default Resource Priority Namespace Network Domain to a SIP Profile to use when handling misconfigured incoming namespace network domains.

Note Digit analysis of translation and route patterns is supported.

The following supplementary services are supported:

- Precedence Call Waiting
- Call Transfer
- Call Forwarding
- Three-way Calling

The following headers, mapping, and queuing are not supported:

- Accept-Resource-Priority header.
- Inclusion of RP header in PRACK and ACK.
- Mapping of precedence levels between namespaces.
- Call queuing and other non-MLPP services.

Resource Priority Namespace Network Domain List

The Resource Priority Namespace Network Domain List contains acceptable network domains and is added to the SIP Profile. Incoming calls are compared to the list and processed if an acceptable network domain is in the list. If the incoming call is not valid, the call is rejected and an error response of 417 (Unknown) is sent to the calling party.

Location-Based MLPP

Cisco Unified Communications Manager supports MLPP on Skinny Client Control Protocol phones and TDM (PRI/CAS) trunks. Cisco Unified Communications Manager also supports MLPP on wide-area network (WAN) links. Location-based call admission control (CAC) manages WAN link bandwidth in Cisco Unified Communications Manager. Enhanced locations take into account the precedence level of calls and preempt calls of lower precedence when necessary to accommodate higher precedence calls.

Enhancing locations mean that, when a precedence call arrives and not enough bandwidth can be found to connect the call to the destination location, Cisco Unified Communications Manager finds the call or calls with the lowest precedence level and preempts the call(s) to make sufficient bandwidth available for a higher precedence call. If the bandwidth requirement still cannot be satisfied after going through the preemption procedure, the newly placed call fails.

Precedence-Based MLPP Preemption

Prior to release 8.6, Cisco Unified Communications Manager randomly chose calls to preempt that had lower precedence levels than the new request. If there are two existing calls with precedence levels of Routine and Priority and a Flash call comes in for that location, Cisco Unified Communications Manager might preempt the Routine call or the Priority call. With release 8.6 and later, Cisco Unified Communications Manager always preempts the Routine call before the Priority call.

Configuration of Nonpreemptable Numbers

With Release 10.0 and later it is possible to designate specific dialed numbers as nonpreemeptable.

To configure nonpreemptable numbers, create the transformation patterns with the MLPP Preemption Disabled check box checked and put them into partitions, import all such partitions into a CSS (for example, NonPreemptionCSS), and select the CSS in "Non-Preemption Pattern CSS" service parameter **(System > Service Parameters)**.

Note For Location based MLPP to work, you need to select the **MLPP Exception Level** service parameter.

The following are limitations to the nonpreemptable number feature:

- For the nonpreemptable feature to work as expected in intercluster scenarios you must configure the same nonpreemptable numbers across all clusters. The nonpreemptable status is not signaled between CallManagers in different clusters.
- In scenarios where incoming calls arrive via a MGCP T1 CAS trunk the calling party number is not available to Cisco Unified Communications Manager. Therefore, the calling party number cannot be checked for nonpreemptability.
- In MGCP FXO scenarios, the calling party number information is provided to Cisco Unified Communications Manager after the call routing process begins. Therefore, the calling party number cannot be checked for nonpreemptability
- In an Overlap Sending scenario only a few digits are collected before gateway selection occurs. All the remaining digits dialed are sent across the gateway for processing. Therefore Cisco Unified Communications Manager does not know the complete number that is dialed and can not check for the nonpreemptable status of the called party number.

CAC Call-State-Based MLPP Preemption

If two calls are in the same location, have the same precedence level, and are using the same media type (audio or video), Cisco Unified Communications Manager preempts the call that is in setup phase before selecting the call that has already completed.

Because location CAC counts bandwidth, when media is established, the bandwidth is being used, therefore, Cisco Unified Communications Manager considers the call setup to be completed.

Minimize Number of Calls to Preempt

For calls with the same precedence level, call state, and that use the same media type (audio or video), Cisco Unified Communications Manager attempts to minimize the number of calls to be preempted; that is, Cisco Unified Communications Manager selects a call with larger bandwidth, rather than several calls with less bandwidth.

Note Cisco Unified Communications Manager always preempts calls with lower precedence levels if a call with a higher precedence level gets selected. This rule applies even when the higher precedence call can satisfy the required bandwidth.

Because each call connects two devices in different locations, each location could result in calls to be preempted. For example, in one location, a Flash call could be preempted while a Priority call is not preempted in the other location. For examples of preemption calls, see the Location-Based Preemption, on page 926.

Preempt Video Calls When Allocating or Adjusting Bandwidth

Cisco Unified Communications Manager 8.6(1) and later preempts lower precedence video calls when allocating or adjusting video bandwidth for high priority calls if there is not enough bandwidth for the new request. When preempting a video call, Cisco Unified Communications Manager clears the call and plays a preemption tone to the party that is preempted.

Preempt Bandwidth Allocated for Annunciator or Music On Hold

Cisco Unified Communications Manager 8.6(1) and later preempts the bandwidth that is allocated for Annunciator and Music On Hold (MOH) when preempting calls. If media resource bandwidth is needed for a higher priority call, an entire call is cleared, rather than simply removing the Annunciator or MOH. When Annunciator or MOH is inserted into a call, such as to play music on hold or a ringback for MLPP Calls, preemption, or reorder tone, the media is streaming; therefore, Cisco Unified Communications Manager considers the call connected and preempts the call after all alerting calls with the same precedence level. However, when Annunciator or MOH is requested but not enough bandwidth is available at neither the media user location or the media resource location, the request for Annunciator or MOH fails and Cisco Unified Communications Manager does not preempt other calls for Annunciator or MOH.

As with all preempted calls, the bandwidth that is allocated for those calls is immediately released and then allocated for another call. When Annunciator is played for preemption tone, or any other tone that causes a call to disconnect, the tone continues to play for a short while even though the bandwidth has already released. That is, when Cisco Unified Communications Manager selects an Annunciator tone to be used for a preemption or reorder tone, the bandwidth might be over-subscribed (over-budget) for a short while before the call is completely cleared.

Enforce Maximum Bandwidth

Cisco Unified Communications Manager 8.6(1) and later enforces configured maximum bandwidth for locations, which can result in calls being cleared when a call is resumed or transferred. In addition, multiple calls could be cleared when new bandwidth requests occur and the bandwidth is over-subscribed. To enforce maximum bandwidth for locations, the service parameters Locations-based Maximum Bandwidth Enforcement Level for MLPP Calls and Locations-based MLPP Enable must be set to Strict Enforcement.

When the value for the Locations-based Maximum Bandwidth Enforcement Level for MLPP Calls service parameter is changed from Lenient to Strict, the result could be more calls than the maximum bandwidth that is allowed. However, Cisco Unified Communications Manager does not immediately preempt calls to bring the bandwidth within the allowed budget, but rather, when new bandwidth is requested for the same type of audio or video call. When the preemption occurs, one possible result is a large amount of difference between bandwidth usage and the maximum allowed.

When handling preemption in over-subscription situations, Cisco Unified Communications Manager considers all existing calls, beginning with the lowest precedence level. Although this preemption is triggered by a bandwidth request, the preempted call could have a higher precedence level than the requesting call.

The service parameter Locations-based Maximum Bandwidth Enforcement Level for MLPP Calls determines whether to restrict the bandwidth usage for a location to be within its configured maximum.

For more information about service parameters, see Location-Based Preemption, on page 926 in the Cisco Unified Communications Manager Administration Guide.

Preempt Audio Calls When Adjusting Bandwidth

Cisco Unified Communications Manager adjusts bandwidth for audio calls when bandwidth usage is changed after a call is presented to the called party, as in the case of called party answer, shared line hold and resume, transfer, and other feature interactions. Cisco Unified Communications Manager attempts to preempt other calls, if possible, but allows the new bandwidth request to proceed even when there is not enough bandwidth for the call to be preempted.

Note If the service parameter Enforce Maximum Bandwidth for MLPP is set to True, the bandwidth request fails, which causes the call to be cleared. The requesting call is cleared as if it is preempted as any other location preemption with the same cause code and preemption tone.

Update Bandwidth After Joining Call Legs

Prior to Cisco Unified Communications Manager 8.6(1), real bandwidth usage was not reflected accurately. For example, when user B transferred user A and user C, the bandwidth that was reserved for the primary call (A and B) was allocated but the bandwidth reserved for the secondary call (B and C) was released.

Cisco Unified Communications Manager 8.6(1) and later updates bandwidth immediately after the Join operation, which reflects the correct bandwidth usage for calls. Updating bandwidth preserves the existing bandwidth that has been allocated to the two call legs. Once the media has connected, Cisco Unified Communications Manager adjusts to the correct bandwidth usage. That is, when the bandwidth is updated after the Join operation, one side of the call leg could have a bandwidth reservation for video and the other side for audio, which results in a call with two types of bandwidth reservation; however, the bandwidth is adjusted to the correct usage after the media connects.

Note Because the update for bandwidth does not request additional bandwidth in either location, Cisco Unified Communications Manager does not preempt any calls.

Update Bandwidth When Redirecting a Call

This section provides examples that describe how bandwidth is reserved when redirecting a calling party and a called party to a new destination.

Redirect Calling Party to New Destination

When Cisco Unified Communications Manager redirects a calling party to a new destination, the bandwidth reserved for IP phone B is released when Cisco Unified Communications Manager attempts to reserve bandwidth for IP phone C.

If a reservation failure occurs for IP phone C, the bandwidth for IP phone B reallocated. If the A to B call is restored, as in the case of an divert failure, the bandwidth for the A to B call is reflected correctly.

If the A to B call is not restored, as in the case of a CFNA failure, the bandwidth for both IP phone A and IP phone B remains allocated even though IP phone B has stopped ringing. Bandwidth for both phones is released when IP Phone A disconnects the call.

Redirect Called Party to New Destination

When redirecting a called party, Cisco Unified Communications Manager reserves double bandwidth for the original called party before ringing the new destination. If there is not enough bandwidth for the doubled reservation, the redirect operation fails. In Cisco Unified Communications Manager 8.6(1) and later, Cisco Unified Communications Manager reuses the original called party’s bandwidth reservation (IP phone B) when reserving bandwidth for the new called party. However, for the redirect action to be successful, if IP phone A and IP phone D are in the same location, Cisco Unified Communications Manager requires bandwidth for both phones.

If the reservation for the new destination for Phone D fails, the existing bandwidth reserved for the original called party is reallocated. When the call for the original called and calling party is restored, the bandwidth reservation for the calling party and the original called party remains.

If the reservation for the e new destination fails and the original A to B call is not restored, the bandwidth for both IP phone A and IP phone B is released.

MLPP Over Intercluster Trunks

Cisco Unified Communications Manager supports MLPP precedence and preemption over intercluster trunks. Dialed digits communicate the precedence level. The location call admission control mechanism controls preemption. Announcements and MLPP cause codes also become available across intercluster trunks.

MLPP Precedence Patterns

To set up MLPP precedence patterns, access the Translation Pattern Configuration window in Cisco Unified Communications Manager Administration where the following MLPP precedence patterns are available:

- Executive override (highest)

- Flash override
- Flash
- Immediate
- Priority
- Routine (lowest)
- Default (means precedence level does not get changed)

See the *Cisco Unified Communications Manager Administration Guide* for details.

MLPP Indication Enabled

MLPP indication-enabled devices include the following characteristics:

- MLPP indication-enabled devices can play preemption tones.
- MLPP indication-enabled devices can receive MLPP preemption announcements that the announcement server generates.
- MLPP indication-enabled devices can receive preemption.

To set up devices to enable MLPP indication, use the configuration window for each respective device. In the MLPP Indication field of each device, set the value to On.

See the *Cisco Unified Communications Manager Administration Guide* for details of setting MLPP indication for devices.

Precedence Call Setup

The following sequence of events takes place during setup of a precedence call:

1. User goes off hook and dials a precedence call. The call pattern specifies NP-XXX, where N specifies the precedence access digit and P specifies the precedence level for the call.
2. The calling party receives the special precedence ringback and a precedence display while the call is processing.
3. The called party receives the special precedence ringer and a precedence display that indicates the precedence call.

Example

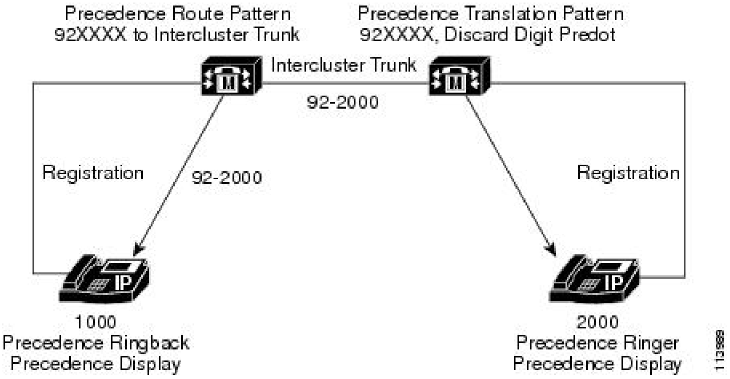
Party 1000 makes a precedence call to party 1001. To do so, party 1000 dials the precedence call pattern, such as 90-1001.

While the call processes, the calling party receives precedence ringback and precedence display on the calling Cisco Unified IP Phone. After acknowledging the precedence call, the called party receives a precedence ringer (receives a special ring) and a precedence display on the called Cisco Unified IP Phone.

Precedence Call Setup Across Intercluster Trunks

The following figure shows an example of a configuration that can be used to set up precedence calls over intercluster trunks. Because no precedence information element support exists over intercluster trunks, transmission of extra digits carries the precedence information. The dial plan must be set up appropriately on both clusters to accomplish transmission of the precedence information.

Figure 122: Precedence Call Setup Across Intercluster Trunks Example



In this example, 1000 dials 92-2000, which matches the appropriate precedence patterns on both clusters and sets up the precedence call.

Alternate Party Diversion

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 setting for precedence calls.

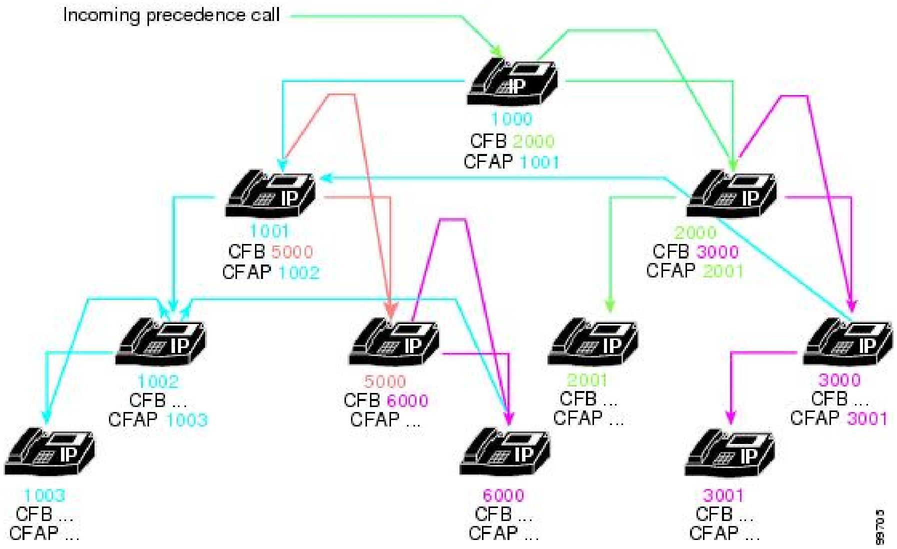
Precedence calls do not normally forward to voice-messaging system, as controlled by the value of the Use Standard VM Handling For Precedence Calls enterprise parameter. See the Set the Enterprise Parameters for MLPP, on page 964 for details.

To set up APD, the administrator configures the Multilevel Precedence and Preemption Alternate Party Settings on the Directory Number Configuration window of the DN that is the target of an MLPP precedence call. See the *Cisco Unified Communications Manager Administration Guide* for details.

Example

The following figure illustrates the Alternate Party Diversion that takes place when a called party receives a precedence call and the party is configured for Alternate Party Diversion.

Figure 123: Alternate Party Diversion Example



In the example, a calling party placed a precedence call to party 1000. Called party 1000 has a Call Forward Busy (CFB) setting of 2000 and a Call Forward Alternate Party (CFAP) setting of 1001. The figure shows the CFB and CFAP settings for all other parties in this example.

When 1000 receives a precedence call but is busy, the call routes to party 2000. If party 2000 is also busy, the call routes to party 3000. If neither party 2000 nor party 3000 answers the call, however, the call routes to party 1001. That is, the call routes to the alternate party that is designated for the originally called party, not to the alternate parties that are designated for the Call Forward Busy parties that are associated with the originally called party.

Likewise, if party 1001 is busy and does not answer the call, the call forwards to party 5000. If party 5000 is busy, the call forwards to party 6000. If neither party 5000 nor party 6000 answers the call, however, the call forwards to the alternate party destination of party 1001, which is party 1002. If party 1002 is busy or does not answer, the call forwards to party 1003, which is the s alternate party designation of party 1002.

MLPP Preemption Enabled

Enable MLPP preemption by explicitly configuring preemption-capable devices for preemption.

Receive Preemption

A device that is preemption disabled (by setting the MLPP Preemption value to Disabled) can still receive precedence calls in an MLPP network, but the device itself does not get preempted. The preemption-disabled device can be connected to a call that gets preempted (at another device), in which case, the device receives preemption.

Preemption Enabled

Enable devices for preemption by setting the device MLPP Preemption value to either Forceful or Default. If the device MLPP Preemption value is set to Forceful, the system can preempt the device at its own interface. That is, the device can get preempted when a precedence call contends for the device resources.

If the device MLPP Preemption setting is Default, the device inherits its MLPP Preemption setting from its common device configuration. If the common device configuration MLPP Preemption setting for the device is Forceful, or if the common device configuration MLPP Preemption setting is also Default but the MLPP Preemption Setting enterprise parameter value is Forceful Preemption, the device inherits preemption enabling.

To set up devices to enable MLPP preemption, use the configuration window for each respective device. In the MLPP Preemption field of each device, set the value to Forceful or Default.

See the *Cisco Unified Communications Manager Administration Guide* for details of setting MLPP preemption for devices.

Preemption Details

The following types of preemption exist:

- User Access Preemption
- Common Network Facility Preemption
- Location-based Preemption

User Access Preemption

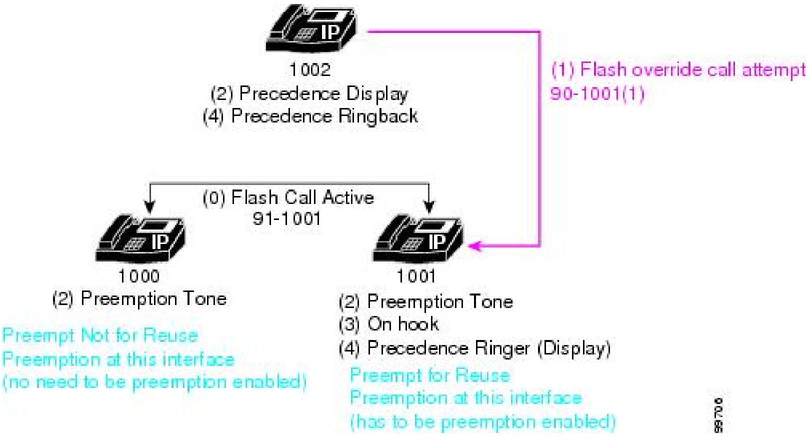
User access preemption takes place when a user places a precedence call to a user that is already active on a lower level precedence call. Both calls exist in the same MLPP domain. You can use this type of preemption for MLPP Indication Enabled phones that the Cisco Skinny Client Control Protocol controls in the Cisco Unified Communications Manager MLPP system. Preemption occurs if a precedence call request is validated and if the requested precedence of the call is greater than the precedence of an existing call that is connected at the destination MLPP Preemption Enabled phone. Call processing uses a preemption tone to notify the connected parties of the preemption and releases the active call. When the called party acknowledges the preemption by hanging up, the called party gets offered the new MLPP call.

To understand the sequence of steps that takes place during user access preemption, see the following example.

Example

The following figure illustrates an example of user access preemption.

Figure 124: User Access Preemption Example



In the example of user access preemption, the following sequence of events takes place:

1. User 1000 places a precedence call of precedence level flash override to user 1001, who answers the call. In this example, user 1000 dials 90-1001 to place the precedence call.
2. User 1002 places a precedence call to user 1001 by dialing 9*-1001. This call, which is of precedence level Executive Override, represents a higher precedence call than the active precedence call.
3. While the call is directed to user 1001, the calling party receives precedence display (that is, flash override display, not executive override display), and the parties who are involved in the existing lower precedence call both receive preemption tones.
4. To complete preemption, the parties who are involved in the lower precedence call (users 1000 and 1001) hang up.
5. The higher level precedence call gets offered to user 1001, who receives a precedence ringer. The calling party, user 1002, receives precedence ringback.

Distinct preemption types take place in this instance. For the party that is not the destination of the higher precedence call, Preemption Not for Reuse takes place. Because preemption is not taking place at this interface, this device does not need to be preemption enabled. For the party that is the destination of the higher precedence call, Preemption for Reuse takes place. Because preemption does take place at this interface, ensure that this device is preemption enabled.

User Access Channel Nonpreemptable

You can configure an end-user device as MLPP Indication Enabled but not MLPP Preemption Enabled. In this case, a phone that can generate MLPP indications (using special preemption tones and ringers) does not have preemption procedures that are supported in its device control protocol in Cisco Unified Communications Manager. The administrator can also disable preemption procedures for a phone even though Cisco Unified Communications Manager Administration supports the procedures.

Historically, user access devices (phones) have limited or no mechanisms for handling multiple, simultaneous calls. Even with the Call Waiting feature, many phones and associated switches do not have a mechanism to allow the user to manage multiple calls simultaneously on the same line.

Cisco Unified Communications Manager Administration effectively enhances the Call Waiting feature to provide this capability for users of Cisco Unified IP Phones 7940, 7942, 7945, 7960, 7962, 7965, and 7975). These Cisco Unified IP Phones include a user interface that gives the user adequate control of multiple, simultaneous calls when interfacing with the Cisco Unified Communications Manager system. This enhanced functionality allows the Call Waiting feature to be applied to all precedence calls that are directed to these types of phones, even though the user may already be managing other calls. When the user receives a precedence call, the user at a destination phone can decide what to do with any existing calls instead of merely releasing the lower precedence call. For users of these devices, the Cisco Unified Communications Manager administrator can configure devices as not MLPP Preemption Enabled to take advantage of this function in Cisco Unified Communications Manager.

Common Network Facility Preemption

Common network facility preemption applies to network resources, such as trunks, in the MLPP system. When a common network facility gets preempted, all existing parties receive notification of the preemption, and the existing connection immediately gets disconnected. The new call gets set up by using the preempted facility in the normal manner without any special notification to the new called party. PRI and T1-CAS trunks on targeted MGCP gateway platforms support this type of preemption in Cisco Unified Communications Manager.

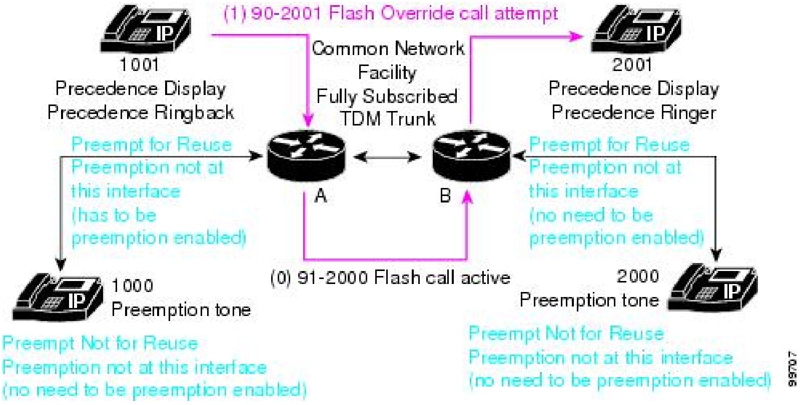
Preemption occurs if a precedence call request is validated and if the requested precedence of the call is greater than the precedence of an existing call through the destination MLPP Preemption Enabled trunk and the trunk is completely busy (that is, cannot handle any more calls). Call processing identifies a call with lower precedence, notifies the connected parties of the preemption for the PRI trunk interface, reserves the channel for subsequent use, and drops the selected lower precedence call. The system uses the reserved channel to establish the connection through the gateway for the precedence call that caused preemption.

For the sequence of steps that takes place during common network facility preemption, see the following examples.

Example 1

The following figure illustrates an example of common network facility preemption.

Figure 125: Common Network Facility Preemption Example



In the example of common network facility preemption, the following sequence of events takes place:

1. User 1000 places a precedence call of precedence level Flash Override to user 2000, who answers the call. In this example, user 1000 dials 90-2000 to place the precedence call. The flash call of precedence level Flash Override specifies active.

   The call uses a common network facility where the two gateways define a fully subscribed TDM trunk.

2. User 1001 next places a higher precedence (executive override) call to user 2001 by dialing 9*-2001. (Assume that the flash call represents the lowest precedence call over gateway A, and users 1000 and 1001 reside in the same MLPP domain.)

   Preemption occurs at gateway A, which is preempted for reuse. Because preemption occurs at this interface, you must ensure that this device is preemption enabled. Gateway B also gets preempted for reuse, but the preemption does not occur at this interface, so this device does not need to be preemption enabled.

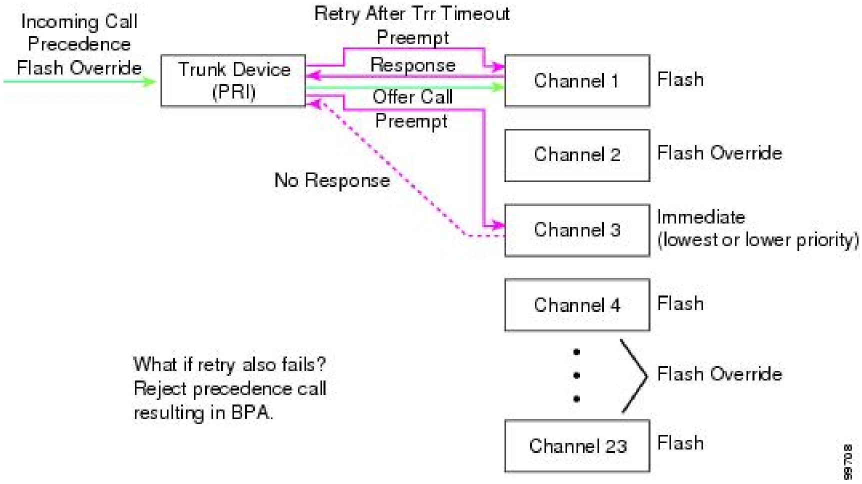
   Users 1000 and 2000 both receive preemption tones. Because both devices are not preempted for reuse and preemption does not occur at these interfaces, you do not need to ensure that these devices are preemption enabled for the preemption to occur.

In this example, almost all events occur instantly. Parties do not need to hang up for common network facility preemption to occur.

Example 2

The following figure illustrates an example of common network facility preemption with the retry timer Trr. The retry timer Trr provides a mechanism, so if preemption is not successful on one channel, preemption gets retried on another channel. This timer applies only to TDM trunks.

Figure 126: Common Network Facility Preemption Example with Retry Timer Trr



In the example of common network facility preemption with the retry timer Trr, the following sequence of events takes place:

1. An incoming call with Flash Override precedence arrives at a PRI trunk device.

   The incoming call causes preemption of channel 3, but a response does not occur within the time that the retry timer Trr specifies.

2. Retry timer Trr expires.

   Channel 3 gets preempted.

3. This preemption causes a response, and the precedence call gets offered on channel 1.

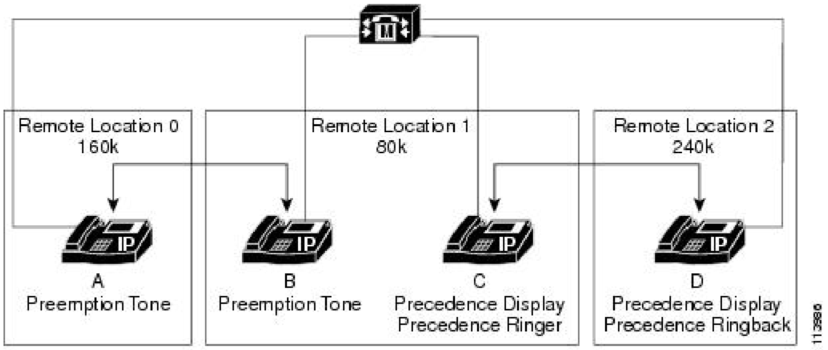
Location-Based Preemption

The following examples illustrate location-based preemption.

Example 1

In the example that follows, the new call and the location-preempted call take place in different devices. See the following figure for an example of this type of location-based preemption.

Figure 127: Location-Based Preemption in Different Devices



This example illustrates the location-based preemption scenario. In the example, three locations exist:

- Remote location 0 (RL0) with phone A and 160K of available bandwidth
- Remote location 1 (RL1) with phones B and C and 80K of available bandwidth
- Remote location 2 (RL2) with phone D and 240K of available bandwidth

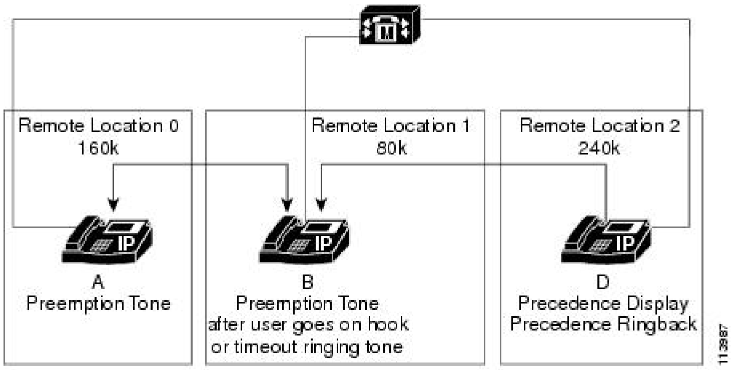
The following sequence of events takes place:

1. A places a call to B with Priority precedence level, and the call becomes active. The available bandwidth specifies 80K in RL0, 0K in RL1, and 240K in RL2.
2. D calls C with Immediate precedence level. The D call preempts the call between A and B because RL1 is out of bandwidth and D call has higher precedence.
3. The call between D and C completes. The available bandwidth specifies 160K in RL0, 0K in RL1, and 160K in RL2.

Example 2

In the example that follows, the new call and the location preempted call take place in the same device. See the following figure for an example of this type of location-based preemption.

Figure 128: Location-Based Preemption in the Same Device



This example illustrates the location-based preemption scenario. In the example, three locations exist:

- Remote location 0 (RL0) with phone A and 160K of available bandwidth
- Remote location 1 (RL1) with phone B and 80K of available bandwidth
- Remote location 2 (RL2) with phone D and 240K of available bandwidth

The following sequence of events takes place:

1. A places a call to B with Priority precedence level, and the call becomes active. The available bandwidth specifies 80K in RL0, 0K in RL1, and 240K in RL2.
2. D calls B with Immediate precedence level. D call preempts the call between A and B because RL1 is out of bandwidth and D call has higher precedence.
3. B receives the preemption tone first, and the End call softkey displays.
4. B presses the EndCall softkey, hangs up, or waits for timeout. The call from D to B gets offered to B. When the call from D to B completes, the available bandwidth specifies 160K in RL0, 0K in RL1, and 160K in RL2.

Example 3

The following example describes basic MLPP preemption on precedence level.

The following calls are present in a location:

Executive Override:

- Call 1 at 80 kbps
- Call 2 at 8 kbps

Flash Override:

- Call 3 at 8 kbps
- Call 4 at 8 kbps

Flash:

- Call5 at 8 kbps
- Call6 at 8 kbps

Immediate:

- Call 7 at 8 kbps
- Call 8 at 8 kbps

Priority:

- Call 9 at 8 kbps
- Call 10 at 8 kbps

Routine:

- Call 11 at 8 kbps

- Call 12 at 8 kbps

No more bandwidth is available at this location.

A new Executive Override call that requires 80 kbps bandwidth in this location is attempted. In this case, calls 3 through 12 are preempted.

Example 4

The following example describes how Cisco Unified Communications Manager preempts multiple lower priority calls and a single higher priority call.

The following calls are present in a location:

Executive Override:

- NA

Flash Override:

- NA

Flash:

- Call 1 at 80 kbps
- Call 2 at 8 kbps

Immediate:

- Call 3 at 8 kbps
- Call 4 at 8 kbps
- Call 5 at 8 kbps
- Call 6 at 8 kbps
- Call 7 at 8 kbps
- Call 8 at 8 kbps

Priority:

- Call 9 at 8 kbps
- Call 10 at 8 kbps

Routine:

- Call 11 at 8 kbps

No more bandwidth is available at this location.

A new Executive Override call that requires 80 kbps bandwidth in this location is attempted. In this case, Cisco Unified Communications Manager preempts calls 2 through 11 due to call 2 having sufficient bandwidth available, while call 1 has more than enough bandwidth.

Example 5

The following example describes how Cisco Unified Communications Manager preempts an Executive Override or lower priority call before other calls.

The following calls are present in a location:

Executive Override:

- Call 1 at 80 kbps
- Call 2 at 8 kbps

Flash Override:

- Call 3 at 80 kbps
- Call 4 at 8 kbps

Flash:

- Call 5 at 8 kbps
- Call 6 at 8 kbps

Immediate:

- Call 7 at 8 kbps
- Call 8 at 8 kbps

Priority:

- Call 9 at 8 kbps
- Call 10 at 8 kbps

Routine:

- Call 11 at 8 kbps

No more bandwidth is available at this location.

A new Executive Override call that requires 80 kbps bandwidth in this location is attempted. In this case, Cisco Unified Communications Manager preempts call 3 and calls 5 through 11.

Example 6

The following example describes how Cisco Unified Communications Manager preempts the maximum possible bandwidth with the minimum required amount.

The following calls are present in a location:

Flash:

- Call 3 at 80 kbps
- Call 4 at 8 kbps
- Call 5 at 8 kbps

- Call 6 at 8 kbps

No more bandwidth is available at this location.

A new Executive Override call that requires 8 kbps bandwidth in this location is attempted. In this case, Cisco Unified Communications Manager preempts one of calls 4, 5, or 6.

Example 7

The following example describes preemption due to precedence level.

Configuration

The total audio bandwidth in location (LOC-BR1) is 100 kbps

The region codec specifies a maximum audio bit rate as 64 kbps

IP phone A and IP phone B are in location Hub None and IP phone X and IP phone Y are in location LOC-BR1.

1. IP phone A (location Hub None) calls IP phone X (location LOC-BR1). The call is made with an Routine precedence level. Because sufficient audio bandwidth is available in LOC-BR1, the call begins alerting IP phone X and is answered.
2. IP phone B (location Hub None) calls IP phone Y (location LOC-BR1). The call is made with an Priority precedence level.
3. Because insufficient bandwidth is available to complete the second call and the second call is made at a higher priority than the first call, the first call is preempted.
4. The call between IP phone B and IP phone Y completes and the call between IP phone A and IP phone X is cleared.

Example 8

The following example describes no preemption for an Executive Override call.

Configuration

The total audio bandwidth in location (LOC-BR1) is 100 kbps

The region codec specifies a maximum audio bit rate as 64 kbps

The service parameter Executive Override Call Preemptable is set to False.

IP phone A and IP phone B are in location Hub None and IP phone X and IP phone Y are in location LOC-BR1.

1. IP phone A (location Hub None) calls IP phone X (location LOC-BR1). The call is made with an Executive Override precedence level. Because sufficient audio bandwidth is available in LOC-BR1, the call begins alerting IP phone X and is answered.
2. IP phone B (location Hub None) calls IP phone Y (location LOC-BR1). The call is made with an Executive Override precedence level.
3. Because insufficient bandwidth is available to complete the second call, it is rejected.
4. The call between IP phone B and IP phone Y is rejected.

Example 9

The following example describes the preemption for an Executive Override call.

Configuration

The total audio bandwidth in location (LOC-BR1) is 100 kbps

The region codec specifies a maximum audio bit rate as 64 kbps

The service parameter Executive Override Call Preemptable is set to True.

IP phone A and IP phone B are in location Hub None and IP phone X and IP phone Y are in location LOC-BR1.

1. IP phone A (location Hub None) calls IP phone X (location LOC-BR1). The call is made with an Executive Override precedence level. Because insufficient audio bandwidth is available in LOC-BR1, the call begins alerting IP phone X and is answered.
2. IP phone B (location Hub None) calls IP phone Y (location LOC-BR1). The call is made with an Executive Override precedence level.
3. Because insufficient bandwidth is available to complete the second call and the Executive Override Call Pre-emptable service parameter is set to True, the first call is preempted.
4. The call between IP phone B and IP phone Y completes and the call between IP phone A and IP phone X is cleared.

Example 10

The following example describes how Cisco Unified Communications Manager selects call preemption based on bandwidth.

Configuration

The total audio bandwidth in location (LOC-BR1) is 140 kbps

The region codec specifies a maximum audio bit rate as 64 kbps

LOC-BR1 contains the following calls:

- Call 1 with a Flash Override precedence level, which is connected and using 80 kbps (G.711) in LOC-BR1
- Call 2 with a precedence level of Flash Override, which is connected and using 80 kbps (G.711) in LOC-BR1
- Call 3 with a precedence level of Flash Override, which is connected and using 80 kbps (G.711) in LOC-BR1

IP phone B is in location Hub None and IP phone Y is in location LOC-BR1.

1. IP phone B (location Hub None) calls IP phone Y location LOC-BR1). The call is made with a precedence level of Executive Override and the region specifies 64 kbps audio bit rate.
2. Because there is insufficient bandwidth available to complete call, call 3 is preempted.
3. The call between IP phone B and IP phone Y completes.

Example 11

The following example describes how Cisco Unified Communications Manager does not preempt calls if sufficient bandwidth cannot be acquired.

Configuration

The total audio bandwidth in location (LOC-BR1) is 140 kbps

The region codec specifies a maximum audio bit rate as 64 kbps

LOC-BR1 contains the following calls:

- Call 1 with a Flash Override precedence level, which is connected and using 80 kbps (G.711) in LOC-BR1
- Call 2 with a precedence level of Flash, which is connected and using 24 kbps (G.729) in LOC-BR1
- Call 3 with a precedence level of Flash, which is connected and using 16 kbps (G.728) in LOC-BR1

IP phone B is in location Hub None and IP phone Y is in location LOC-BR1.

1. IP phone B (location Hub None) calls IP phone Y location LOC-BR1). The call is made with a precedence level of Flash Override and the region specifies 64 kbps audio bit rate.
2. Because there is insufficient bandwidth available to complete call and none of the calls can be preempted, the call between IP phone B and IP phone Y is rejected.

Example 12

The following example describes how Cisco Unified Communications Manager preempts only the required amount of bandwidth wherever possible.

Configuration

The total audio bandwidth in location (LOC-BR1) is 140 kbps

The region codec specifies a maximum audio bit rate as 64 kbps

LOC-BR1 contains the following calls:

- Call 1 with a Flash precedence level, which is connected and using 80 kbps (G.711) in LOC-BR1
- Call 2 with a precedence level of Flash, which is connected and using 24 kbps (G.729) in LOC-BR1
- Call 3 with a precedence level of Flash, which is connected and using 16 kbps (G.728) in LOC-BR1

IP phone B is in location Hub None and IP phone Y is in location LOC-BR1.

1. IP phone B (location Hub None) calls IP phone Y location LOC-BR1). The call is made with a precedence level of Flash Override and the region specifies 24 kbps audio bit rate.
2. Because there is insufficient bandwidth available to complete call 2 is preempted.
3. The call between IP phone B and IP phone Y completes.

Example 13

The following example describes how Cisco Unified Communications Manager preempts the minimum number of calls when all calls are alerting.

Configuration

The total audio bandwidth in location (LOC-BR1) is 140 kbps

The region codec specifies a maximum audio bit rate as 64 kbps

LOC-BR1 contains the following calls:

- Call 1 with a Flash precedence level, which is alerting and using 24 kbps (G.729) in LOC-BR1
- Call 2 with a precedence level of Flash, which is alerting and using 16 kbps (G.728) in LOC-BR1
- Call 3 with a precedence level of Flash, which is alerting and using 80 kbps (G.711) in LOC-BR1

IP phone B is in location Hub None and IP phone Y is in location LOC-BR1.

1. IP phone B (location Hub None) calls IP phone Y location LOC-BR1). The call is made with a precedence level of Flash Override and the region specifies 24 kbps audio bit rate.
2. Because there is insufficient bandwidth available to complete call 1 is preempted.
3. The call between IP phone B and IP phone Y completes.

Example 14

The following example describes how Cisco Unified Communications Manager preempts alerting calls before connected calls at the same precedence level.

Configuration

The total audio bandwidth in location (LOC-BR1) is 140 kbps

The region codec specifies a maximum audio bit rate as 64 kbps

LOC-BR1 contains the following calls:

- Call 1 with a Flash precedence level, which is connected and using 80 kbps (G.711) in LOC-BR1
- Call 2 with a precedence level of Flash, which is alerting and using 16 kbps (G.728) in LOC-BR1
- Call 3 with a precedence level of Flash, which is alerting and is alerting and using 16 kbps (G.728) in LOC-BR1

IP phone B is in location Hub None and IP phone Y is in location LOC-BR1.

1. IP phone B (location Hub None) calls IP phone Y location LOC-BR1). The call is made with a precedence level of Flash Override and the region specifies 24 kbps audio bit rate.
2. Because there is insufficient bandwidth available to complete call 2 and call 3 are preempted.
3. The call between IP phone B and IP phone Y completes.

Example 15

The following example describes how Cisco Unified Communications Manager preempts a lower priority call before a higher priority call.

Configuration

The total audio bandwidth in location (LOC-BR1) is 140 kbps

The region codec specifies a maximum audio bit rate as 64 kbps

LOC-BR1 contains the following calls:

- Call 1 with a Flash Override precedence level, which is connected and using 80 kbps (G.711) in LOC-BR1
- Call 2 with a precedence level of Flash, which is connected and using 16 kbps (G.728) in LOC-BR1
- Call 3 with a precedence level of Flash, which is connected and is alerting and using 16 kbps (G.728) in LOC-BR1
- Call 4 with a precedence level of Flash, which is alerting and using 16 kbps (G.728) in LOC-BR1

IP phone B is in location Hub None and IP phone Y is in location LOC-BR1.

1. IP phone B (location Hub None) calls IP phone Y location LOC-BR1). The call is made with a precedence level of Executive Override and the region specifies 24 kbps audio bit rate.
2. Because there is insufficient bandwidth available to complete call 3 and call 4 are preempted.
3. The call between IP phone B and IP phone Y completes.

Example 16

The following example describes a call that is receiving music on hold that is considered to be at the original precedence.

Configuration

The total audio bandwidth in location (LOC-BR1) is 140 kbps

The region codec specifies a maximum audio bit rate as 64 kbps

LOC-BR1 contains the following calls:

- Call 1 with a Flash precedence level, which is currently receiving music on hold (location LOC-BR1) and uses 80 kbps (G.711) in LOC-BR1
- Call 2 with a precedence level of Flash, which is connected and using 16 kbps (G.728) in LOC-BR1
- Call 3 with a precedence level of Flash, which is connected and using 16 kbps (G.728) in LOC-BR1

IP phone B is in location Hub None and IP phone Y is in location LOC-BR1.

1. IP phone B (location Hub None) calls IP phone Y (location LOC-BR1). The call is made with a precedence level of Flash and the region specifies 24 kbps audio bit rate.
2. Because there is insufficient bandwidth available to complete the call and no calls can be preempted, the call between IP phone B and IP phone Y is rejected.

Example 17

The following example describes a call that is receiving music on hold being preempted due to a preemption on the location of MOH.

Configuration

The total audio bandwidth in location (LOC-BR1) is 100 kbps

LOC-BR1 contains the following calls:

- Call 1 with a Flash precedence level, which is currently receiving music on hold (location LOC-BR1) and uses 80 kbps (G.711) in LOC-BR1
- Call 2 with a precedence level of Flash Override, which is connected and using 16 kbps (G.728) in LOC-BR1

A new call, with an Executive Override precedence level, is attempted from a different location to LOC-BR1, which requires 80 kbps.

Because there is insufficient bandwidth available in LOC-BR1, call 1 is preempted due to preemption on the MOH location. The initial pre-MOH call is also preempted.

Note MOH and Annunciator insertion never preempts another call even if the call has a lower priority.

Example 18

The following example describes an insertion of the ringback tone failing due to insufficient bandwidth

Configuration

The total audio bandwidth in location (LOC-BR1) is 100 kbps

LOC-BR1 contains the following calls:

- Call 1 with a Flash precedence level, which currently uses 80 kbps (G.711) in LOC-BR1
- Call 2 with a precedence level of Flash Override, which is connecting and using 16 kbps (G.728) in LOC-BR1

A new call, with a Flash precedence level, is attempted from LOC-BR1 that requires an annunciator to be inserted in LOC-BR1 to play a ringback tone.

Because there is insufficient bandwidth available, the request is rejected and Annunciator is not inserted.

Example 19

The following example describes a preemption tone, which is played by the annunciator, being preempted because of insufficient bandwidth.

Configuration

The total audio bandwidth in location (LOC-BR1) is 120 kbps

LOC-BR1 contains the following calls:

- Call 1 with a Flash precedence level, which currently uses Annunciator (location LOC-BR1) for a preemption tone and uses 80 kbps (G.711) in LOC-BR1
- Call 2 with a precedence level of Flash Override, which is connecting and using 16 kbps (G.728) in LOC-BR1
- Call 3 with a precedence level of Flash, which is connecting and using 16 kbps (G.728) in LOC-BR1

A new call is attempted from LOC-BR1 to a different location. The call requires 80 kbps (G.711) and uses a Flash Override precedence level.

Because there is insufficient bandwidth available in LOC-BR1, Call 1, which is receiving a preemption tone, is selected and preempted (terminating the preemption tone playback).

Example 20

The following example describes a preemption tone, which is played by the annunciator, being preempted because of insufficient bandwidth.

Configuration

The total audio bandwidth in location (LOC-BR1) is 120 kbps

LOC-BR1 contains the following calls:

- Call 1 with a Flash precedence level, which currently uses Annunciator (location LOC-BR1) for a preemption tone and uses 80 kbps (G.711) in LOC-BR1
- Call 2 with a precedence level of Flash Override, which is alerting and using 16 kbps (G.728) in LOC-BR1
- Call 3 with a precedence level of Flash, which is alerting and using 16 kbps (G.728) in LOC-BR1

A new call is attempted from LOC-BR1 to a different location. The call requires 80 kbps (G.711) and uses a Flash Override precedence level.

Because there is insufficient bandwidth available in LOC-BR1, Call 3, which is alerting, is preempted and call 1, which is receiving a preemption tone, continues to play the tone.

Example 21

The following example describes preemption in both the originating and terminating locations.

Configuration

The total audio bandwidth in location (LOC-BR1) is 140 kbps

The total audio bandwidth in location (LOC-BR2) is 140 kbps

The following calls exist in the system:

- Call 1 with a regular precedence from LOC-BR1 to LOC-BR2 by using 80 kbps
- A new call is attempted with a Flash priority precedence level from LOC-BR1 to LOC-BR2 that requires 80 kbps

Call 1 is preempted and the new call is allowed.

Example 22

In the example, 384 K of bandwidth is required for the video call. Location A has a maximum of 500 K available video bandwidth and 500 K available audio bandwidth.

The SIP trunk is in cluster 1 in location A.

The following sequence of events takes place:

1. IP phone A makes a video call to IP phone B via the SIP trunk with Priority precedence level. Call is answered and the video is established.
2. IP phone C makes a video call to IP phone D via the SIP trunk with Flash precedence level.
3. While reserving bandwidth for the video call for C to D, the C to D call preempts the A to B call because the A to B call has a lower precedence and there is not enough bandwidth for the A to B call at location A in cluster 1 because the C to D call requires 384 K of bandwidth.
4. The A to B call gets cleared.

Example 23

In the example, 384 K of bandwidth is required for the video call. Location A has a maximum of 500 K available video bandwidth and 500 K available audio bandwidth.

The SIP trunk is in cluster 1 in location A.

The following sequence of events takes place:

1. IP phone A makes a call to IP phone B via the SIP trunk with Priority precedence level.
2. IP phone C makes a call to IP phone D via the SIP trunk with Flash precedence level.
3. Media for audio establishes successfully for both calls.
4. The A to B call gets escalated to video by IP phone B. The video connection establishes successfully.
5. The C to D call gets escalated to video by IP phone D. While the media connects for video for C to D, the A to B call gets preempted because it has a lower precedence than C to D and there is not enough bandwidth in location A for the A to B call to be maintained.
6. The C to D video call establishes successfully.

Example 24

In the example, 768 K of bandwidth is required for the new video call and 384 K is reserved for the existing video call. Location A has a maximum of 400 K available video bandwidth and 400 K available audio bandwidth.

The SIP trunk is in location A.

The following sequence of events takes place:

1. IP phone A makes a call to IP phone B via the SIP trunk with Priority precedence level.
2. IP phone C makes a call to IP phone D via the SIP trunk with Flash precedence level.
3. Media for audio establishes successfully for both calls.
4. The A to B call gets escalated to video by IP phone B. The video connection establishes successfully.

5. The C to D call gets escalated to video by IP phone D. While the media connects for video for C to D, the A to B call does not get preempted because there is still not enough bandwidth allowed for the C to D video call.
6. Flow control occurs and the call between C and D gets set up as an audio call.

Note The audio bandwidth gets released while attempting to escalate to video. Flow control occurs when preemption is not possible. If audio bandwidth is not available at this point, the audio bandwidth is oversubscribed.

Example 25

In the example, 384 K of bandwidth is required for the new video call and 384 K is reserved for the existing video call. Location A has a maximum of 384 K available video bandwidth and 300 K available audio bandwidth.

The SIP trunk is in location A.

The following sequence of events takes place:

1. IP phone A makes a call to IP phone B via the SIP trunk with Priority precedence level.
2. IP phone C makes a call to IP phone D via the SIP trunk with Priority precedence level.
3. Media for audio establishes successfully for both calls.
4. The A to B call gets escalated to video by IP phone B. The video connection establishes successfully.
5. The C to D call gets escalated to video by IP phone D. While the media connects for video for C to D, the A to B call does not get preempted because it has the same precedence level as the C to D call.
6. There is not enough bandwidth for the C to D video call; therefore, flow control occurs and the call between C and D gets set up as an audio call.

Example 26

In the example, 384 K of bandwidth is required for the video call. Location A has a maximum of 200 K available video bandwidth and 200 K available audio bandwidth.

The SIP trunk is in location A.

The following sequence of events takes place:

1. IP phone A makes a call to IP phone B via the SIP trunk with Priority precedence level.
2. Media for audio establishes successfully.
3. The A to B call gets escalated to video by IP phone B. While the media connects for video for A to B, there is not enough bandwidth for the A to B video call and there are no calls to preempt. Flow control occurs and the call between A and B gets set up as an audio call.

Example 27

In the example, 384 K of bandwidth is required for each video call. In the example, two locations exist:

- Location A

- Location B

Location A has a maximum of 1500 K available video bandwidth and 400 K available audio bandwidth.

Location B has a maximum of 400 K available video bandwidth and 400 K available audio bandwidth.

IP phones A, C, and F are in cluster 1.

IP phones B and D are in location A in cluster 2.

IP phone B has a shared line B1 in location B in cluster 2.

IP phone E is in location B in cluster 2.

The following sequence of events takes place:

1. IP phone A makes a video call to IP phone B via the SIP trunk with a flash precedence level. The call gets answered and video establishes successfully. IP phone C makes a video call to IP phone D via the SIP trunk with a priority precedence level.
2. The C to D and A to B video calls are active.
3. IP phone F makes a video call over the SIP trunk to IP phone E with a priority precedence level. The video call between F and E is active.
4. IP phone B holds the call and the video for the A t B call stops.
5. B1 (the shared line) resumes the call with a flash precedence level.
6. The F to E call gets preempted because it has a lower precedence level than the A to B1 call. The F to E call gets cleared.
7. The A to B1 call is active.

Example 28

In the example, 384 K of bandwidth is required for each video call. Location A has a maximum of 500 K available video bandwidth and 500 K available audio bandwidth.

IP phone A, C, and E are in location A.

The following sequence of events takes place:

1. IP phone A makes an audio call to IP phone B via the SIP trunk with a priority precedence level. The call gets answered and the A to B audio call is active.
2. IP phone C makes a video call to IP phone D via the SIP trunk with a priority precedence level.
3. The C to D call is active.
4. IP phone A transfers the call to IP phone E (flash call).
5. IP phone E answers the call. IP phone A completes the transfer and the B to E video call gets set up (precedence level of flash).
6. The C to D call gets preempted.
7. The B to E video call is active.

Example 29

In the example, 384 K of bandwidth is required for each video call. Location A has a maximum of 500 K available video bandwidth and 500 K available audio bandwidth.

IP phone A, C, and E are in location A.

The following sequence of events takes place:

1. IP phone A makes an audio call to IP phone B via the SIP trunk with a priority precedence level. The call gets answered and the A to B audio call is active.
2. IP phone C makes a video call to IP phone D via the SIP trunk with a priority precedence level.
3. The C to D call is active.
4. IP phone A transfers the call to IP phone E (flash call).
5. IP phone E answers the call. IP phone A completes the transfer and the B to E video call gets set up (precedence level of flash).
6. The C to D call gets preempted.
7. The B to E video call is active.

Example 30

In the example, 384 K of bandwidth is required for each video call. Location A has a maximum of 800 K available video bandwidth and 500 K available audio bandwidth.

IP phone A, C, and E are in location A.

The following sequence of events takes place:

1. IP phone A makes a Priority video call to IP phone B. IP phone B answers the call and video is established.
2. IP phone C makes a Flash video call to IP phone D. IP phone D answers the call and video is established.
3. IP phone A places the A to B call on hold. The bandwidth is not yet released for the video pool for the A to B video call.
4. IP phone E makes a Flash video call to IP phone F.
5. The A to B call is preempted because there is not enough bandwidth in location A.
6. The E to F video call is active.

Example 31

The following sequence of events takes place:

1. IP phone A calls IP phone B and IP phone B answers the call.
2. IP phone B consult transfers to IP phone C.
3. IP phone B completes the transfer.

Configuration

The Location-based Maximum Bandwidth Enforcement Level for MLPP Calls service parameter is set to Strict and the Location Based MLPP Pre-emption service parameter is set to True.

The call between location 1 (Loc1) and location 2 (Loc2) requires 80 K

The call between location 2 (Loc2) and location 3 (Loc3) requires 24 K

The call between location 1 (Loc1) and location 3 (Loc3) requires 80 K

Location	Total Available Bandwidth
Loc1	160 K
Loc2	160 K
Loc3	24 K

After step 1, the bandwidth that is required for the call between IP phone A and IP phone C is 80 K but only 24 K is available. Cisco Unified Communications Manager 8.6(1) and later clears the call if the Location-based Maximum Bandwidth Enforcement Level for MLPP Calls service parameter is set to Strict and the Location Based MLPP Pre-emption service parameter is set to True.

Example 32

The following example describes multiple calls that are preempted but the new call fails.

Configuration

The total audio bandwidth in location (LOC-BR1) is 140 kbps

The region codec specifies a maximum audio bit rate as 64 kbps

LOC-BR1 contains the following calls:

Call 1 has a precedence level of Flash, which is alerting and using 24 kbps (G.729) in LOC-BR1

Call 2 has a precedence level of Flash, which is alerting and using 16 kbps (G.728) in LOC-BR1

Call 3 has a precedence level of Flash, which is alerting and using 80 kbps (G.711) in LOC-BR1

IP phone B is in location hub None and IP phone Y is in location LOC-BR1.

The following sequence of events takes place:

1. The audio bandwidth in location LOC-BR1 is changed to 10 kbps.
2. IP phone B attempts to call IP phone Y.
3. Because the audio bandwidth in LOC-BR1 is oversubscribed, call 1 through call 3 are preempted.
4. After the preemption, because there is not sufficient bandwidth to complete the new call between IP phone B and IP phone &, the new call is also rejected.

Note The new call may also be a routine precedence call. In this case, a routine precedence call preempts multiple calls with a higher precedence level and the preemption tone is played.

Example 33

The following example describes multiple calls that are preempted and the new call succeeds.

Configuration

The total audio bandwidth in location (LOC-BR1) is 140 kbps

The region codec specifies a maximum audio bit rate as 64 kbps

LOC-BR1 contains the following calls:

Call 1 has a precedence level of Flash, which is alerting and using 24 kbps (G.729) in LOC-BR1

Call 2 has a precedence level of Flash, which is alerting and using 16 kbps (G.728) in LOC-BR1

Call 3 has a precedence level of Flash, which is alerting and using 80 kbps (G.711) in LOC-BR1

IP phone B is in location hub None and IP phone Y is in location LOC-BR1.

The following sequence of events takes place:

1. The audio bandwidth in location LOC-BR1 is changed to 80 kbps.
2. IP phone B attempts to call IP phone Y, with an Executive Override precedence level.
3. Because audio bandwidth in LOC-BR1 is oversubscribed, call 3 is preempted.
4. After the preemption, because sufficient bandwidth is not available to complete the new call between IP phone B and IP phone Y, calls 1 and 2 are preempted.
5. The new call is allowed to go through.

MLPP Announcements

This section discusses specific MLPP announcements. Users who unsuccessfully attempt to place MLPP precedence calls receive various announcements that detail the reasons why a precedence call was blocked.

Unauthorized Precedence Announcement

Users receive an unauthorized precedence announcement when they attempt to make a call with a higher level of precedence than the highest precedence level that is authorized for their line. A user receives an unauthorized precedence announcement when the user dials a precedence call by using a calling pattern for which the user does not have authorization.

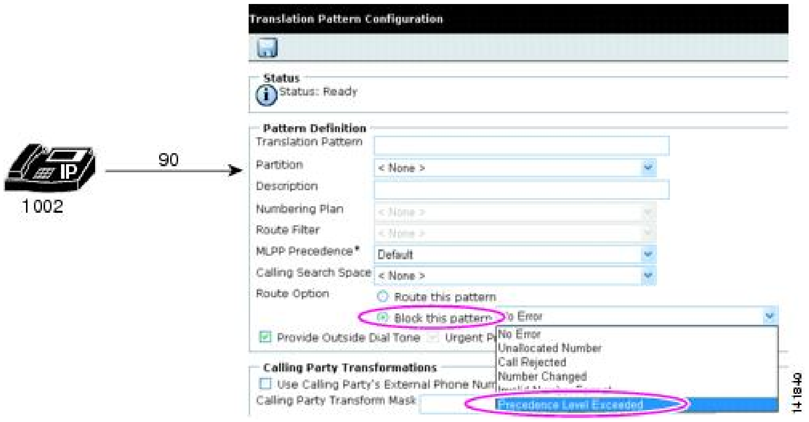
Cisco Unified Communications Manager recognizes the Precedence Level Exceeded condition only if specific patterns or partitions are configured to block a call attempt that matches the pattern and that indicates the reason that the call is blocked.

To assign authorized calling patterns, access the Route Pattern/Hunt Pilot Configuration and the Translation Pattern Configuration windows in Cisco Unified Communications Manager Administration. To configure the MLPP Precedence Level Exceeded condition, use the Route Option field of the Route Pattern/Hunt Pilot Configuration and Translation Pattern Configuration windows and choose the Block this pattern option in Cisco Unified Communications Manager Administration. In the drop-down list box, choose Precedence Level Exceeded. See the *Cisco Unified Communications Manager Administration Guide* for details.

Example

The following figure illustrates an example of a user that receives an unauthorized precedence announcement.

Figure 144: Unauthorized Precedence Announcement Example



Translation Pattern Configuration

Status
Status: Ready

Pattern Definition
Translation Pattern
Partition: < None >
Description
Numbering Plan: < None >
Route Filter: < None >
MLPP Precedence*: Default
Calling Search Space: < None >
Route Option: ○ Route this pattern
● Block this pattern: No Error
☑ Provide Outside Dial Tone □ Urgent P

No Error
Unallocated Number
Call Rejected
Number Changed
Precedence Level Exceeded

Calling Party Transformations
□ Use Calling Party's External Phone Num
Calling Party Transform Mask

In the example, user 1002 dials 90 to start a precedence call. Nine (9) represents the precedence access digit, and zero (0) specifies the precedence level that the user attempts to use. Because this user is not authorized to make flash override precedence calls (calls of precedence level 0), the user receives an unauthorized precedence announcement.

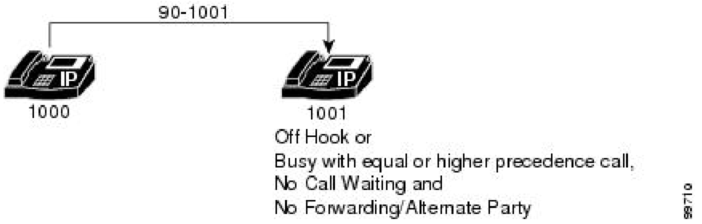
Blocked Precedence Announcement

Users receive a blocked precedence announcement if the destination party for the precedence call is off hook, or if the destination party is busy with a precedence call of an equal or higher precedence and the destination party does not have the Call Waiting nor Call Forward features nor a designated party for alternate party diversion (APD), or due to a lack of a common network resource.

Example

The following figure provides an example of a blocked precedence announcement.

Figure 145: Blocked Precedence Announcement Example



90-1001
IP
IP
1000
1001
Off Hook or
Busy with equal or higher precedence call,
No Call Waiting and
No Forwarding/Alternate Party
99710

In this example, user 1000 makes a precedence call to user 1001 by dialing 90-1001. Because user 1001 is either off hook or busy with a precedence call of equal or higher precedence level and user 1001 does not have Call Waiting nor Call Forward nor an alternate party that is designed for alternate party diversion, user 1000 receives a blocked precedence announcement.

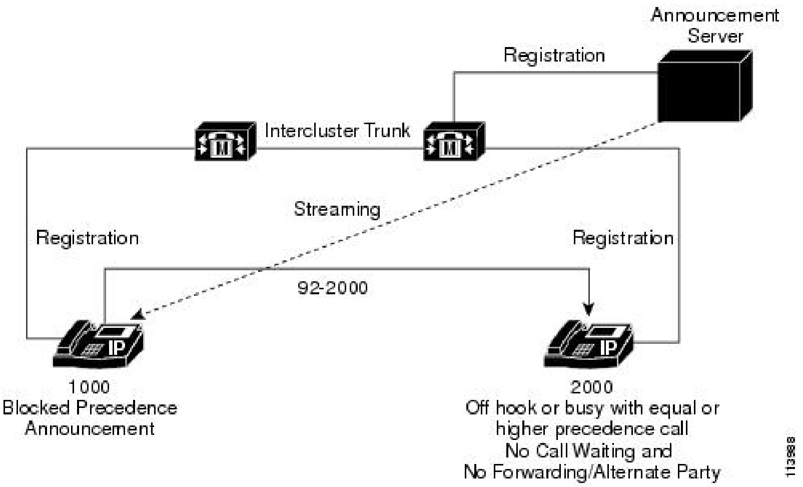
Busy Station Not Equipped for Preemption

Users receive this announcement if the dialed number is nonpreemptable. That is, the dialed number registers as busy and has no call waiting, no call forwarding, and no alternate party designations.

Announcements Over Intercluster Trunks

The following figure illustrates an instance of an MLPP announcement that is streamed over an intercluster trunk.

Figure 146: MLPP Announcement Over an Intercluster Trunk Example



In the example, phones 1000 and 2000 reside on two clusters that an intercluster trunk connects. User 2000 does not have features such as calling waiting and call forwarding configured.

The following sequence of events takes place:

1. User 2000 goes off hook and starts to dial. (Status for User 2000 specifies originating busy and not preemptable.)
2. User 1000 then dials a precedence call over the intercluster trunk to user 2000. Because user 2000 is busy and is not preemptable, the call gets rejected.
3. Because user 1000 originated a precedence call, the call receives precedence treatment, and the announcement server on the remote cluster streams the appropriate Blocked Precedence Announcement (BPA) to 1000 with the switch name and the location of the cluster.

Secured or Encrypted Announcements and Music On Hold

Cisco Unified Communications Manager 8.6(1) and later supports Secure Real-Time Protocol (SRTP) for Annunciator and Music On Hold (MOH). When an announcement or MOH plays to a user, Cisco Unified Communications Manager checks the security capabilities of the Annunciator and MOH and the user’s device. If all devices support SRTP, the announcement or MOH media is encrypted prior to streaming to the user’s device and a secure locked icon displays on the Cisco Unified IP Phone.

For examples that describe how the locked icon displays when secured and unsecured announcements are inserted for precedence calls, see Announcements Over Intercluster Trunks, on page 945. For examples that describe how the locked icon displays when secured and unsecured MOH media is inserted for precedence calls, see Music On Hold, on page 967

MLPP Numbering Plan Access Control for Precedence Patterns

MLPP uses the calling search spaces and partitions that are defined for users to authenticate and validate MLPP calls and provide access control for precedence patterns.

Note The exception for this usage is AS-SIP endpoints. AS-SIP does not signal precedence using dialed digits and has a separate protocol mechanism for establishing precedence authorization. This section applies to all MLPP devices except AS-SIP phones.

The maximum precedence of a user gets set at user configuration time. All MLPP-capable station devices get configured as either MLPP-enabled or MLPP-disabled. A device to which a user profile is applied inherits the precedence level of that user with respect to precedence calls that are initiated from that device. A device that has a default user assigned inherits a Routine precedence level for the default user.

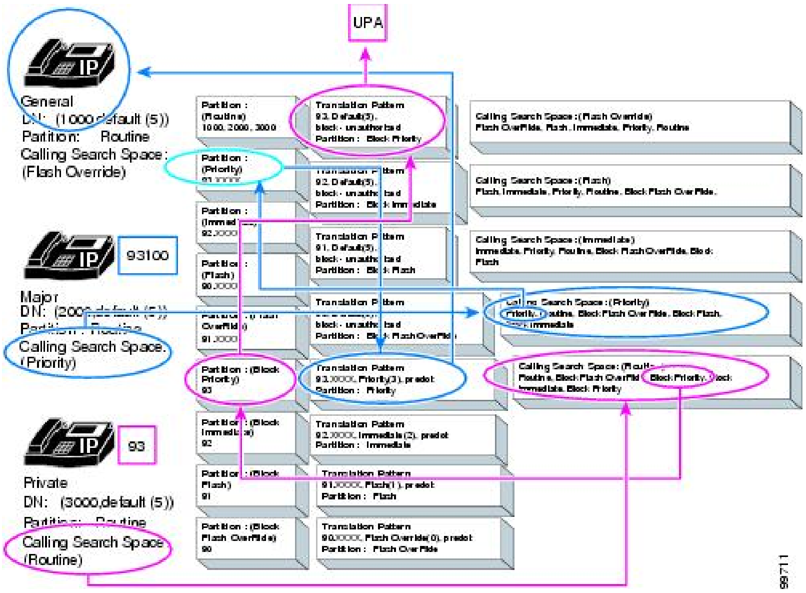
Configuration of the calling search space(s) (CSS) that is associated with the calling party controls ability of a user to dial a precedence pattern (that is, to initiate a precedence call). Cisco Unified Communications Manager does not provide for explicit configuration of an explicit maximum allowed precedence value.

The following example illustrates the differences in access to precedence calls for two users who try to place a priority-level precedence call to a third user.

Example

The following figure provides an example of MLPP numbering plan access control for precedence patterns.

Figure 147: MLPP Numbering Plan Access Control for Precedence Patterns Example



The table defines three users in this illustration:

User	Directory Number (DN)	Partition	Calling Search Space (CSS)
General	1000	Routine	Flash Override

User	Directory Number (DN)	Partition	Calling Search Space (CSS)
Major	2000	Routine	Priority
Private	3000	Routine	Routine

The example shows the use of partitions and calling search spaces to limit access to precedence calls.

If private 3000 tries to place a precedence call by dialing the precedence pattern 93, the following events take place:

- Call processing searches for calling search space for private 3000, which is the Routine CSS.
- Within Routine CSS of private 3000, call processing finds the Block Priority partition.
- In the Block Priority partition, call processing finds the pattern 93 and goes to translation pattern 93.
- Translation pattern 93 determines that priority calls are blocked for this user (DN), and call processing issues an unauthorized precedence announcement (UPA).

If major 2000 places a precedence call by dialing the digits 931000, the following events take place:

- Call processing searches for calling search space for major 2000, which is the Priority CSS.
- Within Priority CSS for major 2000, call processing finds the Priority partition.
- In the Priority partition, call processing finds the pattern 93.XXXX and goes to translation pattern 93.XXXX.
- Translation pattern 93.XXXX determines that priority calls are authorized for this user (DN). Call processing therefore completes the Priority-level precedence call to user 1000, the general.

MLPP Trunk Selection

MLPP trunk selection entails hunting for available trunks by using route lists and route groups. In Cisco Unified Communications Manager Administration, you can configure a route list and associated route group(s) to route calls to several gateways via a single dial pattern to find an available channel. Although a route list has many trunk resources to which the route list can route calls, the individual resources may spread across many gateways.

When no available trunk resource is identified in a collection of gateways (that is, a route list and route group configuration), Cisco Unified Communications Manager attempts to initiate preemption of a lower level precedence shared resource in the collection. Two methods exist for subsequently searching for a preemptable channel within a route list and route group configuration.

Method 1

Configure a route list and a single route group. Add trunk interfaces (gateways) to the route group and position the Direct Route gateway as the first gateway in the route group. Associate the route group with the route list and choose the Top Down distribution algorithm. With this configuration, the system searches all gateways in the route group for an idle channel first. If no idle channel is found in any gateway in the route group, preemptive trunk selection begins with the first gateway in the route group (that is, the Direct Route gateway) as follows:

- Call processing chooses a current route from the collection on the basis of the distribution algorithm and offers the call to this gateway device to determine whether the gateway device can initiate preemption.
- If the current gateway device rejects the precedence call request (that is, the gateway device cannot initiate preemption), call processing chooses the next gateway in the collection as the current route and continues this sequence until a gateway device initiates preemption or until all gateway devices in the route list and route group collection have been searched.

Method 2

Configure a route list and a separate route group for each available route (trunk interface). Designate one route group as the Direct route group and designate the other route groups as Alternate route groups. Add the Direct Route trunk interface (gateway) as the only member of the Direct route group. Add the Alternate Route gateways to the individual Alternate route groups. Associate the route groups with the route list, configuring the Direct route group as the first route group in the route list, and choose the Top Down distribution algorithm for each route group association.

Using this configuration, the Direct gateway in the Direct route group gets searched for an idle channel first. If no idle channel is found in the Direct gateway, the system initiates preemptive trunk selection for this Direct gateway as follows:

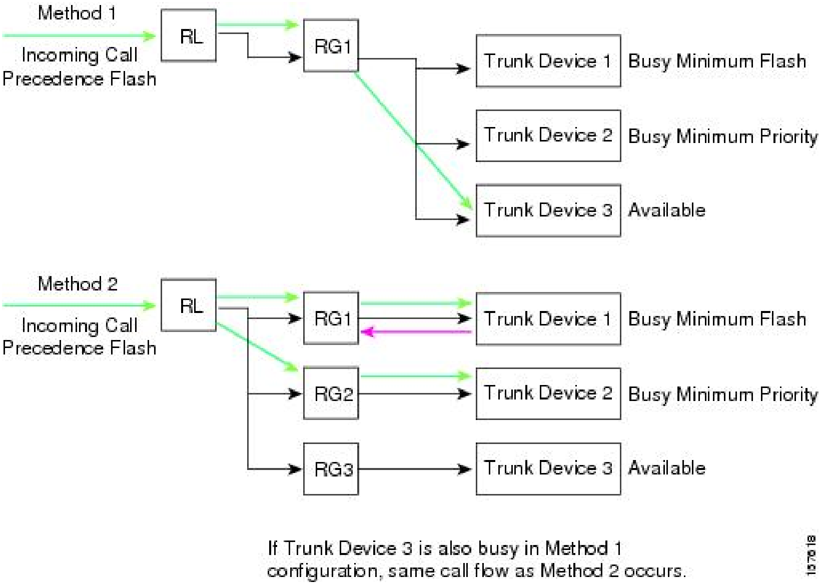
- Call processing chooses the Direct route and offers the call to this gateway device to determine whether the gateway device can initiate preemption.
- If the Direct gateway device rejects the precedence call request (that is, the gateway device cannot initiate preemption), choose the next route group in the route list as the current route. Continue this sequence until an idle channel is found on the current gateway, or until the current gateway device has initiated preemption, or until all gateway devices in the route list and route group collection are searched.

Example

The following example illustrates two methods for finding an available trunk device when an incoming flash-level precedence call seeks an available trunk device.

The following figure provides an example of MLPP trunk selection that uses route lists and route groups to hunt for an available trunk device.

Figure 148: MLPP Trunk Selection (Hunting) Example



In Method 1, the following sequence of events takes place:

1. An incoming flash-level precedence call reaches route list RL, which contains only one route group, RG1.
2. Route group RG1 contains three trunk devices.

   Of the three trunk devices in RG1, Trunk Device1 and Trunk Device2 register as busy, so the system offers the call to Trunk Device3, which is available.

   In Method 2, the following sequence of events takes place:

3. An incoming flash-level precedence call reaches route list RL and first goes to route group RG1, which directs the call to Trunk Device1, which is busy.

   For Trunk Device1, calls must have a higher precedence than flash to preempt calls that are using this device.

4. The call therefore seeks the next route group in route list RL, which is route group RG2. Route group RG2 contains Trunk Device2, which is also busy, but precedence calls of a precedence level higher than Priority can preempt Trunk Device2.

   Because this call is a higher precedence call, the call preempts the existing call on Trunk Device2.

MLPP Hierarchical Configuration

MLPP settings for devices follow this hierarchy:

- If MLPP Indication for a device is set to Off, the device cannot send indication of MLPP calls. If the device MLPP Preemption is set to Disabled, the device cannot preempt calls. These settings override the common device configuration settings for the device.
- If MLPP Indication for a device is set to On, the device can send indication of MLPP calls. If the MLPP Preemption for the device is set to Forceful, the device can preempt calls. These settings override the common device configuration settings for the device.

- If MLPP Indication for a device is set to Default, the device inherits its ability to send indication of MLPP calls from the common device configuration for the device. If the MLPP Preemption for a device is set to Default, the device inherits its ability to preempt calls from the common device configuration for the device.

MLPP settings for common device configurations follow this hierarchy:

- If a common device configuration MLPP Indication is set to Off, devices in the common device configuration cannot send indication of MLPP calls. If the common device configuration MLPP Preemption is set to Disabled, devices in the common device configuration cannot preempt calls. These settings override the MLPP enterprise parameter settings.
- If a common device configuration MLPP Indication is set to On, devices in the common device configuration can send indication of MLPP calls. If the common device configuration MLPP Preemption is set to Forceful, devices in the common device configuration can preempt calls. These settings override the MLPP enterprise parameter settings.
- If a common device configuration MLPP Indication is set to Default, the device inherits its ability to send indication of MLPP calls from the MLPP Indication Status enterprise parameter. If the common device configuration MLPP Preemption is set to Default, the common device configuration inherits its ability to preempt calls from the MLPP Preemption Setting enterprise parameter.

The MLPP Indication Status enterprise parameter defines the indication status of common device configurations and common device configurations in the enterprise, but nondefault settings for common device configurations and individual devices can override its value. The default value for this enterprise parameter specifies MLPP Indication turned off.

The MLPP Preemption Setting enterprise parameter defines the preemption ability for common device configurations and devices in the enterprise, but nondefault settings for common device configurations and individual devices can override its value. The default value for this enterprise parameter specifies No preemption allowed.

The MLPP Domain Identifier enterprise parameter specifies the MLPP domain. The MLPP service applies only to a domain; that is, only to the subscribers and the network and access resources that belong to a particular domain. Connections and resources that belong to a call from an MLPP subscriber get marked with a precedence level and an MLPP domain identifier. Only calls of higher precedence from MLPP users in the same domain can preempt lower precedence calls in the same domain.

Service Parameter Special Trace Configuration

MLPP issues a service parameter for tracing.

See the *Cisco Unified Serviceability Administration Guide* for details.

CDR Recording for Precedence Calls

MLPP precedence calls generate call detail records (CDRs). The CDR identifies the precedence level of the precedence call.

The same precedence levels of the call legs generally apply. With transfer or conference calls, the precedence levels can differ; therefore, Cisco Unified Communications Manager CDRs identify the precedence level of each leg of the call.

Cisco Unified Communications Manager CDRs document the preemption value for preempted call terminations.

See the *Cisco Unified Serviceability Administration Guide* for details.

Line Feature Interaction

This section describes how MLPP interacts with line features.

Call Forward

MLPP interacts with the call forward features as described in the following list:

- Call Forward Busy
    - You optionally can 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 prior to applying any Precedence Alternate Party Diversion procedures to the call.
    - 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.
    - 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 setting is configured for the destination of a precedence call, call processing diverts the precedence call to the Call Forward No Answer setting.
    - Normally, precedence calls route to users and not to the voice-messaging system. The administrator sets the Use Standard VM Handling For Precedence Calls enterprise parameter to avoid routing precedence calls to voice-messaging systems. See the Set the Enterprise Parameters for MLPP, on page 964 for details.

Call Transfer

MLPP interacts with the call-transfer feature. For blind transfers and consult transfers, each connection of the transferred call, including the consult call, maintains the precedence that the connection was assigned when the call was established.

Shared Lines

MLPP interacts with shared lines. A shared-line appearance with a call on hold may be preempted to establish a higher precedence call to another terminal with the same directory number (DN). In this case, the original held call does not disconnect, and the precedence call connects. After the precedence call ends, the user may retrieve the original held call.

Call Waiting

MLPP interacts with the call-waiting feature as described in the following list:

- When a Routine precedence call is offered to a destination station that already has active calls that are configured with call waiting, normal call waiting is activated if the existing call count is less than the busy trigger.
- When a non-routine precedence call is offered to a destination station that already has an active call that is configured with call waiting, precedence call waiting is activated if the existing call count is less than the busy trigger and any of the following conditions exist:
    - The device supports visual call appearances and has an open appearance.
    - The device supports two non-visual call appearances and has an open appearance, and the precedence of the new call is equal to or lower than the existing call.
    - The device has an open appearance (visual or non-visual) and the device is non-preemptable.
- When a non-routine precedence call is offered to a destination station that already has an active call that is configured with call waiting, an existing lower-precedence call is preempted if the existing call count is equal to or greater than the busy trigger.

Call Preservation

Any MGCP trunk call or connection that is preserved according to the Cisco Unified Communications Manager Call Preservation feature preserves its precedence level and MLPP domain after invoking the Call Preservation feature. After the device registers with Cisco Unified Communications Manager, the system only preserves the preserved calls at the device layer in the Cisco Unified Communications Manager system. As a result, the preserved calls gets treated as two disjointed half calls. If preemption does occur on these devices, only one leg can follow preemption protocol to the other leg. The system detects call termination only through closure of the RTP port.

Automated Alternate Routing

The Automated Alternate Routing (AAR) for Insufficient Bandwidth feature, an extension of AAR, provides a mechanism to automatically fall back to reroute a call through the Public Switched Telephone Network (PSTN) or other network by using an alternate number when the Cisco Unified Communications Manager blocks the call due to insufficient location bandwidth. With this feature, the caller does not need to hang up and redial the called party.

If a precedence call attempt meets a condition that invokes the AAR service, the precedence call gets rerouted through the PSTN or other network as specified by the AAR configuration. Cisco Unified Communications Manager handles the precedence nature of the call in the same manner as if the call originally had been routed through the PSTN or other network, based on the MLPP Indication Enabled and MLPP Preemption Enabled nature of the network interface through which the call is routed.

For details of configuring Automated Alternate Routing, see the *Cisco Unified Communications Manager Administration Guide*.

MGCP and PRI Protocol

MLPP supports Common Network Facility Preemption only for T1-CAS and T1-PRI (North American) interfaces on targeted Voice over IP gateways that Cisco Unified Communications Manager controls by using MGCP protocol and that have been configured as MLPP Preemption Enabled.

Secure Endpoints and Secure Communications

The Department of Defense (DOD) TDM network uses legacy analog secure telephone units (STUs) and BRI secure telephone equipment (STEs) as secure endpoints, which are critical for secure communication. The IP STE also requires support to reduce the need for legacy equipment. Cisco Unified Communications Manager supports the Skinny Client Control Protocol for these devices. Modem relay provides secure communication and uses either the legacy V.150 or V.150.1 MER (Minimal Essential Requirements) protocol.

Note If you want a trunk to support V.150.1 Modem over IP (MOIP) calls, you must enable the V150 (subset) check box in Cisco Unified Communications Manager Administration for digital access PRI/T1 port configuration on the gateway. You must also enable the MDSTE package on the gateway by using the mgcp package-capability mdste-package CLI configuration command. For more information, refer to the Cisco Unified Communications Manager Administration Guide.

Map MLPP Precedence to DSCP Values

Cisco Unified Communications Manager maps the MLPP precedence levels to the DSCP values in the ToS field of the IP Header to prioritize calls in an IP network. You can map the following precedence levels to DSCP values:

- Executive Override
- Flash Override
- Flash
- Immediate
- Priority

You must map the MLPP precedence levels to the DSCP values identically for every Cisco Unified Communications Manager cluster within your network.

To map MLPP precedence levels to DSCP values, choose the DSCP value that you want mapped to each precedence level in the Clusterwide Parameters (System-QoS) section of the service parameters. Click the Save button to save the changes.

The DSCP values that you configure are also applicable to the SCCP phones.

Procedure

Procedure

Step 1 Choose **Enterprise Parameter** > **MLPP Parameters** and set the MLPP indication status to MLPP Indication On.

Step 2 For SCCP phones, choose **Phone Configuration** > **MLPP Information** > **MLPP Indication** and set to MLPP Indication On.

If MLPP indication is not set to On in the preceding cases, then the DSCP value corresponding to DSCP for audio calls will be used.

The following table summarizes the list of Media Resource devices and their support for DSCP tagging based on MLPP Precedence:

Table 100: List of Media Resource Devices and their Support for DSCP Tagging based on MLPP Precedence

Media Resource Type Name	Software Based Resource Type Supported	Hardware (IOS Gateway) Based Resource Type Supported
Media Termination Point	Yes	Yes
Music on Hold	Yes	No
Annunciator	Yes	NA
Transcoder	NA	Yes
Audio Conference Bridge	Yes	Yes[1]
Video Conference Bridge[2]	NA	Yes[3]

[1] Cisco IOS Enhanced Conference Bridge

[2] DSCP tagging is supported only for audio conferences using Video Conference Bridge

[3] Radvision CUVC

MLPP precedence calls involving the devices mentioned use the DSCP values configured in the service parameter page for the corresponding MLPP precedence.

MLPP Supplementary Services

This section describes Cisco Unified Communications Manager Administration support for MLPP supplementary services and entities. Each supplementary service description provides configuration information and recommendations, and troubleshooting information.

MLPP Support for Multiple Appearance Lines

If an empty call appearance is available and the busy trigger is not exceeded, an incoming precedence call gets presented such that the active line receives the precedence call-waiting tone and the endpoint display shows the appropriate precedence bubbles. The incoming call does not cause precedence ringing. Instead, precedence call-waiting tone occurs on the active appearance.

If no empty call appearances are available and the called endpoint does not have call forwarding configured, a higher precedence inbound call will preempt a lower active or nonactive call appearance on the endpoint. In the case of a tie, the active appearance gets preempted.

If a nonactive (held) appearance gets preempted, the incoming call shows the appropriate precedence bubbles on the endpoint display, and the precedence call-waiting tone gets presented on the active call appearance. The other preempted user (the other end of the held call) receives call preemption tone.

If the active call appearance gets preempted, normal call preemption takes place (preemption tone gets presented on the active appearance and on the other party active line). Any existing, nonactive (held) call appearances remain unaffected and can be picked up at any time.

Configuration

For MLPP support for multiple appearance lines to function correctly, Cisco recommends the following configuration:

- Cisco recommends, but does not require, setting IP phones with max calls=4 and busy trigger=2.
- When interaction with MLPP supplementary services occurs, no support exists for assigning the same DN twice to the same station by using multiple partitions.
- Disable the Auto Line Select option for all IP phones because the highest precedence call may not get answered when multiple alerting calls are incoming.

Troubleshooting

If you use the CCM trace log (with detailed trace configured), you can tell how the preemption criteria was applied on any inbound call by searching for the whatToDo tag.

Call Forwarding

The Department of Defense (DoD) requires that no precedence calls get forwarded to off-net endpoints, such as mobile phones. Additionally, forwarded calls must retain the original precedence across multiple forwarding hops.

For Call Forward All (CFA) scenarios, precedence calls get routed to the MLPP Alternate Party (MAP) target of the original called party immediately. The CFA target does not get used for MLPP calls.

For Call Forward Busy (CFB) scenarios, precedence calls get forwarded to the configured CFB destination, subject to the hop count limits described in the Restrictions, on page 961 and the state of open appearances on the called party endpoint.

For the Call Forward No Answer (CFNA) scenario, call processing attempts a single forward attempt (hop) to the CFNA target of the original called party. If that endpoint does not answer prior to the expiration of the No Answer timer, the call gets sent to the MAP target of the original called party.

Configuration

MLPP operation in the DoD requires that all MLPP endpoints have an MLPP Alternate Party (MAP) target directory number that is configured. The MAP typically specifies the attendant number and is used as a destination of last resort for forwarded MLPP calls.

If the endpoint does not follow the prescribed configuration when a MAP is needed, the MLPP call originator receives reorder tone, which indicates that the called party configuration does not include the required MAP configuration. This tone plays only if the call would have been directed to the attendant when no other forwarding options were available or configured.

Example

The following example describes a forwarding case. First, the MLPP call rings (3001 calls 3003 at Flash Override precedence level) with the CFNA timer set to 5 seconds. After the timer expires, the call gets redirected to the original called party CFNA target, which is 3004. During the process, the call retains its precedence level, 1, which designates Flash Override.

Three-Way Calling

Cisco Unified Communications Manager prescribes the following requirements for three-way calling:

- Each connection of a three-way call must maintain its original precedence level.
- The phone that performs the split operation of the three-way call uses the higher precedence level of the two calls when different precedence levels are involved.

Cisco Unified Communications Manager MLPP also includes preemption of conference bridge resources. If a conference bridge is saturated with calls, individual streams get preempted when setup of a new higher precedence three-way call occurs.

Configuration

Cisco recommends setting the Maximum Ad Hoc Conference service parameter to 3. This setting limits ad hoc calls to three participants. Cisco Unified Communications Manager uses the ad hoc conference feature to implement a three-way call.

Use the Cisco Unified Communications Manager IP Voice Media Streaming App to service three-way calls. Do not use the IOS DSP farm to service conference calls because the IOS DSP farm does not address MLPP support.

Preemption occurs across a single bridge only.

MLPP three-way calls do not interoperate with the conference chaining features that were added in Release 4.2 of Cisco Unified Communications Manager.

Example 1

This example discusses a three-way call among A, B, and C. A called B at Priority 4; then, A called C at Priority 2 (Flash) and started the conference. The conference now proceeds as active with three participants: A at Flash precedence level, B at Priority precedence level, and C at Flash precedence level. When C hangs up, A and B get joined together in a normal call. A must get downgraded from Flash to Priority.

Example 2

In this example, a conference call preempts an existing conference call. The max streams value on the conference bridge was set to 3 to saturate the bridge. The first three-way call gets established among parties A, B, and C at Routine precedence level (5). Phone D then establishes a three-way call with parties E and F at Flash precedence level (2).

Call Transfer

When a switch initiates a call transfer between two segments that have the same precedence level, the segments should 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 higher precedence level of the two segments.

Cisco Unified Communications Manager supports this requirement by upgrading the precedence level of a call leg that is involved in a transfer operation. For example, party A calls party B with Priority precedence level. Party B then initiates a transfer to C and dials the Flash precedence digits when dialing. When the transfer completes, the precedence level of party A gets upgraded from Priority to Flash.

Note The precedence level upgrade does not work over a trunk device such as an intercluster trunk (ICT) or PRI trunk.

Configuration

The MLPP transfer service entails no configuration requirements. The feature gets enabled automatically when MLPP is enabled, and the phones support the Transfer softkey.

Call Pickup

Cisco Unified Communications Manager adds the criteria of highest precedence to the call pickup algorithm, including the following requirements:

- If a call pickup group has more than one party in an unanswered condition and the unanswered parties are at different precedence levels, a call pickup attempt in that group retrieves the highest precedence call first.
- If multiple calls of equal precedence are ringing simultaneously, a call pickup attempt in that group retrieves the longest ringing call first.
- The system supports group pickup functionality for MLPP calls. Operation follows normal call pickup functionality.
- For MLPP calls, no support exists for Other Group Pickup.
- If multiple calls are ringing at directory number (DN) A, a user that picks up a call from DN A by using the Directed Call Park feature will be connected to the incoming call of highest precedence, assuming that the user is configured to use the Directed Call Park feature to pick up calls from DN A.

Configuration

The Call Pickup for MLPP capability introduces no special configuration considerations; however, MLPP calls do not support other group pickup.

Hunt Pilots and Hunt Lists

Cisco Unified Communications Manager includes modifications to the previous implementation of the hunt pilot feature. The following aspects of MLPP interaction with hunt pilots changed:

- Normal hunt algorithm logic occurs until all lines in the hunt group are busy.
- When all lines are busy, the lowest precedence call gets selected for preemption.
- When preemption occurs, the normal line group No Answer timer continues. When this timer expires, the next lowest precedence call in the hunt group gets selected for preemption.

MLPP gets implemented for the following hunt algorithms:

- Top down
- Longest idle time
- Circular

Preemption can still occur when the broadcast algorithm is in use. Cisco does not provide explicit support for the broadcast algorithm.

Cisco Unified Communications Manager allows configuration of multiple line groups for a hunt group. The current implementation supports only a single line group under a hunt group. Preemption still occurs when multiple line groups are configured, but the lowest precedence call may not get selected for preemption when more than one line group was configured for a hunt group.

Configuration

Hunt pilots and hunt lists require the following configuration:

- Configure only one hunt list in the hunt group. Preemption only happens across the first group in the list.
- Set all hunt group options to Try next member, but do not go to next group. This includes the options for No Answer, Busy, and Not Available.
- Set the hunt group algorithm to Top Down, Circular, or Longest Idle Time. Cisco does not provide support for the Broadcast algorithm.
- Disable the Use personal preferences check boxes on the hunt pilot.
- Ensure the MLPP precedence setting on the hunt pilot specifies Default.
- Configure all stations in the hunt list in a single MLPP domain.

Cisco strongly recommends the following additional configuration:

- Set the Forward No Answer DN hunt pilot to the DN of last resort.
- Set the Forward on Busy DN hunt pilot to the DN of last resort.

Supplementary Services Support for SCCP Gateway Endpoints

These updates bring together Supplementary Services support for SCCP gateway endpoints and MLPP support for basic call on SCCP gateways.

Note This feature is supported on analog phones only.

The Supplementary Services support update incorporates the following functionalities:

- Call Hold - The users can avail of the following functionalities during Call Hold interaction with MLPP on SCCP gateways:
  - Preemption if the new call is higher precedence than both held and active calls.

Note Be aware that Preemption preempts both-the held calls, and the active call.

- Precedence Call Waiting - The users can avail of the following functionalities during Call Waiting interaction with MLPP on SCCP gateways:
  - Precedence Call Waiting tone support on the gateway
  - For single active call, new higher precedence call preemption rather than play Precedence Call Waiting
  - On a phone with ringing precedence calls, an inbound call preempts the lower precedence ringing calls.

Note If the user chooses to invoke the Cancel Call Waiting feature while making a call, this overrides the Precedence Call Waiting settings for just that call. The Cancel Call Waiting settings apply only on the phone from which it is invoked, and have no affect on the phones calling it.

Note For more information on the Cancel Call Waiting feature, see the *Cisco Unified Communications Manager Administration Guide*.

- Allow Call Waiting During an In-Progress Outbound Analog Call Service Parameter - A new service parameter is added to Cisco Unified Communications Manager. This parameter determines whether Cisco Unified Communications Manager allows an inbound call to be presented to a call-waiting-enabled SCCP gateway analog phone, when the analog phone is involved in an outbound call but may be unable to play the call waiting tone. The analog phone may not be able to play the call waiting tone until the outbound call gets to the alerting or connected state. Valid values can specify True or False:
  - True - The call-waiting-eligible analog phone is presented with the inbound call regardless of the phone's ability to play call waiting tone, and the standard call answer time limit applies.
  - False - Cisco Unified Communications Manager treats this as a normal analog line appearance reaching its Busy Trigger call limit; this treatment could involve forwarding actions, tones, or any other features applicable to the trigger.

Note For information on working with service parameters, see the “Configuring Service Parameters for a Service on a Server” section in *Cisco Unified Communications Manager Administration Guide*.

SystemRequirementsforMultilevelPrecedenceandPreemption

MLPP requires Cisco Unified Communications Manager 4.0 or later to operate.

Determine Device Support for Multilevel Precedence and Preemption

Use the Cisco Unified Reporting application to generate a complete list of IP Phones that support MLPP.

Note Only SCCP phones support the Multilevel Precedence and Preemption (MLPP) feature. SIP phones do not support MLPP.

For additional information about the Cisco Unified Reporting application, see the *Cisco Unified Reporting Administration Guide*

Procedure

Step 1 Start Cisco Unified Reporting by using any of the methods that follow. The system uses the Cisco Tomcat service to authenticate users before allowing access to the web application. You can access the application

- by choosing **Cisco Unified Reporting** in the **Navigation** menu in Cisco Unified Communications Manager Administration and clicking **Go.**
- by choosing **File** > **Cisco Unified Reporting** at the Cisco Unified **Real Time Monitoring Tool** (RTMT) menu.
- by entering `https://<server name or IP address>:8443/cucreports/` and then entering your authorized username and password.

Step 2 Click **System Reports** in the navigation bar.

Step 3 In the list of reports that displays in the left column, click the **Unified CM Phone Feature List** option.

Step 4 Click the **Generate a new report** link to generate a new report, or click the **Unified CM Phone Feature List** link if a report already exists.

Step 5 To generate a report of all IP Phones that support call precedence for MLPP, choose these settings from the respective drop-down list boxes and click the **Submit** button:

Product: All

Feature: Call Precedence (for MLPP)

The List Features pane displays a list of all devices that support the MLPP feature. You can click on the Up and Down arrows next to the column headers (Product or Protocol) to sort the list.

Step 6 To generate a report of all IP Phones that support call preemption for MLPP, choose these settings from the respective drop-down list boxes and click the **Submit** button:

Product: All

Feature: Call Pre-emption (for MLPP)

The List Features pane displays a list of all devices that support the MLPP feature. You can click on the Up and Down arrows next to the column headers (Product or Protocol) to sort the list.

Interactions and Restrictions

This section describes the interactions and restrictions for MLPP.

Interactions

MLPP interacts with the following Cisco Unified Communications Manager features as follows:

- Cisco Extension Mobility - The MLPP service domain remains associated with a user device profile when a user logs in to a device by using extension mobility. The MLPP Indication and Preemption settings also propagate with extension mobility. If either the device or the device profile do not support MLPP, these settings do not propagate.
- Immediate Divert - Immediate Divert diverts calls to voice-messaging mail boxes regardless of the type of call (for example, a precedence call). When Alternate Party Diversion (call precedence) is activated, Call Forward No Answer (CFNA) also gets deactivated.
- Cisco Unified Communications Manager Assistant (Unified CM Assistant) - MLPP interacts with Unified CM Assistant as follows:
  - When Cisco Unified Communications Manager Assistant handles an MLPP precedence call, Cisco Unified Communications Manager Assistant preserves call precedence.
  - Cisco Unified Communications Manager Assistant filters MLPP precedence calls in the same manner as it filters all other calls. The precedence of a call does not affect whether the call is filtered.
  - Because Cisco Unified Communications Manager Assistant does not register the precedence of a call, it does not provide any additional indication of the precedence of a call on the assistant console.
- Resource Reservation Protocol (RSVP) - RSVP supports MLPP inherently. The *Cisco Unified Communications Manager System Guide* explains how MLPP functions when RSVP is activated.
- Supplementary Services - MLPP interacts with multiple line appearances, call transfer, call forwarding, three-way calling, call pickup, and hunt pilots as documented in the MLPP Supplementary Services, on page 954 and the subsections that describe the interaction with each service.

Restrictions

The following restrictions apply to MLPP:

- Common Network Facility Preemption support exists only for T1-CAS and T1-PRI (North American) interfaces on targeted Voice over IP gateways that Cisco Unified Communications Manager controls by using MGCP protocol and that have been configured as MLPP Preemption Enabled.

- User Access Channel support exists only for the following Cisco Unified IP Phone models, which must be configured as MLPP Preemption Enabled:
  - Cisco Unified IP Phone 7960, 7962, 7965
  - Cisco Unified IP Phone 7940, 7942, 7945
- IOS gateways support SCCP interface to Cisco Unified Communications Manager. Hence, they support BRI and analog phones which appear on Cisco Unified Communications Manager as supported phone models. SCCP phones support the MLPP feature, and so do some phones with specific SIP loads. See the relevant phone administration and user guides for Cisco IP phone support information.

  .
- Only MLPP Indication Enabled devices generate MLPP-related notifications, such as tones and ringers. If a precedence call terminates at a device that is not MLPP Indication Enabled, no precedence ringer gets applied. If a precedence call originates from a device that is not MLPP Indication Enabled, no precedence ringback tone gets applied. If a device that is not MLPP Indication Enabled is involved in a call that is preempted (that is, the other side of the call initiated preemption), no preemption tone gets applied to the device.
- For phones, devices that are MLPP indication disabled (that is, MLPP Indication is set to Off) cannot be preempted.

  For trunks, MLPP indication and preemption function independently.
- Cisco Unified Communications Manager does not support the Look Ahead for Busy (LFB) option.
- Intercluster trunk MLPP carries precedence information through dialed digits. Domain information does not get preserved and must be configured per trunk for incoming calls.
- 729 Annex A is supported.
- Various location bandwidth preemption limitations exist.
- For the DRSN, CDRs represent precedence levels with values 0, 1, 2, 3, and 4 where 0 specifies Executive Override and 4 specifies Routine, as used in DSN. CDRs thus do not use the DRSN format.
- Cisco Unified Communications Manager preempts lower precedence calls when adjusting video bandwidth for high priority calls. If the bandwidth is not sufficient to preempt, Cisco Unified Communications Manager instructs endpoints to use previously reserved lower video bandwidth. When Cisco Unified Communications Manager preempts a video call, the preempted party receives a preemption tone and the call gets cleared.
- MLPP-enabled devices are not supported in line groups. As such, Cisco recommends the following guidelines:
  - MLPP-enabled devices should not be configured in a line group. Route groups, however, are supported. Both trunk selection and hunting methods are supported.
  - If an MLPP-enabled device is configured in a line group or route group, in the event of preemption, if the route list does not lock onto the device, the preempted call may be rerouted to other devices in the route/hunt list and preemption indication may be returned only after no devices are able to receive the call.
  - Route lists can be configured to support either of two algorithms of trunk selection and hunting for precedence calls. In method 1, perform a preemptive search directly. In method 2, first perform a

friendly search. If this search is not successful, perform a preemptive search. Method 2 requires two iterations through devices in a route list.

If route lists are configured for method 2, in certain scenarios involving line groups, route lists may seem to iterate through the devices twice for precedence calls.

- Turning on MLPP Indication (at the enterprise parameter, common device configuration, or device level) disables normal Ring Setting behavior for the lines on a device, unless MLPP Indication is turned off (overridden) for the device.
- Supplementary Services—MLPP support for supplementary services specifies the following restrictions:
    - The current MLPP design addresses only the basic Call Pickup feature and Group Call Pickup feature, not Other Group Pickup. Support for the Directed Call Pickup feature functions as described in the Call Pickup, on page 957.
    - 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 has been 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 gets sent to the MAP target of the original called party, if the MAP target has been 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 has been configured for forwarding hops. If the maximum hop count gets reached, the call gets sent to the MAP target of the original called party, if the MAP target has been 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.
    - For hunt pilot support, the hunt group algorithm must specify Longest Idle Time, Top Down, or Circular. Ensure the hunt group options for busy treatment, no answer treatment, and unregistered treatment are set to Try next member, but do not go to next group. Preemption only occurs across a single hunt group.

See the Configure MLPP, on page 907 for configuration details.

Install and Activate MLPP

MLPP, a system feature, comes standard with Cisco Unified Communications Manager software and does not require special installation.

MLPP Configuration

This section provides information to set enterprise parameters for MLPP.

Tip Before you configure MLPP, review the configuration summary task for this feature.

Related Topics

Configure MLPP, on page 907

Set the Enterprise Parameters for MLPP

Cisco Unified Communications Manager provides the following enterprise parameters that apply to MLPP. Set the MLPP-related enterprise parameters as indicated to allow MLPP service.

- MLPP Domain Identifier - Default specifies zero (0). Set this parameter to define a domain. Because MLPP service applies to a domain, Cisco Unified Communications Manager only marks connections and resources that belong to calls from MLPP users in a given domain with a precedence level. Cisco Unified Communications Manager can preempt only lower precedence calls from MLPP users in the same domain.

  Note You must reset all devices for a change to this parameter to take effect.

- MLPP Indication Status - Default specifies MLPP Indication turned off. This parameter specifies whether devices use MLPP tones and special displays to indicate MLPP precedence calls. To enable MLPP indication across the enterprise, set this parameter to MLPP Indication turned on.

  Note You must reset all devices for a change to this parameter to take effect.

- MLPP Preemption Setting - Default specifies No preemption allowed. This parameter determines whether devices should apply preemption and preemption signaling (such as preemption tones) to accommodate higher precedence calls. To enable MLPP preemption across the enterprise, set this parameter to Forceful Preemption.

  Note You must reset all devices for a change to this parameter to take effect.

- Precedence Alternate Party Timeout - Default specifies 30 seconds. In a precedence call, if the called party subscribes to alternate party diversion, this timer indicates the seconds after which Cisco Unified Communications Manager will divert the call to the alternate party if the called party does not acknowledge preemption or does not answer a precedence call.
- Use Standard VM Handling For Precedence Calls - Default specifies False. This parameter determines whether a precedence call will forward to the voice-messaging system. If the parameter is set to False, precedence calls do not forward to the voice-messaging system. If the parameter is set to True, precedence calls forward to the voice-messaging system. For MLPP, the recommended setting for this parameter is False, as users, not the voice- -messaging system, should always answer precedence calls.

For more information about enterprise parameters, see the Configure MLPP, on page 907 chapter of the Cisco Unified Communications Manager Administration Guide.

Destination Code Control

Destination Code Control (DCC) limits the number of lower precedence calls that are allowed to a particular destination while allowing an unlimited number of calls for Flash, Flash Override, and Executive Override precedence calls (Flash or higher precedence calls) to that same destination.

A DCC- enabled route pattern allows each Flash or higher precedence calls to proceed, but regulates the percentage of lower precedence calls that are allowed by allowing or disallowing them based on the blocked percentage that is set by the administrator for that destination. The DCC-enabled route pattern limits Immediate, Priority and Routine (lower precedence than Flash) calls in accordance with the call blocking percentage that the administrator configures. In emergency situations, DCC enables the administrator to control the amount of call traffic to a particular destination. At any given time, the number of outgoing low priority calls through the DCC-enabled route pattern are less than or equal to the number of maximum allowed calls configured on that route pattern.

You can set the call blocking percentage on the Route Pattern Configuration window of Cisco Unified Communications Manager.

To access the Apply Call Blocking Percentage check box on the Route Pattern Configuration window, go to **Call Routing** > **Route Hunt** > **Route Pattern**.

Each node on the Cisco Unified Communications Managercluster independently tracks the number of calls to be blocked through it. The following nodes independently track the number of calls being routed through them, without synchronizing the tracking with any other node.

After you enable DCC by selecting the Apply Call Blocking Percentage and setting the call blocking percentage to a certain value, if you then make changes to the Gateway/Route List or Route Class, or any other fields on the Route Pattern window, without changing the blocked call percentage value, then the DCC counters do not get reset, but continue counting based on the number of calls attempted through the route pattern prior to the change. For the DCC counter to reset, there must be a change in the Apply Call Blocking Percentage field.

Note You cannot configure the MLPP level on the Route Pattern window to Flash, Flash Override, or Executive Override levels if you want to enable the DCC feature. You must set these MLPP levels at the translation pattern instead.

AXL

You can configure the DCC feature on the route pattern via the thin AXL layer.

Configuration Requirements

To enable DCC, you must update the following fields:

- Apply Call Blocking Percentage: Check this check box to enable the DCC feature. When DCC is enabled, all calls other than Flash and higher precedence calls that are made to the destination are filtered and allowed or disallowed based on the call blocking percentage quota that is set for the destination. Flash and higher precedence calls are allowed at all times. DCC is disabled by default.

- Call Blocking Percentage (%): Enter the percentage of calls to be blocked for this destination in numerals. This value specifies the percentage of lower precedence calls that are made to this destination that get blocked by the route pattern. This percentage limits the lower precedence calls only; the Flash and higher precedence calls that are made to this destination are allowed at all times.

Note Cisco Unified Communications Manager calculates the maximum number of low priority calls to be allowed through this route pattern based on the call blocking percentage that you set for this destination.

Note The Call Blocking Percentage (%) field gets enabled only if the Apply Call Blocking Percentage check box is checked.

BAT Changes

You can export the DCC details through the Import/Export menu in BAT.

To export DCC details through BAT, go to **Bulk Administration** > **Import/Export** > **Export**. Select the Route Pattern entity for export. The DCC details are found under Call Routing Data.

Note For more details about Import/Export, see the *Cisco Unified Communications Manager Bulk Administration Guide*.

CHAPTER 40

Music On Hold

This chapter provides information about the integrated Music On Hold (MOH) feature, which allows users to place on-net and off-net users on hold with music that is streamed from a streaming source.

Configure Music On Hold

The integrated Music On Hold (MOH) feature allows users to place on-net and off-net users on hold with music that is streamed from a streaming source. The Music On Hold feature allows two types of hold:

- End-user hold
- Network hold, which includes transfer hold, conference hold, and call park hold

Music On Hold also supports other scenarios where recorded or live audio is needed, such as playing a specific MOH depending on the dialed number, caller ID, or IVR interaction of the incoming SIP call. See topics related to caller-specific MOH for more information.

Perform the following steps to configure music on hold.

Procedure

Step 1 The Cisco IP Voice Media Streaming application gets installed automatically upon installation of Cisco Unified Communications Manager. To enable a MOH server, you must use the Cisco Unified Serviceability application to activate the Cisco IP Voice Media Streaming application. When a server is added, the Cisco Unified

Communications Manager automatically adds the media termination point, conference bridge, annunciator, and music on hold devices to the database.

Note During installation, Cisco Unified Communications Manager installs and configures a default music on hold audio source. Music on hold functionality can proceed by using this default audio source without any other changes.

Step 2 Configure the music on hold server.

Step 3 Add and configure audio source files.

Related Topics

Caller-Specific Music On Hold, on page 976
Caller-Specific MOH Interactions and Limitations, on page 976
Configure a Music On Hold Server, on page 1000
Find a Music On Hold Audio Source, on page 991
Music On Hold Audio Sources, on page 978

Configure Multicast

Perform the following steps to configure the various Cisco Unified Communications Manager services to allow multicasting. You must perform all steps for multicast to be available.

Procedure

Step 1 Configure a music on hold server to enable multicast audio sources.

Caution Cisco strongly recommends incrementing multicast on IP address in firewall situations. This results in each multicast audio source having a unique IP address and helps to avoid network saturation.

Step 2 Configure an audio source to allow multicasting.

Note CTI devices do not support the multicast Music On Hold feature. If a CTI device is configured with a multicast MOH device in the media resource group list of the CTI device, call control issues may result. CTI devices do not support multicast media streaming.

Note MTP devices do not support multicast media streaming.

Step 3 Create a media resource group and configure it to use multicast for MOH audio.

Step 4 Create a media resource group list with a multicast media resource group as the primary media resource group.

Step 5 Choose the media resource group list that was created for either a device pool or for specific devices.

Step 6 If necessary, configure the service parameters that affect multicast MOH.

Related Topics

Music On Hold Audio Source Configuration Settings, on page 993
Music On Hold Server Configuration, on page 1001
Multicast and Unicast Audio Sources, on page 979

Multicast Music On Hold Over H.323 Intercluster Trunks, on page 981

Configure Monitoring Music On Hold Performance

Perform the following steps to monitor music on hold performance.

Procedure

Step 1 Use the Cisco Unified Communications Manager Real Time Monitoring Tool (RTMT) to check resource usage and device recovery state.

Step 2 Search the event log for Cisco IP Voice Media Streaming application entries.

Step 3 Verify that the Cisco IP Voice Media Streaming application service is running.

Step 4 Verify that the MoH device is registered.

Step 5 Search the Media Application trace (CMS) to see what music on hold-related activity that it detects.

Music On Hold Feature

The following sections explain the Music On Hold feature by providing definitions, service characteristics, feature functionality with examples, and supported features.

Music On Hold Terminology

In the simplest instance, music on hold takes effect when phone A is talking to phone B, and phone A places phone B on hold. If Music On Hold (MOH) resource is available, phone B receives music that is streamed from a music on hold server.

The following definitions provide important information for the discussion that follows:

- MOH server - A software application that provides music on hold audio sources and connects a music on hold audio source to a number of streams.
- Media resource group - A logical grouping of media servers. You may associate a media resource group with a geographical location or a site as desired. You can also form media resource groups to control server usage or desired service type (unicast or multicast).
- Media resource group list - A list that comprises 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.
- Audio source ID - An ID that represents an audio source in the music on hold server. The audio source can compose either a file on a disk or a fixed device from which a source stream music on hold server obtains the streaming data. A MOH server can support up to 51 audio source IDs (1 to 51). Each audio source (represented by an audio source ID) can stream as unicast and multicast mode, if needed.

- Holding party - In an active, two-party call, the party that initiates a hold action (either user hold or network hold). Example: If party A is talking to party B, and party A presses the Hold softkey to initiate a hold action, party A represents the holding party.
- Held party - In an active, two-party call, the party that does not initiate a hold action but is involved. Example: If party A is talking to party B, and party A presses the Hold softkey to initiate a hold action, party B represents the held party.

The following audio source ID selection rules apply for selecting audio source IDs and media resource group lists:

- The system administrator, not the end user, defines (configures) audio source IDs.
-
- Holding parties define which audio source ID applies to held parties.
- Cisco Unified Communications Manager implements four levels of prioritized audio source ID selection with level four as highest priority and level one as lowest priority.
  - The system selects audio source IDs at level four, which is directory/line-based, if defined. (Devices with no line definition, such as gateways, do not have this level.)
  - If no audio source ID is defined in level four, the system searches any selected audio source IDs in level three, which is device based.
  - If no level four nor level three audio source IDs are selected, the system selects audio source IDs that are defined in level two, which is Common Device Configuration-based.
  - If all higher levels have no audio source IDs selected, the system searches level one for audio source IDs, which are clusterwide parameters.

The following media resource group list selection rules apply:

- Held parties determine the media resource group list that a Cisco Unified Communications Manager uses to allocate a music on hold resource.
- Two levels of prioritized media resource group list selection exist:
  - Level two media resource group list provides the higher priority level, which is device based. Cisco Unified Communications Manager uses the media resource group list at the device level if such a media resource group list is defined.
  - Level one media resource group list provides the lower priority level, which is an optional DevicePool parameter. Cisco Unified Communications Manager uses the DevicePool level media resource group list only if no media resource group list is defined in the device level for that device.
- If no media resource group lists are defined, Cisco Unified Communications Manager uses the system default resources. System default resources comprise resources that are not assigned to any existing media resource group. Be aware that system default resources are always unicast.

Music On Hold Characteristics

The integrated Music On Hold feature allows users to place on-net and off-net users on hold with music that is streamed from a streaming source. This source makes music available to any possible on-net or off-net device that is placed on hold. On-net devices include station devices and applications that are placed on hold, consult hold, or park hold by an interactive voice response (IVR) or call distributor. Off-net users include those who are connected through Media Gateway Control Protocol (MGCP)/skinny gateways, IOS H.323 gateways, and 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 FXS ports on IOS H.323/Media Gateway Control Protocol and for Cisco Media Gateway Control Protocol/skinny gateways.

The integrated Music On Hold feature covers media server, data base administration, call control, media resource manager, and media control functional areas.

The music on hold server provides the music resources/streams. These resources register with the Cisco Unified Communications Manager during the initialization/recovery period.

Database administration provides a user interface to allow the Cisco Unified Communications Manager administrator to configure the Music On Hold feature for the device(s). Database administration also provides Cisco Unified Communications Manager call control with configuration information.

Call control controls the music on hold scenario logic.

The media resource manager processes the registration request from the music on hold server and allocates/deallocates the music on hold resources under the request of call control.

Media control controls the establishment of media stream connections, which can be one-way or two-way connections.

You must ensure that an end device is provisioned with information that is related to music on hold before music on hold functions for that device. Initializing a Cisco Unified Communications Manager creates a media resource manager. The music on hold server(s) registers to the media resource manager with its music on hold resources.

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.

Music On Hold Functionality

For music on hold to function, you must perform the actions in the following list:

- Configure audio sources. For the examples that follow, configure and provision the following audio sources: (ID#5) Thank you for holding and (ID#1) Pop Music 1.
- Configure music on hold servers.
- Configure audio sources. For the examples that follow, configure and provision the following audio sources: Thank you for holding and Pop Music 1.

Note Define audio sources first and then set up the music on hold servers, especially when multicast will be used. The user interface allows either step to take place first.

Note If an audio source is configured for multicast, the MoH server always transmits the audio stream, regardless of whether devices are held.

- Configure media resource groups. If multicast is desired, check the Use Multicast for MoH Audio check box.

Note CTI and MTP devices do not support the multicast Music On Hold feature. If a CTI or MTP device is configured 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.

- Configure media resource group lists.
-
- Assign media resource group lists and audio sources to devices (to override assignments made to device pools).
- Assign audio sources to lines (to override device settings).

Using the preceding configuration actions, if you define music on hold functionality as follows, the examples that follow demonstrate music on hold functionality for user hold, transfer hold, and call park.

Media Resource Groups

MoH designates a music on hold server. MRG designates a media resource group.

- MRG_D comprises MOH_D.
- MRG_S_D comprises MOH_S and MOH_D.

Media Resource Group Lists

MRGL designates a media resource group list.

- MRGL_D comprises MRG_D.
- MRGL_S_D comprises MRG_S_D and MRG_D (prioritized order).

Nodes

- Dallas node comprises phone D and MOH_D.
- San Jose node comprises phone S and MOH_S.
- Assign phone D audio source ID 5, Thank you for holding or plain music (for both user and network hold), and MRGL_D.
- Assign phone S audio source ID 1, Pop Music 1 (for both user and network hold), and MRGL_S_D.

User Hold Example

Phone D calls phone S, and phone S answers. Phone D presses the Hold softkey. Result: Phone S receives Thank you for holding announcement or plain music that is streaming from MOH_S. (MOH_S has available streams.) When phone D presses the Resume softkey, phone S disconnects from the music stream and reconnects to phone D.

Transfer Hold Example

Transfer hold serves as an example of network hold.

Phone D calls phone S, and phone S answers. Phone D presses the Transfer softkey. Phone S receives Thank you for holding announcement or plain music that is streaming from MOH_D. (MOH_S has no available streams, but MOH_D does.) After phone D completes the transfer action, phone S disconnects from the music stream and gets redirected to phone X, the transfer destination.

Call Park Example

Call park serves as an example of network hold.

Phone D calls phone S, and phone S answers. Phone S presses the CallPark softkey. Phone D receives a beep tone. (MOH_D has no available streams.) Phone X picks up the parked call. Phone S gets redirected to phone X (phone D and phone X are conversing).

Supported Music On Hold Features

Music On Hold supports the following features, which are listed by category. Feature categories include internet protocol, music on hold server characteristics, server scalability, server manageability, server redundancy, database scalability, and manageability.

Internet Protocol

Unicast Music On Hold provided by the Cisco IP Voice Media Streaming Application service supports both IPv4 and IPv6 audio media connections. Unicast Music On Hold is configured automatically in dual mode when the platform is configured for IPv6 and the IPv6 enterprise parameter is enabled. Music On Hold supports only IPv4 for the TCP control channel. Music On Hold supports secure media SRTP connections to both IPv4 and IPv6 addresses.

Note Multicast Music On Hold supports only IPv4.

Music On Hold Server Characteristics

- Servers stream music on hold from music on hold data source files that are stored on their disks.
- Servers may stream music on hold from an external audio source (for example, looping tape recorder, radio, or CD).
- Music on hold servers can use a single music on hold data source for all source streams and, hence, all connected streams. When multiple music on hold servers are involved, the local server of each music on hold server always stores the music on hold data source files. Cisco Unified Communications Manager does not support distribution of fixed-device (hardware) audio sources across music on hold servers within a media resource group.
- Music on hold data source files have a common filename across all music on hold servers.
- You must ensure that music on hold data source files are uploaded to each MoH server.
- Each audio source receives a feed from either a designated file or a designated fixed source (for example, radio or CD).

- A designated fixed source comprises a single device, which is either enabled or disabled.
- The audio driver on the local machine makes a single fixed source available to the music on hold server.
- Music on hold servers support the G.711 (a-law and mu-law), G.729a, and wideband codecs.
- Music on hold servers register with one primary Cisco Unified Communications Manager node.

Server Scalability

- Music on hold supports from 1 to 1000 simplex unicast streams per music on hold server.
- Music on hold supports multiple Cisco-developed media-processing applications, including Interactive Voice Response (IVR) and Auto-Attendant (AA). Cisco Unified Communications Manager facilitates this support.
- Music on hold server simultaneously supports up to 50 music on hold data source files as sources.
- Music on hold server supports one fixed-device stream source in addition to the file stream sources. This source comprises the fixed audio source, which gets configured on the Fixed MoH Audio Source Configuration window. This source requires the additional Cisco USB Music-On-Hold-capable adapter.

Server Manageability

- 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 node(s) that supply MOH from an external source.
- The administrator can specify the source for each source stream that the server provides.
- Administration of stream sources takes place through a browser.

Server Redundancy

- Music on hold servers support Cisco Unified Communications Manager lists based on associated Call Manager Group settings. The first entry on the list serves as the primary server, and subsequent Cisco Unified Communications Managers on the list serve as backup Cisco Unified Communications Managers in prioritized order.
- Music on hold servers can maintain a primary and backup connection to Cisco Unified Communications Managers from their Cisco Unified Communications Manager list.
- Music on hold servers can re-home to backup Cisco Unified Communications Managers by following the standard procedures that are used by other servers and phones on the cluster.
- Music on hold servers can re-home to their primary server by following standard procedures for other media servers on the cluster.

Cisco Unified Communications Manager Database Requirements

- When a Cisco Unified Communications Manager is handling a call and places either endpoint in the call on hold, the Cisco Unified Communications Manager can connect the held endpoint to music on hold.

This feature applies for both network hold and user hold. Network hold includes transfer, conference, call park, and so forth.

- A media resource group for music on hold supports having a single music source stream for all connected streams.
- The system supports having music on hold server(s) at a central site without music on hold server(s) at remote sites. Remote site devices that require music on hold service can obtain service from a media resource group across the WAN when service is not available locally.
- You can distribute music on hold servers to any site within a cluster.
- A music on hold server can use a single music on hold data source for all source streams and, hence, all connected streams. When multiple music on hold servers are involved, the music on hold data source may comprise a file that is stored locally on each server.
- The system can detect when the primary media resource group that supplies music on hold for a device is out of streams and can select a stream from the secondary or tertiary media resource group that is specified for that device.
- When it connects a device to music on hold, the system can insert a transcoder when needed to support low-bandwidth codecs.

Database Scalability

- Cisco Unified Communications Manager can support from 1 to 500 unicast sessions per music on hold server.
- A cluster can support from 1 to more than 20 music on hold servers.
- A cluster can support from 1 to more than 10,000 simultaneous music on hold streams across the cluster.
- A cluster can support from 1 to 500 or more media resource groups for music on hold.
- A media resource group for music on hold can support from 1 to 20 or more music on hold servers.

Manageability

- The administrator can select media resource group list per device.
- The administrator can select music on hold source stream per device/DN.
- The administrator can select music on consult (network hold) source stream per device/DN.
- The administrator can configure which music on hold servers are part of a specified media resource group.
- The administrator can designate primary, secondary, and tertiary music on hold/consult servers for each device by configuring media resource groups and media resource group lists.
- The administrator can provision multiple music on hold servers.
- The administrator can provision any device that is registered with the system such that any music on hold server can service it in the system.
- All music on hold configuration and administration take place through a browser.
-

- The administrator can designate a music on hold server as either unicast or multicast, provided that resources exist to support multicast.

Note CTI devices do not support the multicast Music On Hold feature. If a CTI device is configured with a multicast MoH device in the media resource group list of the CTI device, call control issues may result. CTI devices do not support multicast media streaming.

- The administrator can reset all music on hold servers.

Caller-Specific Music On Hold

Cisco Unified Communications Manager can play a different MOH audio source for SIP calls that a phone receives over the SIP trunk, which are then put on hold.

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 PSTN. After the Unified CVP plays prompts and collects information from the user, the MOH stream IDs for user and network hold are relayed to Cisco Unified Communications Manager over the SIP trunk.

After the signaling that contains the MOH audio source stream IDs is received, the call is routed to an agent on the Cisco Unified Communications Manager cluster. If the agent places the call on hold, the caller is played the appropriate MOH audio source according to the signaling information that has been received. If the agent transfers the call to another agent, the caller-specific MOH information in the SIP header is transferred along with the call. You can transfer calls to an agent on the same cluster or to an agent on a different cluster over an SME using SIP trunks.

Caller-Specific MOH Interactions and Limitations

If the incoming SIP call contains MOH audio source information in the SIP header, Cisco Unified Communications Manager initiates the following actions:

- The MOH audio source is played for the caller when the SIP call is placed on user hold.
- The MOH audio source is played for the caller when the SIP call is placed on network hold.
- The MOH audio source is played for the caller if the call is transferred to another endpoint on the same cluster and subsequently placed on user or network hold.
- When a call is sent on a SIP trunk to another cluster, the MOH audio source information is sent along with the call.
- When a call is sent on a SIP trunk to another cluster in an SME scenario, the MOH audio source information is sent along with the call.
- When a call is transferred to another cluster over a SIP trunk, the MOH audio source information is sent along with the call.

- When a call is either forwarded or redirected to another cluster over a SIP trunk, the MOH audio source information is sent along with the call.

Limitations

- If the user and network MOH audio source identifiers are not provisioned, 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.
- 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 0, or the only value is 0, the header in the incoming INVITE is ignored.
- If only one MOH audio source identifier is provided 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 are responsible to maintain consistent caller-specific MOH configurations when multiple Cisco Unified Communications Manager clusters are involved.
- The original incoming caller to the call center cannot change during the course of the entire call.
- The music on hold information is only shared across SIP trunks.
- Caller-specific MOH is not supported when calls are received or transferred over QSIG tunneling-enabled SIP trunks.

Music On Hold Server

The music on hold server uses the Station Stimulus (Skinny Client) messaging protocol for communication with Cisco Unified Communications Manager. A music on hold server registers with the Cisco Unified Communications Manager as a single device and reports the number of simplex, unicast audio streams that it can support. The music on hold server advertises its media type capabilities to the Cisco Unified Communications Manager as G.711 mu-law and a-law, G.729a, and wideband. Cisco Unified Communications Manager starts and stops music on hold unicast streams by sending skinny client messages to the music on hold server.

A music on hold server handles up to 1000 simplex, unicast audio streams. A media resource group includes one or more music on hold servers. A music on hold server supports 51 audio sources, with one audio source that is sourced from a fixed device that uses the local computer audio driver, and the rest that are sourced from files on the local music on hold server.

You may use a single file for multiple music on hold servers, but the fixed device may be used as a source for only one music on hold server. The music on hold audio source files get stored in the proper format for streaming. Cisco Unified Communications Manager allocates the simplex unicast streams among the music on hold servers within a cluster.

The music on hold server, which is actually a component of the Cisco IP Voice Media Streaming application, supports standard device recovery and database change notification.

Each music on hold server uses the local hard disk to store copies of the Music On Hold audio source files. Each audio source file gets distributed to the node(s) when the file is added through the Cisco Unified Communications Manager Administration interface.

Note The administrator must upload Music On Hold audio source files to each MoH server.

Video on Hold (VoH) can be provided instead of MoH by including a VoH server in the Media Resource Group and Media Resource Group List configuration for the Held party. Only the default video configured for the VoH server will be played if the VoH server is selected.

Music On Hold Audio Sources

When the administrator imports an audio source file, the Cisco Unified Communications Manager Administration interface processes the file and converts the file to the proper format(s) for use by the music on hold server.

- The recommended format for audio source files includes the following specifications:
- 16-bit PCM wav file
- Stereo or mono
- Sample rates of 48 kHz, 32 kHz, 16 kHz, or 8 kHz

Create Audio Sources

Most standard wav files serve as valid input audio source files, including the following file types:

- 16-bit PCM wav file
- Stereo or mono
- Sample rates of 48 kHz, 44.1 kHz, 32 kHz, 16 kHz, or 8 kHz

Note The Music On Hold feature does not support the MP3 format.

In creating an audio source, the following sequence takes place:

- The administrator imports the audio source file into the Cisco Unified Communications Manager music on hold server. This step may take some time to transfer the file and convert the file to the proper format(s) for the music on hold server to use.
- The administrator must import the audio source file to each MoH server in each cluster prior to assigning an audio source number to the audio source file.
- The music on hold server uses the local audio source file(s).
- The music on hold server streams the files to held devices Cisco Unified Communications Manager needs or requests.

Store Audio Source Files

In previous releases, Cisco Unified Communications Manager did not limit the amount of space that MoH files used. The MoH upload tool does not limit the number of uploaded files or the file size. The modified upload JSP pages check the disk usage of existing MoH files and only permit uploads if sufficient space is found.

Note The smallest node on the cluster controls MOH capacity.

Manage Audio Sources

After music on hold audio sources are created, their management occurs entirely through Cisco Unified Communications Manager Administration. Choose **Media Resources** > **Music On Hold Audio Source** to display the Music On Hold (MOH) Audio Source Configuration window. For a given audio source, use this window to add, update, or delete a music on hold audio source. For each audio source file, assign a music on hold audio source number and music on hold audio source name and decide whether this audio source will play continuously and allow multicasting. For an audio source, this window also displays the music on hold audio source file status. See the Find a Music On Hold Audio Source, on page 991 for details.

Note The Music On Hold Audio Source Configuration window uploads audio source files only to a particular node. The window does not provide for automatic copying of audio source files to any other nodes. You must manually upload audio source files to subscriber nodes by accessing the Cisco Unified Communications Manager application on each node.

Uploading a New Audio File and the Old File Still Plays

Problem When you upload an audio file with the same name as an existing file that is mapped to an Audio Source ID, your users may hear the existing file still playing back.

Solution To ensure that the updated file is played, follow these steps:

1. After you upload the new audio file to replace the old one, find the audio source ID you want to change under the **Music On Hold Audio Source Configuration** window.
2. Select a different audio source file, such as the default **SampleAudioSource** and then click **Save**.
3. Switch the source file back to your file you want to use, and then click **Save**.
4. Reset the Music On Hold server so that the changes take effect.

Multicast and Unicast Audio Sources

Multicast music on hold conserves system resources. Multicast allows multiple users to use the same audio source stream to provide music on hold. Multicast audio sources associate with an IP address.

Unicast music on hold, the system default, uses a separate stream for each user or connection. Users connect to a specific device or stream.

Note 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 will be heard from the beginning. For multicast users this announcement will not be heard.

Note The MoH feature causes any party that gets placed on hold to hear the same point of the audio source that is streaming, regardless of when the party is placed on hold.

Note If you are using the MoH to deliver a spoken announcement when a party is placed on hold, the standard MoH configuration can create a problem. Users do not hear the announcement from the beginning, except for the first party that gets placed on hold: other parties join the announcement (audio source) in progress.

Note Both multicast and unicast configurations present the same audio-source behavior to held parties. Each audio source gets used once, and the stream gets split internally and gets sent to the held parties. The only difference between multicast and unicast, in this case, is how the data itself gets sent over the network.

Note A MoH audio source may be configured with a periodic announcement that is inserted in the basic MoH audio on a configurable periodic interval. This announcement is heard by both unicast and multicast users. However, the user may be inserted into the MoH audio stream at a point when this announcement is in the middle of being played. This is dependent on whether other held users are already hearing the MoH audio source.

For administrators, multicast entails managing devices, IP addresses, and ports. In contrast, unicast entails managing devices only.

For multicast, 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.

For multicast, an address comprises a combination of an IP address and a port number. Each audio source for multicast requires a set of addresses: one for each format on each MoH server. When configuring the MoH server for multicast, specify whether addresses should be assigned by incrementing the port or the IP address.

Caution Cisco strongly recommends incrementing multicast on IP address instead of port number to avoid network saturation in firewall situations. If you follow this recommendation, each multicast audio source has a unique IP address, and you help to avoid network saturation.

The Max Hops field in the Music On Hold (MoH) Server Configuration window indicates the maximum number of routers that an audio source is allowed to cross. If max hops is set to zero, the audio source must remain in its own subnet. If max hops is set to one, the audio source can cross up to one router to the next subnet. Cisco recommends setting max hops to two.

A standards body reserves IP addresses. Addresses for IP multicast range from 224.0.1.0 to 239.255.255.255. The standards body, however, assigns addresses in the range 224.0.1.0 to 238.255.255.255 for public multicast applications. Cisco strongly discourages using public multicast addresses for music on hold multicast. Instead, Cisco recommends using an IP address in the range that is reserved for administratively controlled applications on private networks (239.0.0.0 to 239.255.255.255).

Valid port numbers for multicast include even numbers that range from 16384 to 32767. (The system reserves odd values.)

Multicast 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. Such servers get labeled as (MOH)[Multicast]. Also, check the Use Multicast for MOH Audio check box when you define a media resource group for multicast.

For media resource group lists, which are associated with device pools and devices, define the media resource group list, so the media resource group that is set up for multicast is the first group in the list. This recommended practice facilitates the device efforts to find the multicast audio source first.

In music on hold processing, the held device (the device placed on hold) determines the media resource to use, but the holding device (the device that initiates the hold action) determines the audio source to use.

Note The following restriction exists for multicast music on hold (MoH) when a media termination point (MTP) is invoked. 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.

Note CTI devices do not support the multicast Music On Hold feature. If a CTI device is configured with a multicast MoH device in the media resource group list of the CTI device, call control issues may result. CTI devices do not support multicast media streaming.

Multicast MoH Direction Attribute for SIP Service Parameter

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 loads 8.4 and earlier for Cisco Unified IP Phones 7940 and 7960, or SIP phone loads 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 Music On Hold Over H.323 Intercluster Trunks

The Multicast Music on Hold (MOH) Over H.323 Intercluster Trunk feature allows multicast MOH to work over H.323 intercluster trunks (ICTs). Prior to the implementation of this feature, multicast MOH used bandwidth for each unicast MOH over the same ICT, which wasted bandwidth.

Prior to the implementation of this feature, the H.323 Open Logical Channel (OLC) ACK message carried the IP address and port for multicast MOH. With the implementation of this feature, the H.323 OLC message now carries the IP address and port for multicast MOH, and Cisco Unified Communications Manager adds the mechanism to handle the information in the H.323 OLC message.

When a call connects over an intercluster trunk and one of the parties presses the Hold key, MOH streams over the intercluster trunk. If multicast MOH is turned on and the holding party and trunk are configured to use the multicast MOH server, MOH streams with multicast. Only one multicast MOH stream streams over the trunk regardless how many calls are put on hold on this trunk.

Send Multicast MOH in H.245 OLC Message Service Parameter

The service parameter, Send Multicast MOH in H.245 OLC Message, controls the Multicast Music On Hold Over H.323 Intercluster Trunk feature. Both Cisco Unified Communications Manager nodes that are involved in a call must support single-transmitter multicast for the setting of this parameter to have any effect. This service parameter affects only the side of the party that places the call on hold and does not affect how the far end carries the multicast transport address. Even if this parameter is turned off, multicast MOH applies for the held-party side of the call as long as the held party has the capability to support single-transmitter multicast.

If you want to configure this feature via the clusterwide service parameter, Send Multicast MOH in H.245 OLC Message, which supports the Cisco CallManager service, choose **System** > **Service Parameters** in Cisco Unified Communications Manager Administration. Then, choose the server and the Cisco CallManager service. From the Send Multicast MOH in H.245 OLC Message drop-down list box, choose True.

The service parameter governs the multicast MOH behavior on H.323 intercluster trunks and devices. The new service parameter does not control multicast MOH over SIP trunks because multicast MOH over SIP trunks does not constitute a new behavior.

Cisco Unified Communications Manager Administration Configuration Tips

Calls that connect over Cisco Unified Communications Manager intercluster trunks use this feature for 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.

No additional configuration exists for this new feature in addition to the normal configuration for setting up multicast MOH. This feature only applies 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. Do so to resolve interoperability issues that the feature may cause.

Note Multicast MOH does not support interoperability between H.323 and SIP protocols.

Secured Music On Hold Through SRTP

Cisco Unified Communications Manager 8.6(1) and later enhances the Cisco IP Voice Media Streaming application service to support Secure Real-Time Protocol (SRTP); therefore, when the Cisco Unified Communications Manager cluster or system is enabled for security, the MOH server registers with the 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 check box, indicating that it is a trusted device.

When the Cisco Unified Communications Manager is configured in a secure deployment environment (the Cluster Security Mode enterprise parameter is set to mixed mode), Cisco Unified IP Phones, voice gateways, and other secure capable endpoints are set to encrypted mode. The media streaming between the devices is done through SRTP. When calls are secure, a locked icon displays on the Cisco Unified IP Phone, indicating that the call is protected for both signaling and media.

Note When Cisco Unified Communications Manager interrupts the media of an encrypted call, such as when call features are activated, the locked icon is removed from the Cisco Unified IP Phone. The icon is restored when the phone reconnects with the encrypted media. The duration of the media interruption and restoration is short when encrypted Music On Hold is activated.

Note Multicast MoH audio streams are not encrypted and do not support SRTP.

Enable Security for Music On Hold

Music On Hold devices are automatically enabled for security when the enterprise parameter Cluster Security Mode is set to 1 (mixed mode). To configure the Cluster Security Mode enterprise parameter, see Find a Music On Hold Audio Source, on page 991

Secured and Non-Secured Music On Hold

The following examples provide scenarios that describe how the locked icon displays when secured and non-secured MOH is inserted into calls.

When a secured MLPP precedence call is put on hold, Cisco Unified Communications Manager inserts a secured MOH to the held party. The media is encrypted and streamed to the held party through SRTP. The secure locked icon displays on the user’s phone.

Example

The following example shows an encrypted MOH for a precedence call.

1. User 2000 dials 77 1000 to reach user 1000. Cisco Unified Communications Manager configured a translation pattern of 77.XXXX to enable users to dial a prefix of 77 to initiate an MLPP Immediate call.

2. Cisco Unified Communications Manager dials user 1000 and user 1000 answers the call.

3. The media between user 2000 and user 1000 is set up with SRTP; therefore, the secure locked icon displays on both IP phones.

4. User 2000 presses the Hold key and Cisco Unified Communications Manager disconnects the media connection between user 2000 and user 1000 and inserts MOH to the device of user 1000. The encrypted

MOH media streams to user 1000 by using SRTP. The locked icon on the IP phone of user 1000 is maintained while MOH plays.

Example

The following example shows an encrypted MOH for an unsecured call.

1. User 1000 dials user 2000.
2. User 2000 answers the call.
3. The media streaming between user 1000 and user 2000 is unencrypted because the IP phone of user 1000 is not secure.
4. User 1000 presses the Hold key and Cisco Unified Communications Manager disconnects the media connection between user 1000 and user 2000. Cisco Unified Communications Manager inserts MOH to user 2000. Because both the MOH server and the device of user 2000 are capable of encryption, the MOH media plays to user 2000 by using SRTP.

Example

The following example describes secured MOH playing unencrypted music on hold to an unsecured device.

If a phone is unsecured, when a call on the device is placed on hold, the MOH that is inserted streams unencrypted media to the phone.

1. User 1000 dials 2000.
2. User 2000 answers the call. User 1000’s IP phone is an unsecured device.
3. The media stream between user 2000 and user 1000 is set up with RTP.
4. User 2000 presses the Hold key and Cisco Unified Communications Manager disconnects the media connection between user 2000 and user 1000 and inserts music on hold to user 1000. Although MOH is capable of encryption, the receiving device is not SRTP capable; therefore, MOH streams to user 1000 by using RTP.

Example

The following example describes an unsecured MOH being inserted into a precedence call when the security of MOH is overridden.

If the advanced service parameter Make MOH Non-secure when Cluster Security is Mixed is set to True, the MOH server does not register with Cisco Unified Communications Manager as an SRTP capable device.

1. User 2000 dials user 1000.
2. User 1000 answers the call.
3. The media stream between user 2000 and user 1000 is set up with sRTP. Both IP phones display the locked icon.
4. User 2000 presses the Hold key and Cisco Unified Communications Manager disconnects the media connection between user 2000 and user 1000 and inserts MOH to user 1000. Because the advanced service parameter Make MOH Non-secure when Cluster Security is Mixed is set to True, MOH is streamed to user 1000 by using RTP.

Example

The following example describes an encrypted Annunciator being inserted for Tone On Hold (TOH).

In cases when MOH is not available, the Annunciator could be inserted to a held party to play Tone On Hold.

For more information about Annunciator, see **Secured and Non-Secured Music On Hold**

1. User 2000 in the local cluster or system dials 86000 to reach user 6000 in the remote cluster or system via the SIP trunk linking the two clusters systems.
2. User 6000 in the remote cluster or system answers the call.
3. The media connection between user 2000 and user 6000 is set up with SRTP; therefore, both IP phones display the secure locked icon.
4. User 6000 in the remote cluster or system presses the Hold key.
5. Cisco Unified Communications Manager in the remote cluster or system disconnects the media connection between user 2000 and user 6000 and inserts the Annunciator to user 6000 via the SIP trunk.

Example

The following example describes a consultation transfer of a secured call to an SRTP capable device.

When a secured call is transferred, when the caller transferring the call presses the Transfer key, the call is effectively put on hold; therefore, MOH is inserted into the call until the caller transferring the call presses the Transfer key again to complete the transfer.

If the MOH server is also a secured device, the security status of the caller to which the call is being transferred is not downgraded and the call maintains its security status throughout the transfer process.

1. User 2000 dials user 1000.
2. User 1000 answers the call.
3. The media streaming between user 1000 and user 2000 is encrypted. The IP phones of both users displays the secure locked icon.
4. User 2000 presses the Transfer key.
5. Cisco Unified Communications Manager disconnects the media connection between user 1000 and user 2000 and inserts MOH to user 1000. Because both the MOH server and user 1000’s IP phone are capable of encryption, the MOH media plays to user 1000 by using SRTP. The locked icon continues to display on user 1000’s phone.
6. User 2000 dials user 3000.
7. User 3000 answers the call.
8. The encrypted media connection is established for the consultation call. The locked icon displays on the phones of both user 2000 and user 3000.
9. User 2000 presses the Transfer key again and Cisco Unified Communications Manager disconnects the media connection between user 2000 and user 3000 and encrypted media is then established between user 3000 and user 1000. the locked icons display on the IP phones of both user 3000 and user 1000.

Example

The following example describes a consultation transfer of a secured call to an unsecured device.

1. User 2000 dials user 1000.
2. User 1000 answers the call.
3. The media streaming between user 1000 and user 2000 is encrypted and the locked icon displays on the IP phones of user 1000 and user 2000.
4. User 2000 presses the Transfer key.
5. Cisco Unified Communications Manager disconnects the media connection between user 1000 and user 2000 and inserts MOH to user 1000. Because both the MOH server and the receiving device are capable of encryption, the MOH media plays to user 1000 by using SRTP. The locked icon on user 1000’s IP phone is maintained.
6. User 2000 dials user 3000.
7. User 3000 answers the call.
8. Because user 3000 is not capable of SRTP, no secure locked icon displays on the IP phone of user 2000 and user 3000.
9. User 2000 presses the Transfer key again. Cisco Unified Communications Manager disconnects the media between user 2000 and user 3000 and unencrypted media is then established between user 3000 and user 1000. The locked icons on the IP phone of user 1000 disappears.

Example

The following example describes a consultation transfer of an unsecured call to an SRTP capable device.

In the example, the secure locked icon displays on the device of the caller to which the call was transferred as soon as the caller who transfers the call presses the Transfer key.

1. User 2000 dials user 1000.
2. User 1000 answers the call.
3. The media streaming between user 1000 and user 2000 is unencrypted because the IP phone of user 2000 is not SRTP capable.
4. User 2000 presses the Transfer key.
5. Cisco Unified Communications Manager disconnects the media connection between user 1000 and user 2000 and inserts MOH to user 1000. Because both the MOH server and the receiving device for user 1000 are capable of encryption, the MOH media plays to user 1000 by using SRTP. The locked icon displays on the IP phone of user 1000.
6. User 2000 dials user 3000.
7. User 3000 answers the call.
8. User 2000 presses the Transfer key again and Cisco Unified Communications Manager disconnects the media connection between user 2000 and user 3000. Encrypted media is then established between user 3000 and user 1000 because both devices are SRTP capable. The locked icon displays on the IP phone for user 1000 and user 3000.

Example

The following example describes a blind transfer of a secured call to an SRTP capable device.

If the caller who is transferring a call presses the Transfer key immediately after dialing the transfer-to-target numbers, the secured MOH is inserted briefly and then removed while the transfer-to-target is ringing. The caller to which the call is transferred hears a ringback tone. Because no media is connected to the caller to which the call is being transferred, no secure locked icon displays on the IP phone. The locked icon displays only when the call is answered.

1. User 2000 dials user 1000.
2. User 1000 answers the call.
3. The media streaming between user 1000 and user 2000 is encrypted. The locked icon displays on the IP phone of user 1000 and user 2000.
4. User 2000 presses the Transfer key.
5. Cisco Unified Communications Manager disconnects the media connection between user 1000 and user 2000 and inserts MOH to user 1000. Because both the MOH server and the receiving device for user 1000 are capable of encryption, the MOH media plays to user 1000 by using SRTP. The locked icon displays on the IP phone of user 1000.
6. User 2000 dials user 3000 and then presses the Transfer key again.
7. The IP phone for user 3000 rings. Cisco Unified Communications Manager removes the MOH from user 1000 and ringback begins on the IP phone for user 1000 while the IP phone for user 3000 rings. The locked icon is removed from the IP phone for user 1000.
8. User 3000 answers the call.
9. The encrypted media connection is established between the IP phone for user 1000 and user 3000. The locked icon displays on the IP phone for user 1000 and user 3000.

Example

The following example describes a blind transfer of a secured call in a remote cluster or system.

system.In this example, when user 5000 blind transfers the call to user 6000, Cisco Unified Communications Manager in the remote cluster or system first inserts MOH to user 2000 in the local cluster or system, then removes it and inserts Annunciator to user 2000 to play ringback tones. When user 6000 answers the call, the media between user 2000 and user 6000 connects.

When the Annunciator, MOH, and user 6000 in the remote cluster or system all support SRTP, the locked icon on the IP phone for user 2000 displays throughout the entire blind transfer process.

For more information about Annunciator, see the following figure

1. User 2000 dials 85000 to reach user 5000 in the remote cluster or system.
2. User 2000 in the remote cluster or system answers the call.
3. The encrypted media is established between user 2000 and user 5000 in the remote cluster or system. The locked icon displays on the IP phones for user 2000 and user 5000.
4. User 5000 in the remote cluster or system presses the Transfer key.

5. Cisco Unified Communications Manager in the remote cluster or system disconnects the media between user 5000 and user 2000 in the local cluster or system and inserts MOH to user 2000 in the local cluster or system. Because both the MOH server and the receiving IP phone for user 2000 are capable of encryption, the MOH media plays to user 2000 by using SRTP. The locked icon is maintained on the IP phone for user 2000.
6. User 5000 dials user 6000 and presses the Transfer key again.
7. Cisco Unified Communications Manager in the remote cluster or system dials user 6000.
8. Cisco Unified Communications Manager in the remote cluster or system removes the MOH and inserts Annunciator to user 2000 to play the inband ringback tone. Because both the Annunciator and the IP phone for user 2000 is capable of encryption, the ringback tone plays by using SRTP. The locked icon is maintained on the IP phone for user 2000 while the phone receives the ringback tone.
9. User 6000 in the remote cluster or system answers the call.
10. The encrypted media is established between user 2000 and user 6000 in the remote cluster or system. The locked icon displays on the IP phones for user 2000 and user 6000.

Note Ensure that the SIP trunk is set to encrypted mode and check the SRTP Allowed check box on the SIP trunk page.

Music On Hold System Requirements and Limits

The following system requirements and limits apply to the Music On Hold feature:

- All audio streaming devices that are using the Music On Hold feature support simplex streams. The music on hold server supports up to 1000 simplex streams.
- The music on hold (MOH) server, a part of the Cisco IP Voice Media Streaming application, gets installed with Unified Communications Manager. Use the Cisco Unified Serviceability application to activate the MOH server. You can activate the Cisco IP Voice Media Streaming application on multiple nodes to provide multiple MOH servers for the cluster.
- For a Unified Communications Manager cluster, you may define up to 50 audio sources. For a Unified Communications Manager system, you may define up to 50 audio sources. A Cisco Unified Communications Manager Administration window supports import, addition, update, and deletion of each audio source. The music on hold server also supports one fixed input source. The system supports the following codecs: G.711 a-law/mu-law, G.729a, and wideband.

  Note Because the G.729a codec is designed for human speech, using it with music on hold for music may not provide acceptable audio quality.

- For each cluster, you may define up to 50 audio sources from files as well as one fixed audio source. You may define up to 50 audio sources from files as well as one fixed audio source. A Cisco Unified Communications Manager Administration window supports addition, update, and deletion of each audio source. All nodes use local copies of the same 50 or fewer files. You must set up the fixed audio source that is configured on each MOH server.

- For each cluster, you may define at most 20 music on hold servers. The Cisco Unified Communications Manager Administration window allows update of music on hold servers. The MOH server automatically gets added when a node gets added. You cannot delete the MOH server unless the server gets deleted. The window allows administrators to specify the following characteristics for each MOH server:
  - Name
  - Node (server host name)
  - Device pool
  - Maximum number of unicast and multicast streams
  - Sources to multicast
  - For each multicast source: IP address, port, and time to live (maximum number of router hops)
- Cisco Unified Communications Manager Administration allows definition of at least 500 media resource groups per cluster. Cisco Unified Communications Manager Administration allows definition of at least 500 media resource groups. Each media resource group may include any combination of at least 20 media resources, including music on hold servers, media termination points, transcoders, and conference devices. Music on hold servers in one cluster support at least 10,000 simultaneous music on hold streams. Music on hold servers support at least 256 simultaneous music on hold streams. See topics related to Media Resource Groups in the *Cisco Unified Communications Manager System Guide* for details of media resource groups.
- Cisco Unified Communications Manager Administration allows definition of media resource group lists. See topics related to Media Resource Group lists in the *Cisco Unified Communications Manager System Guide* for details of media resource group lists.
- Modifications to the Cisco Unified Communications Manager Administration device configuration windows for phones and gateways allow the selection of a media resource group list, hold stream source, and consult stream source as optional parameters for a device.
- Modifications to the Cisco Unified Communications Manager Administration Directory Number configuration windows allow selection of a user hold source and a network hold source.
- Modifications to the Cisco Unified Communications Manager Administration Service Parameters allows entry to a clusterwide, default music on hold stream source (default specifies 1) and default media resource group type (default specifies unicast).
- The following restriction exists for multicast music on hold (MOH) when a media termination point (MTP) is invoked. 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.
- CTI devices do not support the multicast Music On Hold feature. If a CTI device is configured with a multicast MOH device in the media resource group list of the CTI device, call control issues may result. CTI devices do not support multicast media streaming.
- Multicast MOH does not support interoperability between H.323 and SIP protocols.
- Ensure multicast on MOH does not have codec mismatch, as transcoders/MTPs do not support multi-cast streams.

- Codec mismatch results in MOH failure and tone on hold plays based on configuration of the trunk/phone device or by an annunciator.
- 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.
- 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. So, devices with an IP Addressing Mode of IPv6 Only cannot support multicast Music On Hold. Under these circumstances, Unified Communications Manager plays a tone, instead of music, when the phone is on hold. However, devices with an IP Addressing Mode of IPv6 only can stream unicast Music On Hold without Unified Communications Manager inserting an MTP for IPv4 to IPv6 conversion. For more information on IPv6, see the Internet Protocol Version 6 (IPv6), on page 739.
- The Fixed Music On Hold device cannot specify an audio source that connects through a Universal Serial Bus (USB), because Unified Communications Manager does not support USB when running on VMware. VMware does, however, support internal Music On Hold.
- A 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 node(s) that supply MOH from an external source.

Music On Hold Failover and Fallback

The music on hold 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 one is available.

Cisco Unified Communications Manager takes no special action when a music on hold server fails during an active music on hold session. The held party receives nothing from this point, but this situation does not affect normal call functions.

Music On Hold Configuration

This section provides information to configure Music On Hold.

Tip Before you configure Music On Hold, review the configuration summary task for this feature and topics related to configuring multlicast.

Related Topics

Configure Monitoring Music On Hold Performance, on page 969
Configure Multicast, on page 968
Configure Music On Hold, on page 967

Music On Hold Audio Source Configuration

This section provides information to configure Music On Hold audio sources. The integrated Music On Hold feature provides the ability to place on-net and off-net users on hold with music streamed from a streaming source. This feature includes the following actions:

- End user hold
- Network hold, which includes transfer hold, conference hold, and park hold

Music On Hold configuration comprises configuration of Music On Hold audio sources and Music On Hold servers.

Find a Music On Hold Audio Source

Because you might have multiple Music On Hold audio sources in your network, Cisco Unified Communications Manager lets you search for Music On Hold audio sources on the basis of specified criteria. Follow these steps to search for a specific Music On Hold audio source in the Cisco Unified Communications Manager database.

Note During your work in a browser session, Cisco Unified Communications Manager Administration retains your Music On Hold audio source search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your Music On Hold audio source search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Media Resources** > **Music On Hold Audio Source**.

The Find and List Music On Hold Audio Sources window displays. Records from an active (prior) query may also display in the window.

Step 2 To filter or search records

a) From the first drop-down list box, choose a search parameter.
b) From the second drop-down list box, choose a search pattern.
c) Specify the appropriate search text, if applicable.

Note To add additional search criteria, click the **+** button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the **–** button to remove the last added criterion or click the **Clear Filter** button to remove all added search criteria.

Step 3 To find all records in the database, ensure the dialog box is empty, click **Find.**

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

Note You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking **Delete Selected**. You can delete all configurable records for this selection by clicking **Select All** and then clicking **Delete Selected**.

Step 4 From the list of records that display, click the link for the record that you want to view.

Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Configure a Music On Hold Audio Source

Perform the following procedure to add or update a Music On Hold audio source. Use this procedure to associate an existing audio source with an audio stream number or to upload a new custom audio source.

Note If a new version of an audio source file is available, you must perform the update procedure to use the new version.

Procedure

Step 1 Choose **Media Resources** > **Music On Hold Audio Source**.

The Find and List Music On Hold Audio Sources window displays.

Step 2 Perform one of the following tasks:

a) To add a new Music On Hold audio source, click **Add New**.

The Music On Hold Audio Source Configuration window displays.

b) To update a Music On Hold audio source, locate a specific Music On Hold audio source as described in Find a Music On Hold Audio Source, on page 991.

Step 3 Enter the appropriate settings as described in Music On Hold Audio Source Configuration Settings, on page 993.

Step 4 Click **Save.**

If you added a Music On Hold Audio Source, the list box at the bottom of the window now includes the new Music On Hold audio source.

Note The MOH Audio Source File Status pane tells you about the MOH audio translation status for the added source.

Delete a Music On Hold Audio Source

Perform the following procedure to delete an existing Music On Hold audio source.

Note Deletion does not remove the Music On Hold audio source files. Deletion only removes the association with the MOH Audio Stream number.

Procedure

Step 1 Choose **Media Resources** > **Music On Hold Audio Source**.

The Find and List Music On Hold Audio Sources window displays.

Step 2 To locate a specific Music On Hold audio source, enter search criteria and click **Find.**

A list of Music On Hold audio sources that match the search criteria displays.

Step 3 Perform one of the following actions:

a) Check the check boxes next to the Music On Hold audio sources that you want to delete and click **Delete Selected**.
b) Delete all Music On Hold audio sources in the window by clicking **Select All** and then clicking **Delete Selected**.
c) From the list, choose the name of the Music On Hold audio source that you want to delete and click **Delete.**

A confirmation dialog displays.

Step 4 Click **OK.**

The association of the chosen Music On Hold audio source with an audio stream number gets deleted.

Music On Hold Audio Source Configuration Settings

The following table describes the configuration settings that are used for configuring Music On Hold audio sources.

Table 101: Music On Hold Audio Source Configuration Settings

Field	Description
Music On Hold Audio Source Information	
MOH Audio Stream Number	Choose the stream number for this MOH audio source. To do so, click the drop-down arrow and choose a value from the list that displays. For existing MOH audio sources, this value displays in the MOH Audio Source title.
MOH Audio Source File	Choose the file for this MOH audio source. To do so, click the drop-down arrow and choose a value from the list that displays.
MOH Audio Source Name	Enter a unique name in this field for the MOH audio source. This name can comprise up to 50 characters. Valid characters include letters, numbers, spaces, dashes, dots (periods), and underscores.
Allow Multi-casting	Check this check box to specify that this MOH audio source allows multicasting.

Field	Description
MOH Audio Source File Status	This pane displays information about the source file for a chosen MOH audio source. For an MOH audio source, the following attributes display: • InputFileName • ErrorCode • ErrorText • DurationSeconds • DiskSpaceKB • LowDateTime • HighDateTime • OutputFileList • ULAW wav file name and status • ALAW wav file name and status • G.729 wav file name and status • Wideband wav file name and status • Date MOH Audio Translation completed
Announcement Settings	
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 the initial announcement is played: • Always- for all calls (default) • Only for queued calls - in situations when no agents are available
Periodic Announcement	Choose a periodic announcement from the drop-down list box. **Note** To select MoH with no periodic announcement, choose the default option: “Not Selected”. Select View Details to view the following Periodic Announcement information: • Announcement Identifier • Description • Default Announcement **Note** MOH server always plays the periodic announcement regardless of other settings. **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 specify 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.
MoH Audio Sources	
(list of MoH audio sources)	For each MoH audio source that has been added, the MoH audio source name displays in this list box. Click the audio stream number of an MoH audio source to configure that MoH audio source. **Note** If <None> is selected, the system default MoH audio source service parameter (Default Network Hold MoH Audio Source ID) is used for the MoH audio source.

Field	Description
Upload File	To upload an MOH audio source file that does not display in the drop-down list box, click the Upload File button. In the Upload File popup window that displays, enter the path to a file that specifies an audio source file. If you do not know the path and file name, search for the file by clicking the Browse... button to the right of the Upload File field. 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 tells you the result of the upload. Click Close to close this window. **Note** Uploading a file uploads the file to the 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. 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 Unified Communications Manager on each server. MOH audio source files do not automatically propagate to other MOH servers in a cluster. 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 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. 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 Unified Communications Manager on each server. MOH audio source files do not automatically propagate to other MOH servers in a cluster.

Fixed Music On Hold Audio Source Configuration

This section provides information to configure the fixed Music On Hold audio source. The music on hold server supports one fixed-device stream source in addition to the file stream sources. This source represents the fixed audio source, which gets configured in the Fixed MOH Audio Source Configuration window. The fixed audio source gets sourced from a fixed device that uses the local computer audio driver.

For each cluster, you may define one fixed audio source. You must set up the fixed audio source that is configured per cluster on each MOH server. To do so, connect a Cisco USB MOH sound adapter, which must be ordered separately, into the USB port for each MOH server in the cluster that you want to provide the fixed audio source.

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, however, is supported on VMware.

Configure the Fixed Music On Hold Audio Source

Perform the following procedure to configure the fixed music on hold audio source.

Procedure

Step 1 Choose **Media Resources** > **Fixed MOH Audio Source**.

The Fixed MOH Audio Source Configuration window displays.

Step 2 To configure and enable a fixed music on hold (MOH) audio source, enter the appropriate settings as described in Fixed Music On Hold Audio Source Configuration, on page 997.

Step 3 Click **Save.**

The Fixed MOH Audio Source Configuration window displays an Update Successful status message.

Delete a Fixed Music On Hold Audio Source

Perform the following procedure to delete an existing fixed music on hold audio source.

Procedure

Step 1 Choose **Media Resources** > **Fixed MOH Audio Source**.

The Fixed MOH Audio Source Configuration window displays.

Step 2 If the fixed MOH audio source that displays is enabled (that is, the Enable check box has been checked), you can delete this fixed MOH audio source.

To delete this fixed MOH audio source, click **Delete.**

A confirmation dialog box displays.

Step 3 Click **OK.**

The chosen fixed music on hold audio source gets deleted from the database.

Fixed Music On Hold Audio Source Configuration

The following table describes the configuration settings that are used for configuring the fixed music on hold (MOH) audio source.

Table 102: Fixed Music On Hold (MOH) Audio Source Configuration Settings

Field	Description
Fixed MOH Audio Source Information	
Source ID	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 Unified Communications Manager does not support USB when running on VMware. Internal Music On Hold, however, is supported on VMware.
Allow Multicasting	Check this check box to specify that this fixed MOH audio source allows multicasting.
Enable (If checked, Name is required.)	Check this check box to enable this fixed MOH audio source.
Announcement Settings	
Initial Announcement	Choose an initial announcement from the drop-down list. **Note** To select MoH with no initial announcement choose the default option: “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 Played	Choose one of the following to determine when the initial announcement is played: • Always- for all calls (default) • Only for queued calls - in situations when no agents are available **Note** To disable Initial Announcement completely, set Initial Announcement to “Not Selected” **AND** set Initial Announcement Played to "Only for Queued Calls".

Field	Description
Periodic Announcement	Choose a periodic announcement from the drop-down list box. **Note** To select MoH with no periodic announcement, choose the default option: “Not Selected”. Select View Details 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.

Music On Hold Server Configuration

This section provides information to configure servers for music on hold for a media resource group.

For any music on hold server that you configure, you may trace the configuration of that server. See the *Cisco Unified Serviceability Administration Guide* for more information.

Find a Music On Hold Server

Because you might have several music on hold servers in your network, Cisco Unified Communications Manager lets you locate specific music on hold servers on the basis of specific criteria. Use the following procedure to locate music on hold servers.

Procedure

Step 1 Choose **Media Resources** > **Music On Hold Server**.

The Find and List Music On Hold Servers window displays. Records from an active (prior) query may also display in the window.

Step 2 To filter or search records

a) From the first drop-down list box, choose a search parameter.
b) From the second drop-down list box, choose a search pattern.
c) Specify the appropriate search text, if applicable.

Note To add additional search criteria, click the **+** button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the **–** button to remove the last added criterion or click the **Clear Filter** button to remove all added search criteria.

Step 3 To find all records in the database, ensure the dialog box is empty, click **Find.**

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

Note You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking **Delete Selected**. You can delete all configurable records for this selection by clicking **Select All** and then clicking **Delete Selected**.

Step 4 From the list of records that display, click the link for the record that you want to view.

Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Configure a Music On Hold Server

Perform the following procedure to update a music on hold server.

Note You cannot add nor delete a music on hold server.

Procedure

Step 1 Choose **Media Resources** > **Music On Hold Server**.

The Find and List Music On Hold Servers window displays. Use the two drop-down list boxes to search for a music on hold server.

Step 2 To update a music on hold server, click the music on hold server that you want to update. The Music On Hold (MOH) Server Configuration window displays.

Step 3 Enter or update the appropriate settings as described in Music On Hold Server Configuration, on page 1001.

Step 4 To update this music on hold server, click **Save.**

The music on hold server gets updated in the database.

Reset or Restart a Music On Hold Server

Perform the following procedure to reset an existing music on hold server.

Procedure

Step 1 Locate the music on hold server by using the procedure in the Find a Music On Hold Server, on page 999.

Step 2 Click the music on hold server that you want to reset.

Step 3 Click the **Reset** button.

A popup window displays an information message.

Step 4 After reading the message, click **Restart** to restart the music on hold server or click **Reset** to reset the music on hold server.

Step 5 To close the popup window, click **Close.**

Synchronize a Music On Hold Server

To synchronize a Music on Hold Server with the most recent configuration changes, perform the following procedure, which will apply any outstanding configuration settings in the least-intrusive manner possible. (For example, a reset/restart may not be required on some affected devices.)

Procedure

Step 1 Choose **Media Resources** > **Music on Hold Server**.

The Find and List Music on Hold Servers window displays.

Step 2 Choose the search criteria to use.

Step 3 Click **Find.**

The window displays a list of Music on Hold Servers that match the search criteria.

Step 4 Check the check boxes next to the Music on Hold Servers that you want to synchronize. To choose all Music on Hold Servers in the window, check the check box in the matching records title bar.

Step 5 Click **Apply Config to Selected**.

The Apply Configuration Information dialog displays.

Step 6 Click **OK.**

Music On Hold Server Configuration

The following table describes the configuration settings that are used for configuring music on hold servers.

Table 103: Music On Hold Server Configuration Settings

Field	Description
Device Information	
Registration	Registration details for the server.
IPv4 Address	IPv4 address for the server.
IPv6 Address	IPv6 address for the server.
Host Server	For existing music on hold servers, this field serves for display only.

Field	Description
Music On Hold Server Name	Enter a unique name for the music on hold server in this required field. This name can comprise up to 15 characters. Valid characters include letters, numbers, spaces, dashes, dots (periods), and underscores.
Description	Enter a description for the music on hold server. This description can comprise up to 50 characters. Ensure Description does not contain ampersand (&), double quotes ("), brackets ([]), less than (<), greater than (>), or the percent sign (%).
Device Pool	Use this required field to choose a device pool for the music on hold server. To do so, click the drop-down arrow and choose a device pool from the list that displays.
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. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this MOH server consumes. A location setting of Phantom specifies 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. For more details about locations, see the Administration Guide for Cisco Unified Communications Manager. For an explanation of location-based CAC across intercluster trunks, see the System Configuration Guide for Cisco Unified Communications Manager.
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 Multicast 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 box, enable or disable whether Unified Communications Manager inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values: • Off - Choose this value to disable the use of a TRP with this device. • On - Choose this value to enable the use of a TRP with this device. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. 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 gets used as the required MTP. See the System Configuration Guide for Cisco Unified Communications Manager for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, 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, Unified Communications Manager first tries to find a transcoder that is also designated as a TRP. See the System Configuration Guide for Cisco Unified Communications Manager for a complete discussion of network virtualization and trusted relay points.
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.
Multicast Audio Source Information	
Enable Multicast Audio Sources on this MOH Server	Check or uncheck this check box to enable or disable 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 group(s) either by removing this MOH server or by changing the multicast setting 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 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. Cisco strongly recommends using IP addresses 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.
Selected Multicast Audio Sources	
	Only audio sources for which the Allow Multicasting check box was checked display in this listing. If no such audio sources exist, the following message displays: There are no Music On Hold Audio Sources selected for Multicasting. Click **Configure Audio Sources** in the top right corner of the page to select Multicast Audio Sources. From the Related Links drop-down list box, choose **Configure Audio Sources** and click **Go.**
No.	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 display.
Audio Source Name	Designates name of audio source that is defined as allowing 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 File Management Configuration

This section provides information to manage the music on hold audio source audio files. You can manage the audio files that the Music On Hold feature uses as audio sources. The **Media Resources** > **MOH Audio File Management** menu option allows the administrator to perform the following functions:

- Display a list of the MOH audio files that are stored on the system.
- Upload new MOH audio files.
- Delete MOH audio files.

Display Music On Hold Audio Files

Use the following procedure to display a list of music on hold audio files that are stored on the system.

Procedure

In Cisco Unified Communications Manager Administration, choose **Media Resources** > **MOH Audio File Management**.

The Music On Hold Audio File Management window displays.

For each entry in the list of records, the following information displays:

- Check box - If the audio file can be deleted, a check box displays in the first column of the display.
- 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 the file status, including the following values:
- Translation Complete - Files with this status uploaded successfully and are available for use as audio files for a music on hold audio source.
- In Use - After you add a music on hold audio source that uses this audio file as its MOH audio source file, the file status for this audio file changes to In Use. You cannot delete files with this file status.

Upload a Music On Hold Audio File

Perform the following procedure to upload a music on hold audio file. Uploading the audio file makes it available for use as a music on hold audio source. If you use the **Media Resources** > **Music On Hold Audio Source** menu option to add a new audio source, the addition makes the newly uploaded audio file available in the MOH Audio Source File drop-down list box.

Procedure

Step 1 Choose **Media Resources** > **MOH Audio File Management**.

The Music On Hold Audio File Management window displays.

Step 2 Click the **Upload File** button.

The Upload File popup window displays.

Step 3 Choose one of the following options:

a) If you know the path to a file that specifies an audio file, enter the path in the File field.
b) If you do not know the path and file name, search for the audio file by clicking the **Browse...** button to the right of the File field. After you find the audio file, click the desired audio file and click **Open**. The path to the chosen audio file displays in the File field of the Upload File popup window.

Step 4 To upload the specified audio file, click **Upload.**

After the audio file gets uploaded, the Upload Result window tells you the result of the upload.

Note Uploading a file uploads the file 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 or each 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.

Step 5 To close the Upload Result window, click **Close.**

The newly uploaded audio file gets added to the list of audio files in the MOH Audio File Management window.

Delete a Music On Hold Audio File

Perform the following procedure to delete an existing music on hold audio file.

Note You cannot delete MOH audio files that specify the In Use state. To delete such files, first use the **Media Resources** > **Music On Hold Audio Source** menu option to find MOH audio sources that use this audio file. Either delete those MOH audio sources or modify them, so they use a different audio file.

Procedure

Step 1 Choose **Media Resources** > **MOH Audio File Management**.

The Music On Hold Audio File Management window displays.

Step 2 Click the check box to the left of a music on hold audio file that you want to delete.

Note You can click several audio files to delete multiple audio files at once. You can also click the **Select All** button to select all audio files for deletion. Use the **Clear All** button to deselect audio files that you have selected.

Step 3 Click the **Delete Selected** button.

A popup window warns that this file will be deleted permanently.

Step 4 To complete the deletion, click **OK.**

The audio file gets deleted from the list of music on hold audio files.

View Music On Hold Server Performance

To view music on hold server perfmon counters, use the Cisco Unified Real Time Monitoring Tool (RTMT).

The following table details the performance monitoring counters that display in the Cisco Unified Real Time Monitoring Tool Performance window.

Table 104: Music On Hold Performance Counters

Performance Counter Name	Description
MOHConnectionState	Indicates primary and secondary Cisco Unified Communications Manager: • 1 = Primary • 2 = Secondary • 0 = Not connected
MOHAudioSourcesActive	Specifies total number of active audio sources, including each supported codec type. If audio Source 1 has mu-law and G.729 enabled, count for this audio source may show 2.
MOHStreamsActive	Specifies total number of active streams. Two potential overhead streams exist for each audio source/codec type: one for actual audio source, another for multicast.
MOHStreamsAvailable	Specifies total number of available simplex streams. Total represents total number of streams that are available in device driver for all devices.
MOHConnectionsLost	Specifies number of times that connection has been lost for the corresponding Cisco Unified Communications Manager.
MOHStreamsTotal	Specifies total number of streams that are processed.

Check Service States

To check whether the music on hold service is running, use Performance Management.

CHAPTER 41

Originally Called Party Name in Placed Call History

Originally Called Party Name in Placed Call History

Cisco Unified IP Phones display call history information, which includes placed calls. For placed calls, the phone displays the dialed digits or the dialed universal resource identifier (URI), and in many cases the name of the dialed user. However, in Cisco Unified Communications Manager (Unified CM) releases earlier than Release 9.0 there were scenarios, such as Call Forwarding, in which IP phones displayed “Unknown” in the placed call history, even when the called party had a valid name configured.

In Unified CM Release 9.0 and later releases, SIP phones supporting the Originally Called Party Name in Placed Call History feature always display the name of the originally called party when the dialed party has a valid name configured and its presentation is not restricted. Unified CM provides the name to the calling SIP phone, which allows the SIP phone to populate the name in the placed call history accurately, even when a call is forwarded by the called party.

Unified CM indicates the alerting name of the originally called party to the calling SIP phone. If an alerting name is not configured for the originally called party, but the originally called party answers the call, Unified CM will send the connected display name of the originally called party if configured. If the called party has Calling Line ID Restricted (CLIR) enabled, Unified CM indicates that the name is private and the calling phone does not display name information in the placed call history.

Neither the end user nor the administrator needs to make configuration changes to enable the Originally Called Party Name in Placed Call History feature.

Intercluster Calls Limitations

Unified CM uses the Remote-Party-ID (RPID) header to send the alerting name of the called party. For intercluster calls, Remote-Party-ID must be enabled on the SIP intercluster trunk for the SIP phones on the calling cluster to obtain the name of the dialed party. This includes all intermediate hops involving Cisco Unified Communications Manager Session Management Edition.

On a SIP trunk, it is possible to turn off the RPID header and use only the P-Asserted-ID (PAI) or P-Preferred-ID (PPI) headers. If only PAI or PPI is used between two Unified CM clusters, the placed call history on SIP phones may not contain the display name corresponding to the dialed number or the dialed URI.

Endpoint Features and Behavior

The placed call history information on SIP phones will have the dialed number, or the dialed URI, and name (where available and not private). For the name of the dialed party to be displayed on the SIP phone, the alerting name must be provisioned on Unified CM and its presentation must not be restricted. For intercluster calls the ASCII alerting name must be provisioned.

Note In some cases, Cisco Unified IP Phones 8900 and 9900 Series may have the display name rather than the alerting name in the placed call history.

Note 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 rather than “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.

Unified CM Features and Feature Behavior

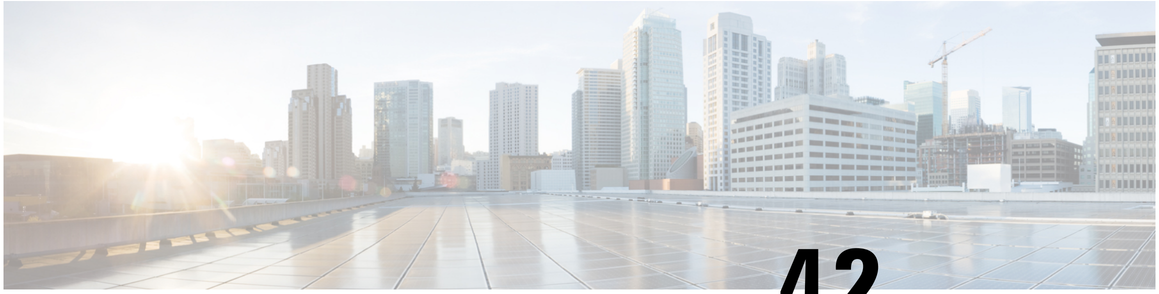
The Originally Called Party Name in Placed Call History feature is automatically negotiated between Unified CM and the SIP phone firmware during initial registration without requiring any configuration or administrative intervention. SIP phone firmware load 9.3.1 and higher supports the Originally Called Party Name in Placed Call History feature.

Supported Phone Models

The Originally Called Party Name in Placed Call History feature is supported on the following Unified IP Phones

- Cisco Unified IP Phones 6900 Series models 6921, 6941, 6945, 6961
- Cisco Unified IP Phones 7900 Series models 7906, 7911, 7931, 7941, 7942, 7945, 7961, 7962, 7965, 7970, 7971, 7975
- Cisco Unified IP Phones 8900 Series models 8941, 8945, 8961
- Cisco Unified IP Phones 9900 Series models 9951, 9971

SIP phone firmware load 9.3.1 and higher supports the Originally Called Party Name in Placed Call History feature.



CHAPTER 42

Paging

This chapter describes the Singlewire InformaCast product that is for use with Cisco Unified Communications Manager.

Paging

Now included with Cisco Unified Communications Manager is the Singlewire InformaCast product that provides paging capabilities for users to make point-to-point or group pages to and from Cisco IP Phones. The software and documentation for the InformaCast product is on a separate DVD included with the purchase of Cisco Unified Communications Manager or available online as a software download on `www.cisco.com`.

The InformaCast paging functionality is broken down into two categories: basic and advanced functionality. The basic paging features allow paging between Cisco IP Phones to groups and zones that the administrator configures. There are unlimited groups possible with 50 users total in each group in basic paging. Basic paging is provided as a new Cisco Unified Communications Manager feature at no cost. Should there be a requirement for more than 50 users in a single group or for higher level capabilities, the advanced features of InformaCast are required and highly recommended. This includes valuable features such as:

- Paging and Emergency Notification to All Users
- Paging to Overhead Analog and IP Speakers
- Bell Scheduling
- Prioritizing Emergency Notifications with call barge option
- Pre-Recorded and Text only pages
- Integration with Social Media Sites for Notification
- Email and SMS Mass Notification
- Call Number Monitoring- 911 Alerting
- Integration with Jabber clients

There are numerous additional features of Advanced Paging. To determine if Advanced Paging/Notification is appropriate for the end user Cisco Unified Communications Manager deployment, there is a 60 day trial of the advanced functionality to evaluate the higher level features. After installation of the software, there will be an option to begin the demonstration period for full access to all capabilities. To retain Advanced

Functionality after trial or if this functionality is required at the time of the Cisco Unified Communications Manager purchase, the Advanced Paging and Notification functionality can be purchased as a perpetual license from SolutionsPlus or as a subscription directly from Singlewire. For more information on the product's capabilities or for sales questions, contact Singlewire or refer to the documentation and support information included with the product.

CHAPTER 43

Proxy TFTP Server

The Cisco Proxy TFTP Server allows all the endpoints in a large-scale deployment to download the configuration file and get registered to the Cisco Unified Communications Manager.

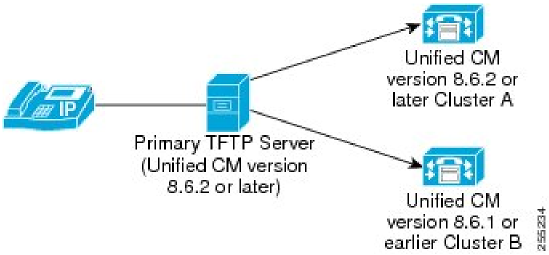
Cisco Proxy TFTP Server Deployment Models

Cisco Proxy TFTP Server supports two deployment models.

Cisco Proxy TFTP Server Deployment Model 1

For the deployment model illustrated in the following figure, the Primary TFTP Server should have Unified CM version 8.6 (2) or later.

Figure 159: Cisco Proxy TFTP Server Deployment Model 1



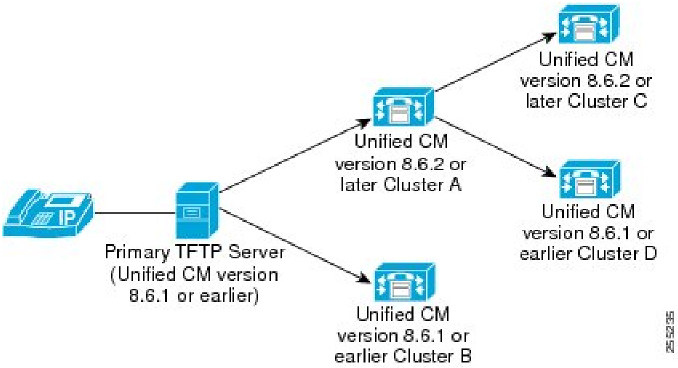
The two remote clusters, Cluster A and Cluster B, are configured to the Primary TFTP Server. However, you can configure any number of remote clusters to the Primary TFTP Server. Whenever an endpoint sends a request for configuration file, the Primary TFTP Server looks into the local cache and the configured remote clusters. So, an endpoint that is configured to the Primary TFTP Server Cluster, Cluster A, and Cluster B can retrieve the configuration file and register to the Cisco Unified Communications Manager.

Note Cisco recommends that you use deployment model 1 for better system performance. However, if you do not wish to change your existing Centralized TFTP (8.6 (1) or earlier), you can use deployment model 2.

Cisco Proxy TFTP Server Deployment Model 2

In the deployment model illustrated in the following figure, the centralized Unified CM TFTP server acts as a Primary TFTP server.

Figure 160: Cisco Proxy TFTP Server Deployment Model 2


IP
Primary TFTP Server (Unified CM version 8.6.1 or earlier)
Unified CM version 8.6.2 or later Cluster A
Unified CM version 8.6.1 or earlier Cluster B
Unified CM version 8.6.2 or later Cluster C
Unified CM version 8.6.1 or earlier Cluster D
255235

The two remote clusters - Cluster A and Cluster B have been configured to the Primary TFTP Server. However, you can configure any number of remote clusters to the Primary TFTP Server. Two more remote clusters have been added to the Cluster A. Whenever an endpoint sends a request for configuration file, the Primary TFTP Server looks into the local cache and the configured remote clusters (Cluster A and Cluster B). Cluster A further looks into its configured remote clusters (Cluster C and Cluster D). Thus, all the endpoints configured to the Primary TFTP Server Cluster, Cluster A, Cluster B, Cluster C and Cluster D can get the configuration file and get registered to the Cisco Unified Communications Manager.

Use Cases and Best Practices

Consider the following scenarios that detail how Proxy TFTP can be used and the best practices for implementation.

1. The cluster can act as just a proxy TFTP cluster with no other purpose. In this case, the cluster has no relationship with the other clusters, and does not process calls. For this scenario, the Remote Cluster TFTP is manually defined and rollback to pre-8.0 is recommended.

Note Autoregistration will not work in this scenario.

2. The cluster is a remote cluster that is also acting as a Proxy TFTP server for remote clusters. The remote cluster is manually defined, and Autoregistration should not be enabled.

TFTP Setup

Cisco Proxy TFTP Server can be configured manually as well as dynamically. This section provides configuration procedures for TFTP.

Set Up TFTP Manually

Follow this procedure to configure Cisco Proxy TFTP Server manually in your network.

Procedure

Step 1 Create a new cluster.

a) In Cisco Unified Communications Manager Administration, choose **Advanced Features > Cluster View**.
b) Enter the **Cluster Id** and **Fully Qualified Domain Name**.

Step 2 Check the **Enable** check box for the TFTP service.

Step 3 Click **TFTP** hyperlink.

The Remote Cluster Manually Override Configuration window appears.

Step 4 Choose **Manually Configure Remote Service addresses**.

Step 5 Enter IP addresses for the TFTP servers of the remote clusters.

Step 6 Click **Save**.

Set Up TFTP Dynamically

Perform the following steps to dynamically configure Cisco Proxy TFTP Server in your network.

- Configure EMCC.
- In Cisco Unified Communications Manager Administration, choose **Advanced Features** > **Cluster View** > **Update Remote Cluster Now**.

Proxy TFTP Server and Centralized TFTP Server

For large scale deployments, the Centralized TFTP server has the following limitations:

- Sometimes, endpoints are unable to download the configuration file because the primary TFTP server takes more time to get the configuration file from the alternate TFTP servers. By the time the primary TFTP server gets the file, the endpoints get timed out. As a result, endpoints never get registered to their Unified CM.
- Only 10 alternate TFTP servers can be added.

These limitations are not applicable to Cisco Proxy TFTP Server.

Note When a phone requests a common file from a central or proxy TFTP server and that file has a common name such as `ringlist.xml.sgn` or is a locale file, the TFTP server sends its own local copy of the file instead of the file from the home cluster of the phone. The phone rejects the file due to a signature verification failure because the file has the signature of the TFTP server's local cluster, which does not match the Initial Trust List (ITL) of the phone. To resolve this issue, you can either disable Security By Default (SBD) for the phone or perform the bulk certificate export procedure to make the Trust Verification System (TVS) return a success when the phone verifies a signature from a different cluster. See the procedure in the "Default Security Setup" section of the *Cisco Unified Communications Manager Security Guide* for performing a bulk certificate export when migrating IP phones between clusters to perform the bulk certificate export. To disable Security by Default, see the procedure to update the ITL file for IP Phones in the *Cisco Unified Communications Manager Security Guide*.

Phone Behavior with Proxy TFTP Server

For phones configured to remote clusters, first-time phone registration may take a few minutes. The time delay is due to Proxy TFTP Server searching for the configuration file in the remote clusters. The delay will vary based on the number of end points and the number of remote clusters configured. However, subsequent registrations will not have any delay.

Cisco Proxy TFTP Server System Requirements

The following system requirements exist for Cisco Proxy TFTP Server:

- Cisco Unified Communications Manager, Release 8.6 (2) or higher
- Cisco TFTP service - should be activated and in running state

Cisco Proxy TFTP Server Interactions and Restrictions

This section provides the details of interactions and restrictions for Cisco Proxy TFTP Server.

Cisco Proxy TFTP Server Interactions

Cisco TFTP service of the Proxy TFTP server interacts with the TFTP services of the remote clusters. In the Cluster View window (**Advanced Features > Cluster View**), for a particular remote cluster, TFTP service can have a maximum of three IP addresses, and Proxy TFTP server will interact with all three IP addresses if they are configured.

Note You must ensure that the Cisco TFTP service is active and in running state on the configured IP addresses.

When a phone requests a common file from a central or proxy TFTP server and that file has a common name such as `ringlist.xml.sgn` or is a locale file, the TFTP server sends its own local copy of the file instead of the file from the home cluster of the phone. The phone rejects the file due to a signature verification failure because the file has the signature of the TFTP server's local cluster, which does not match the Initial Trust List (ITL) of the phone. To resolve this issue, you can either disable Security By Default (SBD) for the phone or perform the bulk certificate export procedure to make the Trust Verification System (TVS) return a success when the phone verifies a signature from a different cluster. See the procedure in the "Default Security Setup" section of the *Cisco Unified Communications Manager Security Guide* for performing a bulk certificate export when migrating IP phones between clusters to perform the bulk certificate export. To disable Security by Default, see the procedure to update the ITL file for IP Phones in the *Cisco Unified Communications Manager Security Guide*.

Cisco Proxy TFTP Server Restrictions

This section describes the restrictions and limitations of the Cisco Proxy TFTP Server with other Cisco Unified Communications Manager Administration components.

Phones Unable to Register with Cluster

Follow these steps if phones in your cluster are no longer able to register correctly with the cluster.

1. Verify that full security mesh is established between the home and Proxy TFTP clusters:
   a. Perform a bulk import of the CallManager certificates from the Proxy TFTP server to the home cluster.
   b. Perform a bulk import of the CallManager certificates from the home clustser to the Proxy TFTP server.
2. On the home cluster, keep the **Prepare Cluster for Rollback to pre 8.0** set to **False**. This makes sure that phones will have Security by Default (SBD) enabled during normal operation.
3. On the Proxy TFTP cluster, set the **Prepare Cluster for Rollback to pre 8.0** to **False**. This step makes sure that SBD is enabled on the Proxy TFTP server as well.

Caution When the Proxy TFTP cluster is set up, do not remove the cluster view configuration from the Proxy TFTP configuration. Removing the cluster view from the Proxy TFTP configuration can result in phones receiving a 404 file not found error, which sends the phones a default ITL file from the Proxy TFTP server. This scenario requires that the ITL files be manually deleted from the phones to correctly register back to the home cluster.

Registration Problems for Phones with SBD Loads for Previous Versions of Cisco Unified Communications Manager 8.0

For remote cluster TFTP servers that are running on Cisco Unified Communications Manager 8.0 and later, the phones with SBD load can register to these remote cluster Unified Communications Managers through a Proxy TFTP server. However, for the remote cluster TFTP servers that running on a version that is earlier than Cisco Unified Communications Manager 8.0, the phones with SBD load are unable to register to the remote cluster Unified Communications Managers through a Proxy TFTP server, because the Identity Trust List (ITL) file is unavailable in versions that are earlier than Unified Communications Manager 8.0.

Use the following procedure to resolve this problem.

1. Connect the endpoint directly to the remote cluster Unified Communications Manager:
   a. Disable the DHCP option.

   b. Enter the TFTP IP address on the phone manually.

   The phone gets the required SBD load and registers to the Unified Communications Manager.

2. Enable the DHCP option and reset the phone manually.

The phone gets registered to the remote cluster through Proxy TFTP.

Note This procedure is applicable only if you have new phones with SBD load or if you plan to move the phones from a Unified Communications Manager with SBD support to a Unified Communications Manager without SBD support. This procedure is not applicable if the number of phones in a cluster is large.

Problems When You Move a Device From One Remote Cluster to Another

When you move a device from one cluster to another, the device may lose its trusted status. For a secure cluster, you must re-run the CTL Client.

The following procedures show actions you can take to restore the trusted status for devices in various deployments:

10.0 Proxy TFTP deployments

1. Export the TFTP certificate from the Proxy TFTP.
2. Import the certificate to all the slave SBD-aware clusters.
3. Add the TFTP certificate from the Proxy TFTP to the CTL file for all of the mixed-mode 7.x slave clusters.

8.6 and 9.0 Proxy TFTP deployments

1. If the Proxy TFTP is not on the highest release, export the locale and ring list files from the cluster with the highest Unified Communications Manager release.
2. Import the TFTP certificate from the Proxy TFTP to all the SBD-aware slave clusters.
3. Add the TFTP certificate from the Proxy TFTP to the CTL file of all the mixed-mode 7.x slave clusters.

8.0 and 8.5 Centralized TFTP deployments

1. If the Centralized TFTP is not on the highest release, export the locale and ring list files from the cluster with the highest Unified Communications Manager release.
2. Import the TFTP certificate from the Centralized TFTP to all the slave SBD aware clusters.
3. Add the TFTP certificate form the Centralized TFTP in the CTL Files of all the mixed-mode 7.x slave clusters.

The following procedures detail the best practices for successfully moving endpoints between clusters.

Move Endpoints From an 8.0+ Cluster to a Cluster with a CTL File

Note If the second cluster is in mixed mode, the first cluster must have a CTL file.

1. Run the CTL client if needed (with desired cluster security mode).
2. If the two clusters have CTL files signed by USB eTokens that are trusted by endpoints in both clusters, no action is required; go to Step 4.
3. Physically ship the USB eTokens from the second cluster to the first cluster and add the USB eTokens in the CTL file of the first cluster.
4. Point the endpoints in the first cluster to the second cluster, for example, through DHCP.

Move Endpoints From a 7.x Cluster with a CTL File to Another Cluster with a CTL File

1. If the two clusters have CTL files that are signed by trusted USB eTokens in both clusters, no action is required; go to Step 3.
2. Physically ship the USB eTokens from the second cluster to the first cluster and add the USB eTokens in the CTL file of the first cluster.
3. Point the endpoints in the first cluster to the second cluster, for example, through DHCP.

Moving Endpoints From an 8.0+ Cluster with a CTL File to Another Cluster

1. If the two clusters have CTL files that are signed by trusted USB eTokens in both clusters, no action is required.
2. Physically ship the USB eTokens from the second cluster to the first cluster and add the USB eTokens in the CTL file of the first cluster.

Phones Take Time to Register While Upgrading the Remote Cluster

When a remote cluster is upgraded, phones request the new load file, which must be downloaded to the Proxy TFTP local cache. If you plug in an Ethernet cable to a phone and then set up the phone on the Unified Communications Manager, the phone takes about 30 minutes to register. However, if you set up the phone on the Unified Communications Manager and then plug in the Ethernet cable, the phone is registered immediately.

Proxy TFTP and Security

Endpoints in a Cisco Unified Communications Manager cluster are configured with Proxy TFTP (for example, through Dynamic Host Configuration Protocol, or DHCP). Proxy TFTP can find the target cluster of the endpoint.

Note It is recommended that you keep the Proxy TFTP on the current release while you upgrade the rest of the clusters, as well as have a combination of nonsecure and mixed-mode clusters.

The Proxy TFTP server does not have to be on the highest Unified Communications Manager release, and clusters in a Proxy TFTP deployment can be either nonsecure or in mixed-mode.

Proxy TFTP can find the target cluster of endpoints because the MAC address of the endpoints is part of the filename in the TFTP GET request (for example, `SEP001956A3A472.cnf.xml.sgn`). Proxy TFTP discovers the target in the following way:

1. Proxy TFTP polls all the clusters that it controls for the requested file, starting from its own database.
2. The cluster where the endpoint is configured returns the file.
3. The locale and ring list file requests do not contain a MAC address, so Proxy TFTP returns its own copies of these files.

Note The locale and ring list files are backward compatible for Unified Communications Manager releases.

When Security-by-Default (SBD) was introduced for Unified Communications Manager, Proxy TFTP (and TFTP servers in general) served both signed and nonsigned requests.

If the home cluster of an endpoint does not accept the ITL file request, the endpoint requests a default ITL file which the Proxy TFTP serves. After the endpoint receives the configuration file from its home cluster, the endpoint cannot validate the signature, because the endpoint has the ITL file from the Proxy TFTP and not its home cluster.

10.0(1) Proxy TFTPs perform the following steps for signing files and serving them to endpoints:

- Automatically discover the cluster in the deployment that is on the highest release
- Get the locale and ring list files from the cluster
- Strip the signature of the locale or ring list file
- Sign the files with their own TFTP private key before serving them to endpoints that are requesting the files

Cisco Proxy TFTP Server Installation and Activation

After you install Cisco Unified Communications Manager, your network can support the Cisco Proxy TFTP Server feature if you perform the necessary configuration tasks. For information on configuration tasks that you must perform, see the TFTP Setup, on page 1017

Remote Cluster Settings

In Cisco Unified Communications Manager Administration, use the **Advanced Features > Cluster View** menu path to configure remote clusters.

Tips About Finding Remote Clusters

The Find operation locates only those remote clusters that you added previously. The Find operation does not locate the clusters that belong to the enterprise automatically.

Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the “Navigating the Cisco Unified Communications Manager Administration Application” section in the Cisco Unified Communications Manager Administration Guide and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration Settings Table

The following table provides detailed descriptions of the remote cluster settings that you configure in the Cluster View window (**Advanced Features > Cluster View**).

Table 105: Remote Cluster Settings

Field	Description
Remote Cluster Information	
Cluster Id	Enter the cluster ID of the remote cluster. Valid values include alphanumeric characters, period (.), and hyphen (-).
Description	Enter a description for the remote cluster. This field accepts up to 128 characters. You may use any character except quotes (“), close angle bracket (>), open angle bracket (<), backslash (\), dash (-), ampersand (&), and percent sign (%).
Fully Qualified Name	Enter the fully qualified name of the remote cluster/IP address. This field accepts up to 50 characters and allows the following characters: alphanumeric (a through z, A through Z, and 0 through 9), period (.), dash (-), asterisk (*), and space ( ).
Remote Cluster Service Information	

Field	Description
EMCC	For the EMCC service, the following column headings detail the configuration for this service: • Enabled—If the EMCC service is enabled, this box gets checked. • Service—This entry specifies the EMCC service. • Remote Activated—Valid values specify true or false. • Address 1—This column lists the first address for this service. • Address 2—This column lists the second address for this service. • Address 3—This column lists the third address for this service.
PSTN Access	For the PSTN access, the following column headings detail the configuration for this service: • Enabled—If the PSTN access is enabled, this box gets checked. • Service—This entry specifies the PSTN access • Remote Activated—Valid values specify true or false. • Address 1—This column lists the first address for this service. • Address 2—This column lists the second address for this service. • Address 3—This column lists the third address for this service.

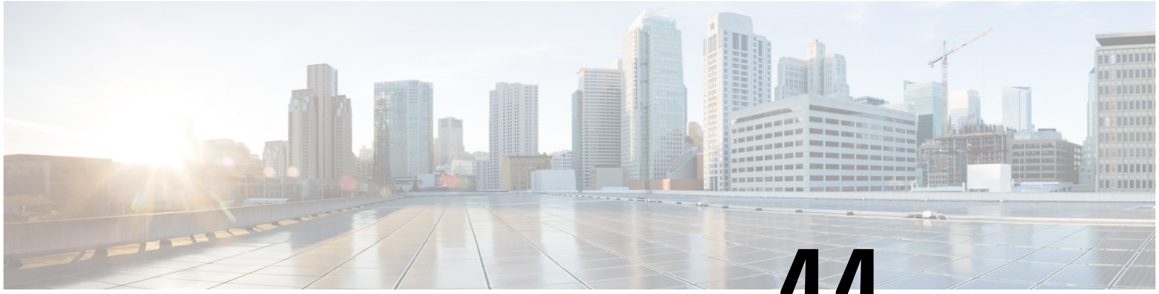
Field	Description
RSVP Agent	For the RSVP agent, the following column headings detail the configuration for this service: • Enabled—If the RSVP agent is enabled, this box gets checked. • Service—This entry specifies the RSVP agent • Remote Activated—Valid values specify true or false. • Address 1—This column lists the first address for this service. • Address 2—This column lists the second address for this service. • Address 3—This column lists the third address for this service.

Field	Description
TFTP	For the TFTP service, the following column headings detail the configuration for this service: • Enabled—If the TFTP service is enabled, this box gets checked. • Service—This entry specifies the EMCC service. • Remote Activated—Valid values specify true or false. **Note** The value of the Remote Activated column is set to true whenever remote IP addresses are configured either manually or dynamically. • Address 1—This column lists the first address for this service. **Note** When you upgrade from Cisco Unified Communications Manager 8.6 (1) to Cisco Unified Communications Manager 8.6 (2) or later, Address 1 is automatically updated by the system. However, if this field is blank after the upgrade due to some reason such as DNS lookup failure, you must manually update it with the appropriate IP address of the TFTP service. • Address 2—This column lists the second address for this service. • Address 3—This column lists the third address for this service.
Enabled All Services	Click this button to enable all services (EMCC, PSTN Access, and RSVP Agent).
Disabled All Services	Click this button to disable all services (EMCC, PSTN Access, and RSVP Agent).
Update Remote Cluster Now	Click this button to update the remote cluster immediately.

Remote Cluster Manually Override Settings

The following table provides detailed descriptions of the remote cluster settings that you configure in the Remote Cluster Manually Override Configuration window (**Advanced Features > Cluster View > TFTP**).

Field	Description
Use automatically determined remote server addresses	Choose this option to use automatically-determined remote server addresses.
Manually configure remote server addresses	Choose this option to manually configure remote server addresses.
Address 1	Enter the first address of the TFTP service.
Address 2	Enter the second address of the TFTP service.
Address 3	Enter the third address of the TFTP service.



CHAPTER 44

Quality Report Tool

This chapter provides information about the Quality Report Tool (QRT), a voice-quality and general problem-reporting tool for Cisco Unified IP Phones, which acts as a service that allows users to easily and accurately report audio and other general problems with their IP phone. QRT automatically loads with the Cisco Unified Communications Manager installation, and the Cisco Extended Functions (CEF) service supports it. (For more information about the Cisco Extended Functions service, see the Cisco Unified Serviceability Administration Guide.)

As system administrator, you can enable QRT functionality by creating, configuring, and assigning a softkey template to associate the QRT softkey on a user IP phone. You can choose from two different user modes, depending upon the amount of user interaction with QRT that is desired.

Note The system gives users with administrator privileges the authorization to configure QRT and view the reports.

Configure QRT

The Quality Report Tool (QRT), a voice-quality and general problem-reporting tool for Cisco Unified IP Phones, acts as a service that allows users to easily and accurately report audio and other general problems with their IP phone. QRT automatically loads with the Cisco Unified Communications Manager installation, and the Cisco Extended Functions (CEF) service supports it. (For more information about the Cisco Extended Functions service, see the Cisco Unified Serviceability Administration Guide.)

As system administrator, you can enable QRT functionality by creating, configuring, and assigning a softkey template to associate the QRT softkey on a user IP phone. You can choose from different user modes, depending upon the amount of user interaction with QRT that is desired.

Perform the following steps to configure the QRT feature in Cisco Unified Communications Manager.

Procedure

Step 1 Create a copy of the Standard User softkey template and add the QRT softkey for the following call states:

- On Hook
- Connected

Step 2 Add the new softkey template to the common device configuration.

Step 3 Add the new softkey template to the user phones by using the Phone Configuration window.

Note You can assign the common device configuration to the phone configuration if you are using common device configuration for the softkey. Alternatively, you can add the softkey individually to each phone.

Step 4 Using the Cisco Unified Serviceability tool, Service Activation, activate Cisco Extended Functions service.

Step 5 From Cisco Unified Serviceability, configure alarms and traces for QRT.

Step 6 Configure the Cisco Extended Functions service parameters for QRT.

Step 7 Access the QRT Viewer to create, customize, and view IP phone problem reports.

Related Topics

Create a Softkey Template with the QRT Softkey, on page 1043
Configure the QRT Softkey Template in Common Device Configuration, on page 1045
Add the QRT Softkey Template in Phone Configuration, on page 1046
Activate the Cisco Extended Functions Service for QRT, on page 1047
Configure Alarms and Traces for QRT, on page 1048
Set the Cisco Extended Functions Service Parameters for QRT, on page 1049
Use the QRT Viewer, on page 1051

Quality Report Tool Feature

This section provides information about the various components and the architecture of the QRT feature. When you install Cisco Unified Communications Manager, the Cisco Extended Functions service installs and loads the QRT functionality on the Cisco Unified Communications Manager server. Then, as system administrator, you enable the QRT feature through the use of softkey templates and define how the feature will work in your system by configuring system parameters and setting up Cisco Unified Serviceability tools. You can then create, customize, and view phone problem reports by using the QRT Viewer application. (The system includes the QRT Viewer application as part of the Real Time Monitoring Tool.

You can configure QRT availability for up to four different call states and choose from two different user modes. The user modes determine the level of user interaction that is enabled with QRT and allow either detailed voice-quality reports or more general phone problem reports and relevant statistics.

When users experience problems with their IP phones, they can invoke this feature by pressing the QRT softkey on their Cisco Unified IP Phone during the Connected call state. From a supported call state, and using the appropriate problem classification category, users can then choose the reason code that best describes the problem that they are experiencing with their IP phone.

Related Topics

Use the QRT Viewer, on page 1051
Extended Menu Choices, on page 1037
Problem Classification Categories and Reason Codes, on page 1038

Components of QRT

QRT, a multitiered, web-based application, includes the following key components:

- Client Components
    - IP phone browser for end-user interface
    - Cisco Unified Communications Manager Administration windows for feature and tools configuration and viewer application
- Server Components
    - Cisco Extended Functions service
    - Cisco Unified Communications Manager for skinny messages
    - CTIManager for QBE messages
    - Database for configuration data and device data
    - Cisco RIS Data Collector for runtime device-related information
    - Alarm interface
    - System Diagnostic Interface (SDI) trace
- Service - Cisco Extended Functions service for collecting and managing user reports. It also handles the user interface on the IP phone as well as notifying Cisco RIS Data Collector for alerts and issuing SNMP traps.
- Viewer Application - The QRT Viewer application, which is included as part of the trace collection feature in the Cisco Real Time Monitoring Tool (RTMT), allows you to filter, format, and view generated reports. Reports automatically open in the QRT Viewer when you view a trace file that includes QRT information.

Overview of QRT Architecture

The QRT feature uses the Cisco Extended Functions service, which comprises the following interfaces:

- Cisco CTIManager interface (QBEHelper)
- CUCM database interface (DBL Library)
- Screen helper and dictionary

- Redundancy manager
- DB change notifier
- SDI trace and alarm

The Cisco Extended Functions service interfaces with the phone by using the XML services interface (XSI) over skinny protocol (a protocol that is used between a Cisco Unified IP Phone and Cisco Unified Communications Manager) and the Quick Byte Encoding protocol (a protocol that is used between the Cisco CTIManager and TSP/JTAPI).

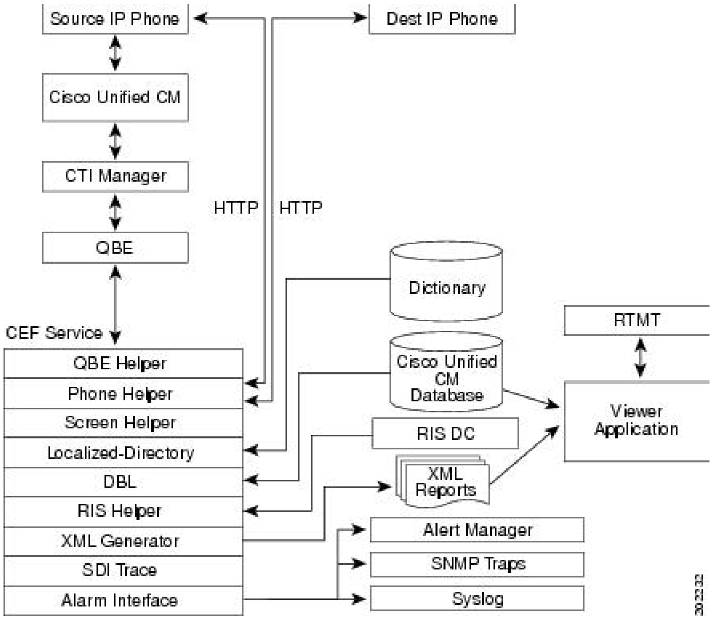
When a user presses the QRT softkey, QRT opens the device and presents up to four different screens that display problem categories and associated reason codes to obtain user feedback.

After the user chooses the option that best describes the problem, the system logs the feedback in the XML file; the system then issues alarms to notify the Cisco RIS Data Collector to generate alerts and SNMP traps. When QRT detects that user interaction is complete, it then closes the device.

Note The actual information that is logged depends upon the user selection and whether the destination device is a Cisco Unified IP Phone.

The following figure shows an illustration of the Cisco Extended Functions service architecture.

Figure 161: Using the Cisco Extended Functions Service Architecture



Cisco CTIManager Interface (QBEHelper)

The QBEHelper library provides the interface that allows the Cisco Extended Functions service to communicate with a configured Cisco CTIManager.

CUCM Database Interface (DBL Library)

The DBL library provides the interface that allows the Cisco Extended Functions service to perform queries on various devices that are configured and registered in the Cisco Unified Communications Manager database.

Screen Helper and Dictionary

The screen helper of the Cisco Extended Functions service reads the XML dictionary files and creates Document Object Model (DOM) objects for all installed locales when the CEF service starts. The system uses these DOM objects for constructing XSI screens that the Cisco Unified IP Phone needs.

Redundancy Manager

When multiple Cisco Extended Functions are active within a Cisco Unified Communications Manager cluster, the redundancy manager uses an algorithm to determine which CEF service is active and which is the backup CEF. The Redundancy Manager uses the lowest IP address of the server that is running the CEF service as the active service. The remaining CEF services serve as backup services.

DB Change Notifier

The DB Change Notifier handles all the database change notifications, such as service parameter changes, trace parameter changes, alarm configuration changes, and status changes of other Cisco Extended Functions services, and reports the changes to the CEF service.

SDI Trace and Alarm

The Cisco Extended Functions service uses the SDI Trace and Alarm libraries. The libraries generate traces and alarms to the Event Viewer. The alarm library publishes information about the CEF service to Syslog, SNMP, and the Cisco RIS Data Collector service. For more information about traces and alarms, see the Cisco Unified Serviceability Administration Guide.

System Requirements for QRT

To operate, the QRT feature requires the following software components:

- Cisco Unified Communications Manager
- Cisco Real-Time Monitoring Tool

Support for the QRT feature extends to any model IP phone that includes the following capabilities:

- Support for softkey templates
- Support for IP phone services
- Controllable by CTI
- An internal HTTP server

Note For more information, see the Cisco Unified IP Phone guide for your phone model.

Extended Functions Service Dependency

The Cisco Extended Functions service depends on the following services:

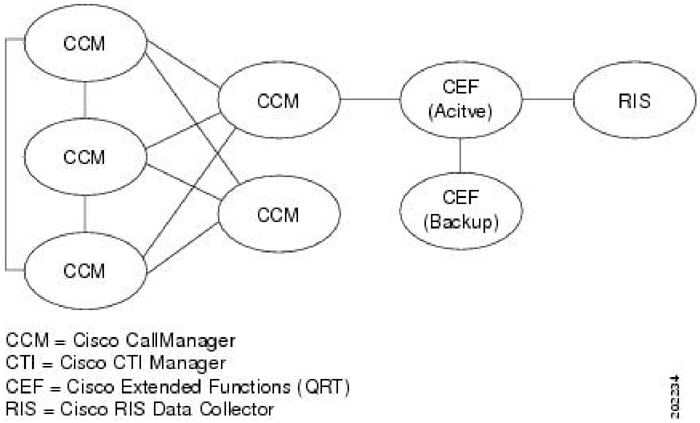
- Cisco CallManager - Ensure a minimum of one Cisco CallManager service is running.
- Cisco CTIManager - Ensure a minimum of one Cisco CTIManager service is running.
- Cisco Database Layer Monitor - Ensure one Cisco Database Layer Monitor service is running on the same server as CEF.
- Cisco RIS Data Collector - Ensure one Cisco RIS Data Collector service is running on the same server as CEF.

Note Ensure Cisco Database Layer Monitor and Cisco RIS Data Collector are running on the same server. You can include more than one CEF service in a Cisco Unified Communications Manager cluster.

Tip Install all the services on one server for one-server Cisco Unified Communications Manager systems.

The following figure shows a typical Cisco Extended Functions service configuration.

Figure 162: Cisco Extended Functions Service Dependency (Typical Configuration)



Extended Functions Applications in a Cluster

If multiple Cisco Extended Functions services are active within a Cisco Unified Communications Manager cluster, CEF uses an algorithm to determine which service should be active and to order the remaining as backups.The CEF application with the lowest IP address becomes active. The service with the next lowest IP address becomes the backup to the active service. Any remaining services act as backups to each other, beginning with the service with the next lowest IP address. If you add any new services to the cluster, CEF restarts the algorithm to determine which service will be active.

Note When a Cisco Extended Functions service gets started in a cluster, the CEF service with the lowest IP address becomes active.This process may cause service interruption for approximately 2 minutes.

To verify the directory status and Cisco Extended Functions service registration status to the Cisco CTIManager, use the Real Time Monitoring Tool as described in the *Cisco Unified Real Time Monitoring Tool Administration Guide*.

Securing a TLS Connection to CTI

QRT supports a secure Transport Layer Security (TLS) connection to CTI. Obtain the secure connection by using the “CCMQRTSecureSysUser” application user, as described in the following procedure.

Note If you enable security from the Service Parameter Configuration window, the QRT will open a secure connection to CTI Manager by using the Application CAPF profile. You should configure both the “CTI Manager Connection Security Flag” and the “CAPF Profile Instance Id for Secure Connection to CTI Manager” service parameters for the secure connection to succeed. See topics related to setting the Cisco extended functions service parameters for QRT. You can also see topics related to application user CAPF profile configuration and Service Parameter configuration in the *Cisco Unified Communications Manager Administration Guide* for more information.

Note You must also configure the security service parameter “Cluster Security Mode CAPF Phone Port” to secure a TLS connection to CTI, giving it a value of 1. You can do this from **System** > **Enterprise Parameters** in Cisco Unified Communications Manager Administration. For more information, see topics related to Enterprise Parameter configuration in the *Cisco Unified Communications Manager Administration Guide*.

Perform the following procedure to configure the application user.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **User Management** > **Application User**.

The Find and List Application Users window displays.

Step 2 Click **Find.**

Step 3 From the Find and List Application Users Configuration window, click CCMQRTSecureSysUser or CCMQRTSysUser.

Note To configure a CAPF profile, see topics related to application user CAPF profile configuration in the *Cisco Unified Communications Manager Administration Guide* for general information and the *Cisco Unified Communications Manager Security Guide* for details.

Related Topics

Set the Cisco Extended Functions Service Parameters for QRT, on page 1049

QRT Operation

This section describes the user interaction features with QRT. After you properly install and configure QRT, the QRT softkey can be configured on certain Cisco Unified IP Phone models. See the system requirements for QRT for the IP phone models that are supported with QRT.

Note The Cisco Unified Communications Manager Standard User template does not include the QRT softkey. You must enable QRT functionality and make it available to users through the use of a QRT softkey. To do this, create, configure, and assign the QRT softkey from Cisco Unified Communications Manager Administration. See topics related to configuring the QRT feature for information about setting up the softkey template.

For more user-related information, see the Cisco Unified IP Phone guide for your phone model:

Related Topics

QRT Feature Configuration, on page 1043

System Requirements for QRT, on page 1033

User Interface

The QRT user interface includes several components:

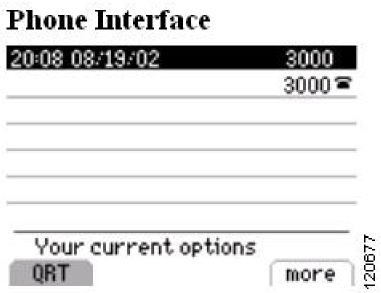
- Phone Screens - Available to all IP phones that are in the common device configuration where the QRT softkey is configured, the phone screen supports different locales.

Only the Cisco Unified Communications Manager administrator can access the following components:

- Serviceability
- Alert Configuration
- Service Parameters
- Viewer Application

The following figure shows an example of the QRT softkey as it displays on a Cisco Unified IP Phone.

Figure 163: QRT Phone Interface Display



Your current options

Related Topics

Configure Alarms and Traces for QRT, on page 1048
Configure the Cisco Unified Serviceability Features, on page 1047
Set the Cisco Extended Functions Service Parameters for QRT, on page 1049
Use the QRT Viewer, on page 1051

Extended Menu Choices

Extended menu choices allow a user to interact with QRT and provide additional details regarding the phone problem that they are reporting. You can choose to enable extended menu choices or provide users with a more passive interface, depending upon the amount of information that you want users to submit.

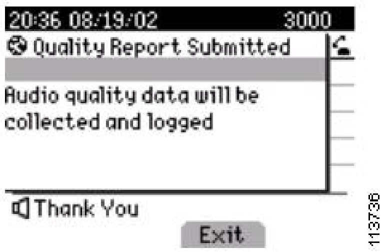
From the Cisco Unified Communications Manager Service Parameters Configuration window, configure the user interface mode for QRT from the following options:

- Silent Mode - In this mode, the user does not get presented with extended menu choices. When the user presses the QRT softkey, the system collects the streaming statistics and logs the report without additional user interaction.

  The system supports silent mode only when the IP phone is in the Connected call state.

  The following figure shows an example of the QRT display as it appears in silent mode.

Figure 164: Submitting Voice Quality Feedback in Silent Mode



Quality Report Submitted

Audio quality data will be collected and logged

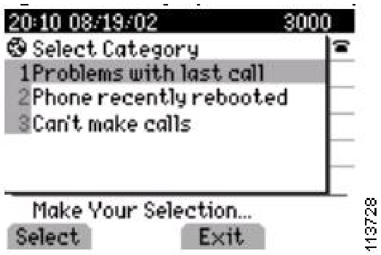
Thank You

- Interview Mode - In this mode, the user gets presented with extended menu choices, which allow additional user input that is related to audio quality on the IP phone (see the Problem Classification Categories and Reason Codes, on page 1038 for the applicable reason codes). This mode also allows the user to report other, non-audio-related problems such as the phone rebooting or the inability to make calls.

  The system supports interview mode only when the IP phone is in the Connected or On Hook call state.

The following figure shows an example of the QRT display as it appears when the QRT softkey is pressed while the phone is on hook and in interview mode.

Figure 165: QRT Phone Interface - On Hook, Interview Mode Display



20:10 08/19/02 3000

Select Category

1 Problems with last call

2 Phone recently rebooted

3 Can't make calls

Make Your Selection...

Note Ensure that you configure the QRT softkey only for the supported call states.

Note Configure the “Display Extended QRT Menu Choices” field in the Cisco Unified Communications Manager Administration Service Parameters configuration window to determine whether the users can access the extended menu choices. See the Set the Cisco Extended Functions Service Parameters for QRT, on page 1049 for additional information.

Problem Classification Categories and Reason Codes

The following tables show the problem categories and corresponding reason codes that users can choose when they report problems with their IP phones:

- Additional options become available after you configure extended menu choices.
- Users can choose only one reason code per category, per problem.
- Each problem category becomes available only when the IP phone is in the supported call state.

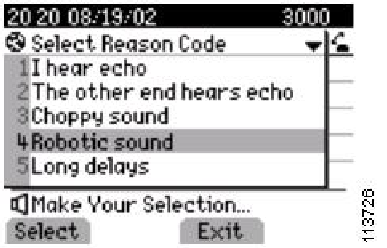
The following table shows the supported call states and the reason codes that are available for the “Problems with current call” category.

Table 106: Problem Category - Problems with Current Call

Problem Category	Supported Call States	Reason Codes	Statistics
Problems with current call	• Connected	• I hear echo • The remote end hears echo • Choppy audio • Robotic sound • Long delays • Low volume • The remote end experiences low volume • I can't hear the remote end • The remote end can't hear me	The system collects streaming statistics from the source and destination devices. **Note** Source device/IP phone refers to the device on which the QRT softkey gets pressed. For example, "source" and "destination" in this case do not see the calling party and called party in a connected call.

The following figure shows an example of the phone display as it appears after the QRT softkey is pressed on an IP phone in the connected state. This menu allows the user to provide additional details before submitting a problem with the current phone call.

Figure 166: Reporting Problem with the Current Call



20 20 08:19:02 3000
Select Reason Code
1 I hear echo
2 The other end hears echo
3 Choppy sound
4 Robotic sound
5 Long delays
Make Your Selection...
Select Exit

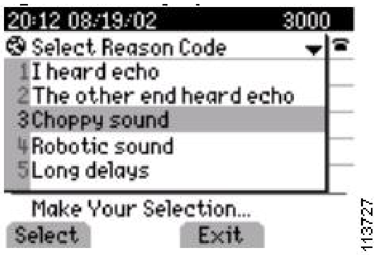
The following table shows the supported call state and the reason codes that are available for the "Problems with last call" category.

Table 107: Problem Category - Problems with Last Call

Problem Category	Supported Call States	Reason Codes	Statistics
Problems with last call	• On Hook	• I heard echo • The remote end heard echo • Choppy audio • Robotic sound • Long delays • Low volume on my end • Low volume on the remote end • I could not hear the remote end • The remote end could not hear me • The call dropped	The system collects streaming statistics from the source device.

The following figure shows an example of the phone display as it appears after the user selects the "Problems with last call" category. This menu allows the user to provide additional details before submitting a problem report for the last phone call.

Figure 167: Reporting Problem with the Last Call



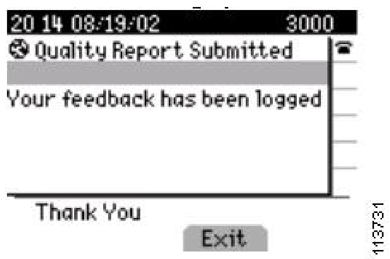
The following table shows the supported call state that is available for the "Phone recently rebooted" category. No associated reason codes exist for this category.

Table 108: Problem Category - Phone Recently Rebooted

Problem Category	Supported Call States	Reason Codes	Statistics
Phone recently rebooted	• On Hook	None	

The following figure shows an example of the phone display after the user chooses the "Phone recently rebooted" category. The system logs user feedback.

Figure 168: Reporting Problem with Phone That Recently Rebooted



20 14 08/19/02 3000

Quality Report Submitted

Your feedback has been logged

Thank You

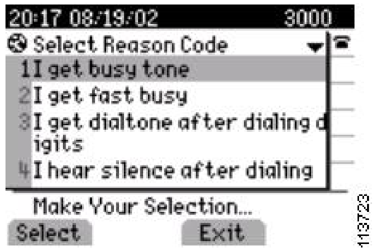
The following table shows the supported call state and the reason codes that are available for the "I can't make calls" category.

Table 109: Problem Category - I Can't Make Calls

Problem Category	Supported Call States	Reason Codes	Statistics
I can't make calls	• On Hook	• I get a busy tone • I get a fast busy tone • I get dial tone after dialing digits • I hear silence after dialing • I don't get dial tone	

The following figure shows an example of the phone display as it appears after the user chooses the "I can't make calls" category.

Figure 169: Reporting Problem with I Can't Make Calls



20:17 08/19/02 3000

Select Reason Code

1 I get busy tone

2 I get fast busy

3 I get dialtone after dialing d igits

4 I hear silence after dialing

Make Your Selection...

Note QRT collects information from various sources, such as the source IP phone, the destination IP phone, the Cisco RIS Data Collector, the Cisco Unified Communications Manager database, and the user. "Source" and "destination" in this case do not see the calling party and called party in a connected call. See the QRT Reports, on page 1051 for detailed information about the fields that the phone problem report includes.

Interactions and Restrictions

The following interactions and restrictions apply when you use the QRT feature with Unified Communications Manager:

- Ensure that Cisco Extended Functions, Cisco CallManager, CTI Manager, and Cisco RIS Data Collector services are running and fully operational.
- As system administrator, you must create, configure, and assign softkey templates to enable the QRT softkey feature on IP phones.
- Ensure that you configure the QRT softkey only for the supported call states.
- The system makes the extended menu choices option available only when the “Display Extended QRT Menu Choices” service parameter is set to True; it provides support for the “Problems with current call” category.
- If another application feature (such as Cisco Call Back or Cisco Unified Communications Manager Assistant) or a function key (such as Settings, Directories, or Messages) is invoked while the user is interacting with QRT, or if the user does not complete the QRT selection, the system can overwrite the QRT display. In this case, the system forces the device into a wait state, which prevents QRT from completing the interaction and then closes the device.

Note Because unattended devices consume large amounts of resources and could impact CTI performance, the system configures QRT to regularly check for opened devices. You cannot modify these system settings.

- Phone that is running SIP that is configured to use UDP as the transport, instead of TCP, will not support the “device data pass-through” functionality. QRT requires the pass-through functionality, so QRT does not support these UDP-configured phones that are running SIP.
- The Quality Report Tool supports IPv6 if the device uses an IP Addressing Mode of IPv4 Only or IPv4 and IPv6 (dual-stack mode). Users with phones with an IP Addressing Mode of IPv6 Only cannot report audio and other problems by pressing the QRT softkey on the phone. In addition, the QRT report does not include the streaming statistics for a phone that has an IP Addressing Mode of IPv6 Only. For more information on IPv6, see the Internet Protocol Version 6 (IPv6), on page 739.

Install and Activate QRT Functions

As a feature within the Cisco Extended Functions service, QRT automatically installs as part of the Cisco Unified Communications Manager installation.

Perform the following steps after installation to enable QRT availability for users and to set up administrative reporting capabilities:

Procedure

Step 1 Properly configure the QRT feature for Cisco Unified IP Phone users.

Step 2 From Cisco Unified Serviceability, activate the Cisco Extended Functions service and configure alarms and traces for use with QRT.

Step 3 Define how the QRT feature will work in your system by configuring the applicable service parameters for the Cisco Extended Functions service.

Step 4 Create, customize, and view phone problem reports by using the QRT Viewer application.

Note If users require the QRT feature to display (softkeys and messages on the IP phone) in any language other than English, verify that the locale installer is installed before configuring QRT. See the Cisco Unified Communications Operating System Administration Guide for more information.

Related Topics

QRT Feature Configuration, on page 1043
Configure the Cisco Unified Serviceability Features, on page 1047
Set the Cisco Extended Functions Service Parameters for QRT, on page 1049
Use the QRT Viewer, on page 1051

QRT Feature Configuration

This section provides configuration information for enabling QRT. For successful configuration of the QRT feature, review the QRT Configuration Checklist, perform the configuration requirements, activate the Cisco Extended Functions service, and set the service parameters.

Tip Before you configure the QRT feature, review the configuration summary task for this feature.

Related Topics

Configure QRT, on page 1029

Create a Softkey Template with the QRT Softkey

Perform the following procedure to create a new softkey template with the QRT softkey.

Procedure

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

Step 2 Click **Add New**. (Alternatively, you can click the Find button to view a list of the available softkey templates.)

a) If you click the **Add New** button, choose the Standard User softkey template from the Create a softkey template based on drop-down list.

b) If you click the **Find** button to view a list of the available softkey templates, choose the Standard User softkey template from the Softkey Template list.

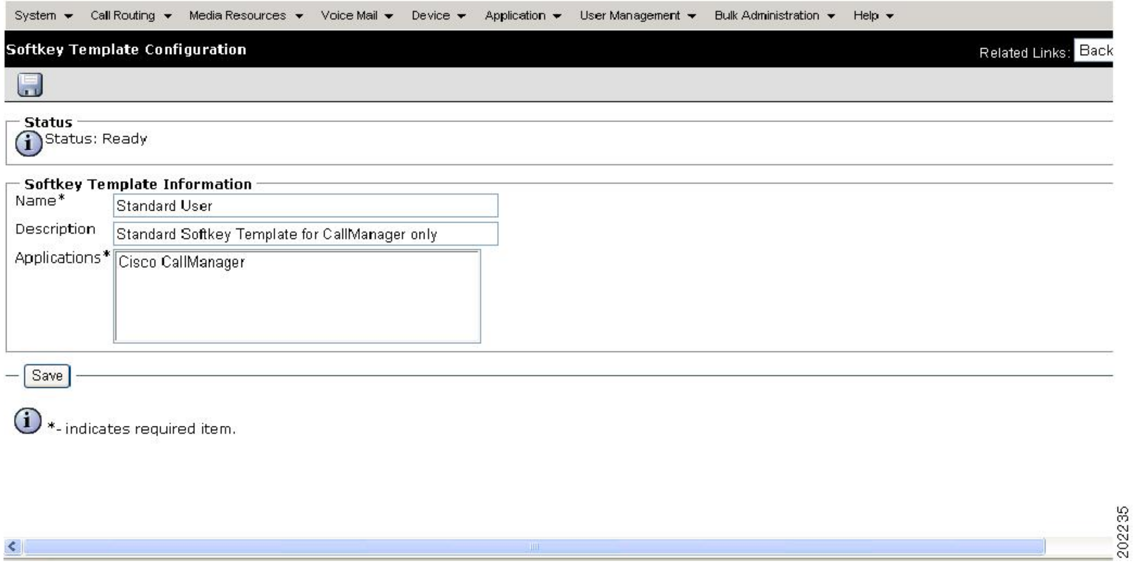
Step 3 Click the **Copy** button.

The Softkey Template Configuration window displays with new information.

Step 4 In the Softkey Template Name field, enter a new name for the template; for example, QRT Standard User; then, add a description.

The following figure shows an example of the Cisco Unified Communications Manager Administration Softkey Template Configuration window where you copy a softkey template.

Figure 170: Softkey Template Configuration Window



Status: Ready

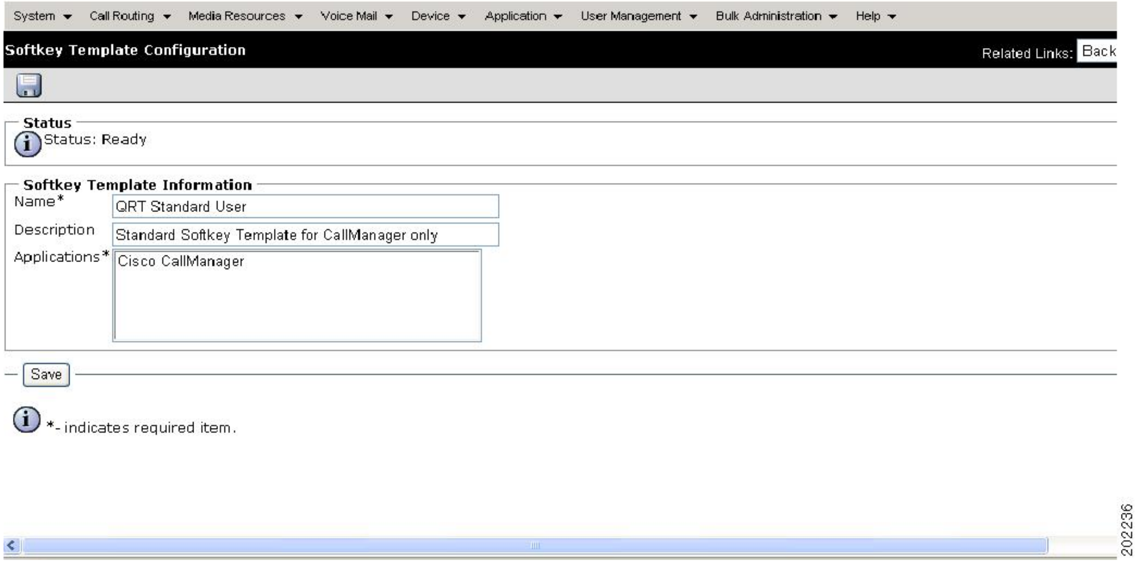
Name* Standard User

Description Standard Softkey Template for CallManager only

Applications* Cisco CallManager

*- indicates required item.

Figure 171: Softkey Template Configuration Window After Copy



Status: Ready

Name* QRT Standard User

Description Standard Softkey Template for CallManager only

Applications* Cisco CallManager

*- indicates required item.

Step 5 Click **Save.**

The Softkey Template Configuration redisplays with new information.

Step 6 To add an application, click the **Add Application** button. See the *Cisco Unified Communications Manager Administration Guide* for detailed instructions.

Step 7 To add the QRT softkey to the template, choose Configure Softkey Layout from the Related Links drop-down list box on the Softkey Template Configuration window and click **Go.**

The Softkey Layout Configuration window displays.

Note You must add the QRT softkey to the Connected and On Hook call states.

Step 8 To add the QRT softkey to the On Hook call state, choose **On Hook** from the call states drop-down list box.

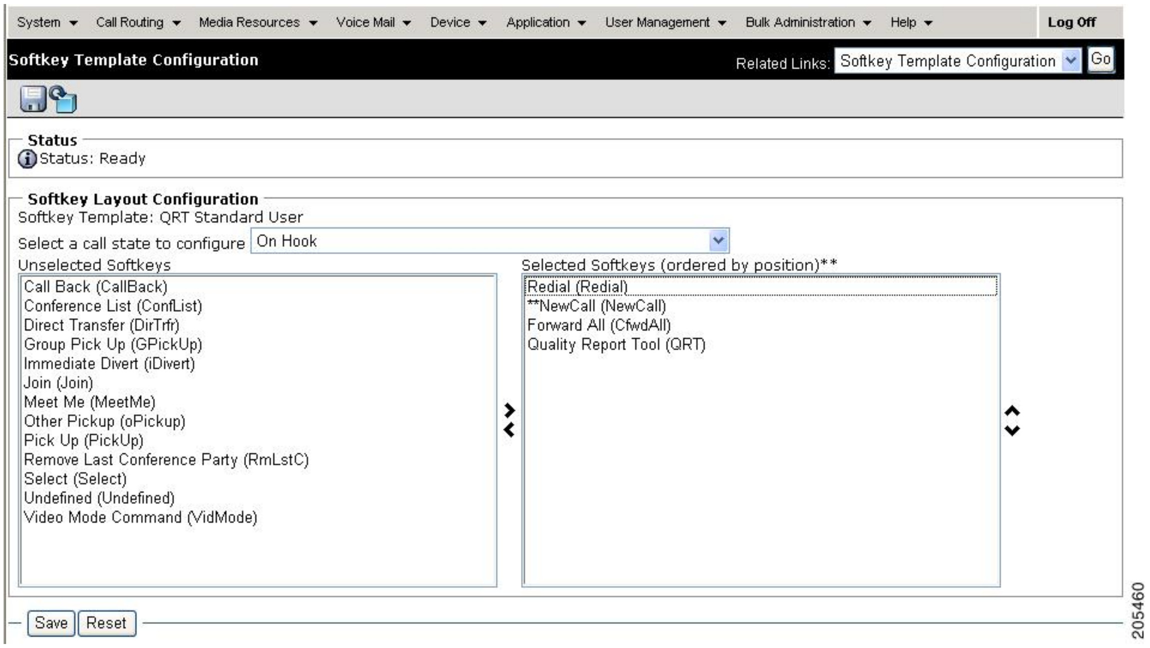
The Softkey Layout Configuration window redisplays with the Unselected Softkeys and Selected Softkeys lists.

Step 9 From the Unselected Softkeys list, choose the **Quality Report Tool** (QRT) softkey and click the right arrow to move the softkey to the Selected Softkeys list.

You can prioritize the items in the Selected Softkeys list by using the up and down arrow keys.

The following figure shows an example of the Cisco Unified Communications Manager Administration Softkey Layout Configuration window.

Figure 172: QRT Softkey Layout Configuration



Softkey Template Configuration

Status

Status: Ready

Softkey Layout Configuration

Softkey Template: QRT Standard User

Select a call state to configure: On Hook

Unselected Softkeys:
- Call Back (CallBack)
- Conference List (ConfList)
- Direct Transfer (DirTrfr)
- Group Pick Up (GPickUp)
- Immediate Divert (iDivert)
- Join (Join)
- Meet Me (MeetMe)
- Other Pickup (oPickup)
- Pick Up (PickUp)
- Remove Last Conference Party (RmLstC)
- Select (Select)
- Undefined (Undefined)
- Video Mode Command (VidMode)

Selected Softkeys (ordered by position)**:
- Redial (Redial)
- **NewCall (NewCall)
- Forward All (CfwdAll)
- Quality Report Tool (QRT)

Step 10 To save and continue, click **Save.**

Step 11 To add the QRT softkey to the Connected call state, repeat the procedure for each individual call state.

Note Ensure that you configure the QRT softkey only for the supported call states and click the **Save** button after each entry.

Configure the QRT Softkey Template in Common Device Configuration

Perform the following procedure to add the QRT softkey template to the common device configuration.

Procedure

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

Step 2 Click **Find.**

Step 3 Choose any previously created common device configuration that displays.

You can add the template to any customized common device configuration for QRT feature users.

Step 4 In the Softkey Template field, choose the softkey template that contains the QRT softkey from the drop-down list box. (If you have not created this template, see the Create a Softkey Template with the QRT Softkey, on page 1043.)

Note All IP phones that are part of this common device configuration inherit this softkey template to provide an easy way for you to assign softkey templates to multiple phones. To associate softkey templates to individual IP phones, see the Add the QRT Softkey Template in Phone Configuration, on page 1046.

Step 5 Click **Save.**

Add the QRT Softkey Template in Phone Configuration

Perform the following procedure to add the QRT softkey template to each user phone.

Procedure

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

The Find and List Phones window displays.

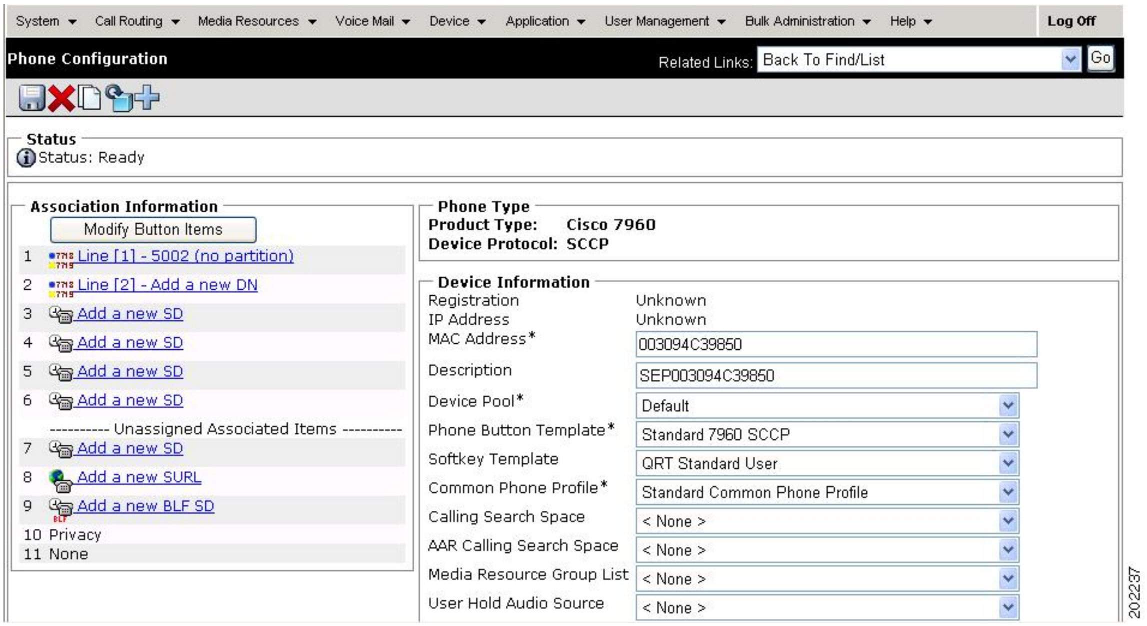
Step 2 Find the phone to which you want to add the softkey template. See the *Cisco Unified Communications Manager Administration Guide*.

Step 3 In the Softkey Template field, choose the softkey template that contains the QRT softkey from the drop-down list box. (If you have not created this template, see the Create a Softkey Template with the QRT Softkey, on page 1043.)

If you alternatively configured the softkey template in the common device configuration, from the Common Device Configuration field, choose the common device configuration that contains the new softkey template.

The following figure shows an example of the Cisco Unified Communications Manager Administration Phone Configuration window.

Figure 173: Phone Configuration



Phone Configuration

Related Links: Back To Find/List

Status

Status: Ready

Association Information

1 Line [1] - 5002 (no partition)
2 Line [2] - Add a new DN
3 Add a new SD
4 Add a new SD
5 Add a new SD
6 Add a new SD
---------- Unassigned Associated Items ----------
7 Add a new SD
8 Add a new SURL
9 Add a new BLF SD
10 Privacy
11 None

Phone Type

Product Type: Cisco 7960
Device Protocol: SCCP

Device Information

Registration	Unknown
IP Address	Unknown
MAC Address*	003094C39850
Description	SEP003094C39850
Device Pool*	Default
Phone Button Template*	Standard 7960 SCCP
Softkey Template	QRT Standard User
Common Phone Profile*	Standard Common Phone Profile
Calling Search Space	< None >
AAR Calling Search Space	< None >
Media Resource Group List	< None >
User Hold Audio Source	< None >

Step 4 Click **Save.**

Configure the Cisco Unified Serviceability Features

This section describes how to activate and configure the Cisco Unified Serviceability features for use with QRT. The Cisco Extended Functions service uses the following Cisco Unified Serviceability features:

- Service Activation - Configured from the Cisco Unified Serviceability Tools window.
- SDI Trace - Configured from the Cisco Unified Serviceability Trace Configuration window.
- Alarm Interface - Configured from the Cisco Unified Serviceability Alarm Configuration window.
- Real Time Monitoring Tool (RTMT) - Used to monitor the operating status of QRT and CTIManager. For detailed information about RTMT, see the Cisco Unified Real Time Monitoring Tool Administration Guide.

For additional information about Cisco Unified Serviceability, see the *Cisco Unified Serviceability Administration Guide*.

Activate the Cisco Extended Functions Service for QRT

Follow this procedure to activate the Cisco Extended Functions service for use with the QRT feature.

Procedure

Step 1 From the Navigation drop-down list box in Cisco Unified Communications Manager Administration, located in the upper, right corner of the window, choose Cisco Unified Serviceability and click **Go.**

The Cisco Unified Serviceability window displays.

Step 2 To activate the Cisco Extended Functions service, choose **Tools** > **Service Activation**.

A Server drop-down list box displays.

Step 3 From the Server drop-down list box, choose the Cisco Unified Communications Manager server on which you want to activate the Cisco Extended Functions service.

Step 4 Check the Cisco Extended Functions check box.

Step 5 Click **Save.**

The CEF activation status changes from deactivated to activated.

Tip You can check the activation status of the Cisco Extended Functions service from Cisco Unified Serviceability by choosing **Tools** > **Control Center - Feature Services**. Look for Cisco Extended Functions; if the Cisco Extended Functions service is active, it displays as Activated.

Configure Alarms and Traces for QRT

Follow these procedures to configure alarms and SDI traces through Cisco Unified Serviceability.

Procedure

Step 1 From the Cisco Unified Serviceability window, choose **Alarm** > **Configuration.**

A Server drop-down list box displays.

Step 2 From the Server drop-down list box, choose the Cisco Unified Communications Manager server on which you want to configure alarms.

Step 3 From the Service Group drop-down list box, choose **CM Services**.

Step 4 From the Service drop-down list box, choose **Cisco Extended Functions**.

Step 5 Check the Enable Alarm check box for both Local Syslogs and SDI Trace.

Step 6 From the drop-down list box, configure the Alarm Event Level for both Local Syslogs and SDI Trace by choosing one of the following options:

a) Emergency
b) Alert
c) Critical
d) Error
e) Warning
f) Notice
g) Informational
h) Debug

The default value specifies Error.

Step 7 Click **Save.**

Step 8 From the Cisco Unified Serviceability window, choose **Trace** > **Configuration.**

A Server drop-down list box displays.

Step 9 From the Server drop-down list box, choose the Cisco Unified Communications Manager server on which you want to configure traces.

Step 10 From the Service Group drop-down list box, choose **CM Services**.

Step 11 From the Service drop-down list box, choose **Cisco Extended Functions**.

Step 12 Check the following check boxes:

a) Trace On
b) Cisco Extended Functions Trace Fields

Step 13 From the drop-down list box, configure the Debug Trace Level by choosing one of the following options:

a) Error
b) Special
c) State Transition
d) Significant
e) Entry_exit
f) Arbitrary
g) Detailed

The default value specifies Error.

Note Cisco recommends that you check all the check boxes in this section for troubleshooting purposes.

Step 14 Click **Save.**

For additional information about configuring alarms and traces, see the *Cisco Unified Serviceability Administration Guide*.

Set the Cisco Extended Functions Service Parameters for QRT

Follow this procedure to set the Cisco Extended Functions service parameters by using Cisco Unified Communications Manager Administration.

Note Cisco recommends that you use the default service parameters settings unless the Cisco Technical Assistance Center (TAC) instructs otherwise.

Procedure

Step 1 If your display shows the Cisco Unified Serviceability window, from the Navigation drop-down list box, located in the upper, right corner of the window, choose Cisco Unified CM Administration and click **Go.**

Step 2 The Cisco Unified CM Administration window displays. Choose **System** > **Service Parameters**.

Step 3 A Server drop-down list box displays. Choose the Cisco Unified Communications Manager server where the QRT application resides.

Step 4 A Service drop-down list box displays. Choose the Cisco Extended Functions service.

Step 5 Configure the following Cisco Extended Functions service parameters for QRT.

a) Display Extended QRT Menu Choices - Determines whether extended menu choices are presented to the user. You can choose one of the following configuration options:

- Set this field to true to display extended menu choices (interview mode).
- Set this field to false to not display extended menu choices (silent mode).
- The recommended default value specifies false (silent mode).

b) Streaming Statistics Polling Duration - Determines the duration that is to be used for polling streaming statistics. You can choose one of the following configuration options:

- Set this field to -1 to poll until the call ends.
- Set this field to 0 to not poll at all.
- Set it to any positive value to poll for that many seconds. Polling stops when the call ends.
- The recommended default value specifies -1 (poll until the call ends).

c) Streaming Statistics Polling Frequency (seconds) - Designates the number of seconds to wait between each poll:

- The value ranges between 30 and 3600.
- The recommended default value specifies 30.

d) Maximum No. of Files - Specifies the maximum number of files before the file count restarts and overwrites the old files:

- The value ranges between 1 and 10000.
- The recommended default value specifies 250.

e) Maximum No. of Lines per File - Specifies the maximum number of lines in each file before starting the next file:

- The value ranges between 100 and 2000.
- The recommended default value specifies 2000.

Step 6 To configure a secure TLS connection to CTI, configure the following service parameters.

a) CAPF Profile Instance Id for Secure Connection to CTI Manager - Specifies the Instance ID of the Application CAPF Profile for application user CCMQRTSysUser that the Cisco Extended Function service will use to open a secure connection to CTI Manager. You must configure this parameter if CTI Manager Connection Security Flag is enabled.

Note Remember to turn on security by enabling the CTI Manager Connection Security Flag service parameter. You must restart the Cisco Extended Functions service for the changes to take effect.

See the Securing a TLS Connection to CTI, on page 1035 for information on configuring the Application CAPF Profile.

b) CTI Manager Connection Security Flag - Indicates whether security for Cisco Extended Functions service CTI Manager connection is enabled or disabled. If enabled, Cisco Extended Functions will open a secure connection to CTI Manager using the Application CAPF Profile configured for the Instance ID for application user CCMQRTSysUser.

c) The value choices are True and False.

d) You must choose True to enable a secure connection to CTI.

Step 7 Click **Save.**

Use the QRT Viewer

You can use the QRT Viewer to view the IP phone problem reports that the Quality Report Tool generates. The QRT Viewer allows you to filter, format, and view the tool-generated phone problem reports, so they provide you with the specific information that you need.

- To view the QRT Viewer application, you need to install the Cisco Real Time Monitoring Tool (RTMT) plug-in, which includes the trace collection feature.
- The trace collection feature enables collection and viewing of log files; the QRT Viewer is included with the trace collection feature.

Note For detailed information about installing and configuring the RTMT and trace collection feature, and for detailed information about accessing, configuring, using, and customizing the QRT Viewer for IP phone problem reports, see the *Cisco Unified Serviceability Administration Guide* and the *Cisco Unified Real Time Monitoring Tool Administration Guide*.

QRT Reports

QRT collects information from various sources, such as the source IP phone, the destination IP phone, the Cisco RIS Data Collector, Cisco Unified Communications Manager, and the user. (The system does not collect information from gateways or other devices.) “Source” and “destination” in this case, do not see the calling party and called party in a connected call.

Note See the QRT Viewer chapter in the Cisco Unified Serviceability Administration Guide for additional information about QRT reports.

The following list provides information, segmented by information source, about the QRT report fields.

Information Collected From the Source Device

- Directory number of source device (in the case of multiline devices, the information shows only the first primary directory number)
- Source device type (for example, CP-7960, CP-7940)
- Source stream1 port number

- Source codec (for example, G.711u)
- Source packets (for example, 2,45,78)
- Source rcvr packets (for example, 12,45,78)
- Source rcvr jitter (for example, 0 0)
- Source rcvr packet lost (for example, 0,21 0,21)
- Source sampling timestamp, implicit (for example, 12:30, 13:00, 13:30, 14:00)
- Destination device name (IP)
- Destination stream1 port number

Note The number of samples that are collected for packets, jitter, packets lost, and so on, depends on the sampling duration and polling frequency. The streaming information gets collected only one time per call. For example, if phone A called phone B and both phone A and phone B submit multiple reports for the same call, only the first report includes the streaming data. Also, for the "Problems with last call" category, these values might reflect only the last snapshot of the streaming statistics that are stored in the phone device.

Information Collected From the Destination Device

The system collects the following information if the destination device is a supported Cisco Unified IP Phone within same Cisco Unified Communications Manager system or cluster. If the destination device is not an IP phone, the information includes only IP address, device name, and device type.

- Directory number of destination device (in the case of multiline devices, the information shows only the first primary directory number)
- Destination device type (for example, CP-7960, CP-7940)
- Destination codec
- Destination packets
- Destination rcvr packets
- Destination rcvr jitter
- Destination rcvr packet lost
- Destination sampling timestamp (Implicit)

Note The number of samples that are collected for packets, jitter, packets lost, and so on, depends on the sampling duration and polling frequency. The streaming information gets collected only one time per call. For example, if phone A called phone B and both phone A and phone B submit multiple reports for the same call, only the first report includes the streaming data that is included. QRT attempts to collect the information from the destination IP phone only for the "Problems with current call" category.

Information Collected From RIS Data Collector

- Source device owner (user name that is currently logged in to the IP phone; if no explicitly logged-in user exists, this field specifies null)
- IP address for source device
- Registered Cisco Unified Communications Manager name for source device
- Source device type (if the device is not one of the supported IP phones; for example, RISCLASS_PHONE, RISCLASS_GATEWAY, RISCLASS_H323, RISCLASS_CTI, RISCLASS_VOICEMAIL)
- Source device model (for example, DBLTypeModel::MODEL_TELECASTER_MGR, DBLTypeModel::MODEL_TELECASTER_BUSINESS)
- Source device product (for example, DBLTypeProduct::PRODUCT_7960, DBLTypeProduct::PRODUCT_7940)
- Destination device name
- Destination device type (if the device is not one of the supported IP phones; for example, RISCLASS_PHONE, RISCLASS_GATEWAY, RISCLASS_H323, RISCLASS_CTI, RISCLASS_VOICEMAIL)
- Destination device model (for example, DBLTypeModel::MODEL_TELECASTER_MGR, DBLTypeModel::MODEL_TELECASTER_BUSINESS)
- Destination device product (for example, DBLTypeProduct::PRODUCT_7960, DBLTypeProduct::PRODUCT_7940)
- Registered Cisco Unified Communications Manager name for destination device
- Destination device owner (user name that is currently logged in to the IP phone; if no explicitly logged-in user exists, this field specifies null)

Information Collected From Cisco Unified Communications Manager/CTIManager

- Source device name (MAC address)
- CallingPartyNumber (the party who placed the call; for transferred calls, the transferred party becomes the calling party)
- OriginalCalledPartyNumber (the original-called party after any digit translations occurred)
- FinalCalledPartyNumber (for forwarded calls, this specifies the last party to receive the call; for non-forwarded calls, this field specifies the original called party)
- LastRedirectDn (for forwarded calls, this field specifies the last party to redirect the call; for non-forwarded calls, this field specifies the last party to redirect, via transfer or conference, the call)
- globalCallID_callManagerId (this field distinguishes the call for CDR Analysis and Reporting (CAR))
- globalCallID_callId (this field distinguishes the call for CAR)
- CallState (Connected, On Hook)

Information Collected From the Cisco Unified Communications Manager Database

- Sampling duration - Service parameter (for example, 50 seconds)
- Sampling frequency - Service parameter (for example, 30 seconds)
- Cluster ID - Enterprise parameter

Information Collected From the User

- Category
- ReasonCode
- TimeStamp (Implicit)

The following table shows the available fields for each supported category.

Note The following QRT report fields will display appropriate phone model and product names (for example, Phone That Is Running SCCP): Source Model, Source Product, Destination Model, Destination Product, and CallState.

Table 110: QRT Fields by Supported Category

Information Source	Problems with Current Call	Problems with Last Call	Phone Recently Rebooted	Can’t Make Calls
Source Device Name	X	X	X	X
DN of Source Device	X	X	X	X
IP Address of Source Device	X	X	X	X
Source Device Type	X	X	X	X
Source Device Owner	X	X	X	X
Registered Cisco Unified Communications Manager for Source Device	X	X	X	X
Source Model	X	X	X	X
Source Product	X	X	X	X
Source Stream 1 Port Number	X	X		

Information Source	Problems with Current Call	Problems with Last Call	Phone Recently Rebooted	Can't Make Calls
Source Codec	X	X		
Source Packets	X	X		
Source Rcvr Packets	X	X		
Source Rcvr Jitter	X	X		
Source Rcvr Packet Lost	X	X		
Source Sampling Timestamp	X			
Destination Device Name	X	X		
DN of Destination Device	X	X		
IP Address of Destination Device	X	X		
Destination Device Type	X	X		
Destination Stream 1 Port Number	X			
Destination Codec	X			
Destination Packets	X			
Destination Rcvr Packets	X			
Destination Rcvr Jitter	X			
Destination Rcvr Packet Lost	X			
Destination Sampling Timestamp	X			
Destination Device Owner	X	X		

Information Source	Problems with Current Call	Problems with Last Call	Phone Recently Rebooted	Can’t Make Calls
Registered Cisco Unified Communications Manager for Destination Device	X	X		
Destination Model	X	X		
Destination Product	X	X		
Calling Party Number	X			
Original Called Party Number	X			
Final Called Party Number	X			
Last Redirect DN	X			
globalCallID_callManagerId	X			
globalCallID_callId	X			
Sampling Duration	X	X	X	X
Sampling Frequency	X	X	X	X
Cluster ID	X	X	X	X
Category	X	X	X	X
Reason Code	X	X		X
TimeStamp When Report is Submitted	X	X	X	X

Information Source	Problems with Current Call	Problems with Last Call	Phone Recently Rebooted	Can't Make Calls
sProtocol **Note** sProtocol represents the source protocol for the phones. This protocol has a value of 1 for phones that are running SCCP, 2 for phones that are running SIP, and 0 for UNKNOWN.	X	X	X	X
dProtocol **Note** dProtocol represents the destination protocol for the phones. This protocol has a value of 1 for phones that are running SCCP, 2 for phones that are running SIP, and 0 for UNKNOWN.	X	X		

Provide Information to Users for the QRT Feature

The Cisco Unified IP Phone guides provide procedures for how to use the QRT feature on the Cisco Unified IP Phone. For more information, see the Cisco Unified IP Phone guide for your phone model. http://software.cisco.com/download/release.html?mdfid=284510097&flowid=45900&softwareid=282074294&release=9.1(2)&relind=AVAILABLE&rellifecycle=&reltype=latest

Troubleshooting the QRT Feature

Cisco Unified Serviceability provides web-based tools to assist in troubleshooting Cisco Unified Communications Manager problems. Use the Cisco Unified Serviceability Trace Configuration, Alarm Configuration, and Real Time Monitoring Tool to help troubleshoot problems with QRT. See the Cisco Unified Serviceability Administration Guide for more information.

The Trace and Alarm tools work together. You can configure trace and alarm settings for Cisco CallManager services and direct alarms to local Syslogs or system diagnostic interface (SDI) log files. (SDI log files are viewable in text format only.)

You can set up traces for Cisco CallManager services on debug levels, specific trace fields, and Cisco Unified Communications Manager devices such as phones or gateways. You can also perform a trace on the alarms that are sent to the SDI trace log files.

Use the trace collection feature to collect trace files and to analyze trace data for troubleshooting problems. (The trace collection feature includes the QRT Viewer.)

The trace collection feature provides three main functions:

- Configure trace parameters
- Collect trace files
- Analyze trace data for troubleshooting problems

Note Enabling Trace decreases system performance; therefore, enable Trace only for troubleshooting purposes. For assistance in using Trace, contact Cisco TAC.

Troubleshooting Tips

The following examples provide some common problems and recommended actions when troubleshooting scenarios for QRT:

The QRT softkey is not available.

Ensure that you have created, configured, and assigned the softkey template to enable the QRT feature.

The QRT softkey is not working.

Ensure that the Cisco Extended Functions service, the Cisco CallManager service, the Cisco CTIManager service, and the Cisco RIS Data Collector service are operational.

The QRT report does not include data.

The system collects data from various sources, such as the user, source IP phone, destination IP phone, RIS Data Collector, Cisco Unified Communications Manager, and Cisco Unified Communications Manager databases. Check to make sure that the destination device is a supported IP phone and not a gateway or other unsupported device; otherwise, the system does not collect data from the destination device.

Note For more information about Cisco Unified Serviceability tools, see the *Cisco Unified Serviceability Administration Guide*.

Note For information about troubleshooting Cisco Unified Communications Manager, see the *Troubleshooting Guide for Cisco Unified Communications Manager*.

CHAPTER 45

Remote Worker Emergency Calling

Cisco Unified Communications Manager (Unified CM) can serve users on the customer premises and also users not on the customer premises (off-premises), using remote Virtual Private Network (VPN) connections. When users are on-premises, their location can be discovered automatically, by Unified CM Device Mobility or by Cisco Emergency Responder (ER), for the purpose of determining how to route emergency calls to the appropriate Public Safety Answering Point (PSAP) and to indicate the caller’s location to the PSAP. Without correct location information, emergency calls may reach a PSAP that is unable to dispatch emergency services to the caller’s location, or emergency services may be dispatched to the wrong location.

The Remote Worker Emergency Calling feature supported by Unified CM and ER enables customers to extend reliable emergency calling support to remote workers, by requiring remote workers to confirm or update their location whenever their device registration is interrupted. Users of devices designated for off-premises (connected remotely to the customer network) use are first presented with a (customizable) disclaimer notice, which assures that users are aware of the need to provide correct location information. Then the off-premises location currently associated with the designated device is presented. Users may confirm their current location or select another previously stored location from their device display; if their location is new, then they are directed to the ER Off-Premises User web page to create a new location.

Prior to completion of this process, the user’s device may be restricted by the customer to calling a single configured destination. This assures that the user has acknowledged the disclaimer and provided their current location information before the user’s device is enabled for normal use.

Intrado V9-1-1 service validates and stores the location the user provides, and emergency calls from off-premises users are forwarded by ER and Unified CM to Intrado. Intrado routes emergency calls to the PSAP with jurisdiction for the caller’s location and delivers the user-provided location information together with each call.

Set Up Remote Worker Emergency Calling

Before you begin

The Remote Worker Emergency Calling features requires that the off-premises user be equipped with a hardware IP phone or software client that supports this feature. The customer must deploy ER as well as Unified CM, and must subscribe to Intrado V9-1-1 emergency call delivery service. Intrado V9-1-1 service is available only in the United States of America.

Procedure

Step 1 Configure the **Owner User ID** on the **Phone Configuration** page to associate the device to be used as off-premises, with the user who is the owner of the device.

For more information, see Cisco Unified IP Phone Configuration of the *Cisco Unified Communications Manager Administration Guide*.

Step 2 Select **Require off-premise location**, under Device Information on the **Phone Configuration** page.

For more information, see Cisco Unified IP Phone Configuration of the *Cisco Unified Communications Manager Administration Guide*.

Step 3 Provision alternate routing to be used when a user chooses not to set their location on the phone.

Alternate routing is accomplished using Clusterwide CallManager Service Parameters:

- Alternate Destination for Emergency Call
- Alternate Calling Search Space for Emergency Call

Note These parameters specify the calling search space and destination number that are used to restrict the routing of any call made from a registered off-premise device where the user chose not to set a location. If these parameters are not configured, then calls will be routed normally.

For more information, see Service Parameters of the *Cisco Unified Communications Manager Administration Guide*.

Step 4 Provision the application server to enable the E911 Proxy to communicate with the Cisco ER provider. This URL is used to direct the end-user to the application server where they enter the location of the device.

For more information, see Application Server Configuration of the *Cisco Unified Communications Manager Administration Guide*.

Step 5 Provision the E911 messages that appear on the end-users phone.

These messages appear on the end-users device when they are off-premise. Optionally, these messages may be edited.

For more information, see Set up E911 Messages of the *Cisco Unified Communications Manager Administration Guide*.

CHAPTER 46

Single Sign-On

This chapter provides information about the Single Sign-On feature which allows end users to log into a Windows client machine on a Windows domain, then use certain Cisco Unified Communications Manager applications without signing on again.

For more information about the Single Sign-On feature, refer to the Cisco white paper A complete guide for installation, configuration and integration of CUCM8.5 with Open Access Manager and Active Directory for SSO.

Configure Single Sign-On

The single sign-on feature allows end users to log into a Windows client machine, then use certain Cisco Unified Communications Manager applications without signing on again.

Perform the following steps to configure single sign-on in your network.

For information about configuring single sign-on with Cisco Unified Communication interface for Microsoft Office Communicator, refer to the Cisco Unified Communication interface for Microsoft Office Communicator documentation.

Procedure

Step 1 Ensure that your environment meets the requirements.

Step 2 Provision the OpenAM server in Active Directory, then generate keytab files.

Note If your Windows version does not include the ktpass tool for generating keytab files, then you must obtain it separately.

Step 3 Import the OpenAM server certificate into the Cisco Unified Communications Manager tomcat-trust store.

Note You can not access any web applications if you do not import the OpenAM server certificate while enabling SSO.

Step 4 Configure Windows single sign-on with Active Directory and OpenAM.

Step 5 (For Cisco Unified Administration only) Verify that the user is provisioned in the Active Directory.

Step 6 (For Cisco Unified Administration only) Synchronize the user data to the Cisco Unified Communications Manager database using the DirSync service.

Step 7 (For Cisco Unified Administration only) Add the user to the CCM Super Users group to enable access to Cisco Unified Administration.

Step 8 Configure client browsers for single sign-on.

Step 9 Enable single sign-on in Cisco Unified Communications Manager.

Related Topics

System Requirements for Single Sign-On, on page 1064
Import the OpenAM Certificate Into CUCM, on page 1066
Configure Windows Single Sign-On with Active Directory and OpenAM, on page 1066
Configure Client Browsers for Single Sign-On, on page 1066
CLI Commands for Single Sign-On, on page 1068

Single Sign-On For CUCM Feature

The Single Sign-On feature allows end users to log into Windows, then use the following Cisco Unified Communications Manager applications without signing on again:

- Cisco Unified Communications Self Care Portal
- Cisco Unified Communications Manager Administration
- Real-Time Monitoring Tool (RTMT) Administration
- Cisco Unified Communication interface for Microsoft Office Communicator

System Requirements for Single Sign-On

The following single sign-on system requirements exist for Cisco Unified Communications Manager:

- Cisco Unified Communications Manager release 8.5(1) on each server in the cluster

The feature requires the following third-party applications:

- Microsoft Windows Server 2003 or Microsoft Windows Server 2008
- Microsoft Active Directory
- ForgeRock Open Access Manager (OpenAM) version 9.0

The single sign-on feature uses Active Directory and OpenAM in combination to provide single sign-on access to client applications.

These third party products must meet the following configuration requirements:

- Active Directory must be deployed in a Windows domain-based network configuration, not just as an LDAP server.

- The OpenAM server must be accessible on the network to all client systems and the Active Directory server.
- The Active Directory (Domain Controller) server, Windows clients, Cisco Unified Communications Manager, and OpenAM must be in the same domain.
- DNS must be enabled in the domain.
- No third-party products may be installed on the Cisco Unified Communications Manager server.
- The clocks of all the entities participating in SSO must be synchronized

See the third-party product documentation for more information about those products.

Install and Activate Single Sign-On

After you install Cisco Unified Communications Manager 8.6(1), your network can support single sign-on if you perform the necessary configuration tasks. For information on configuration tasks that you must perform, see the Configure Single Sign-On, on page 1063.

Configure Single Sign-On

This section provides information to configure single sign-on.

Tip Before you configure single sign-on, review the configuration summary task for this feature.

Related Topics

Configure Single Sign-On, on page 1063

Configure OpenAM

Perform the following tasks using OpenAM:

- Configure policies in OpenAM for the following:
  - CUCM User and UDS web application
  - Query Parameters
    - Configure a J2EE Agent Profile for Policy Agent 3.0.
    - Configure a Windows Desktop SSO login module instance.
    - Configure “Login Form URI” and “OpenAM Login URL” for the PA.
    - Disable local user profiles.

Import the OpenAM Certificate Into CUCM

Because communication between Cisco Unified Communications Manager and OpenAM is secure, you must obtain the OpenAM security certificate and import it into the Cisco Unified Communications Manager tomcat-trust store. Configure the OpenAM certificate to be valid for five years.

For information about importing certificates, see the Cisco Unified Communications Operating System Administration Guide.

Configure Windows Single Sign-On with Active Directory and OpenAM

This section describes how to configure Windows single sign-on with Active Directory and OpenAM. This procedure allows Cisco Unified Communications Manager to authenticate with Active Directory.

Procedure

Step 1 In Active Directory, create a new user with the OpenAM Enterprise host name (without the domain name) as the User ID (login name).

Step 2 Create keytab files on the Active Directory server.

Step 3 Export the keytab files to the OpenAM system.

Step 4 In OpenAM, create a new authentication module instance with the following configuration:

- The type is Windows Desktop SSO.
- The realm attributes are determined as follows:
- Service Principal: Enter the principal name that you used to create the keytab file.
- Keytab File Name: Enter the path where you imported the keytab file.
- Kerberos Realm: Enter the domain name.
- Kerberos Server Name: Enter the FQDN of the Active Directory server.
- Authentication level: Enter 22.

Configure Client Browsers for Single Sign-On

This section describes how to configure client browsers to use single sign-on. To use single sign-on for a browser-based client application, you must configure the web browser.

Configure Internet Explorer for Single Sign-On

The single sign-on feature supports Windows clients running Internet Explorer version 6.0 and higher. Do the following tasks to configure Internet Explorer to use single sign-on:

- Select the Integrated Windows Authentication option.
- Create a custom security level configured as follows:

    - Select the Automatic Logon Only in Intranet Zone option
    - Select all of the options for sites.
    - Add OpenAM to the local zone, if it not already added.

- Do the following tasks for Internet Explorer 8.0 running on Windows 7:
    - Disable Protected Mode.
    - Under registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\, add DWORD value SuppressExtendedProtection - 0x02.

Configure FireFox for Single Sign-On

The single sign-on feature supports Windows clients running Firefox version 3.0 and higher.

To configure Firefox to use single sign-on, enter the trusted domains and URLs that are permitted to engage in SPNEGO Authentication with the browser into the network.negotiate-auth.trusted-uris preference.

Configure the SSO Application

To configure SSO, click **Cisco Unified OS Administration** > **Security** > **Single Sign On**.

Note SSO is supported only for End User accounts, such as Agent Flow or SAML. SSO is not supported for Application User accounts.

This application is split into three components:

- Status
- Select Applications
- Server Settings

Status

A warning message displays indicating that the change in SSO settings causes Tomcat restart.

The following error messages may display when enabling the SSO application:

- Invalid Open Access Manager (Open AM) server URL - This error message displays when you give and invalid OpenAM server URL.
- Invalid profile credentials - This error message displays when you give a wrong profile name or wrong profile password or both.
- Security trust error - This error message displays when the OpenAM certificate has not been imported.

If you get any of the above error messages while enabling SSO, then the status changes to the above errors.

Select Applications

You can select or deselect the application for enabling or disabling SSO for a specific application.

The following applications are available:

- Cisco Unified Communications Manager Administration - Enables SSO for Cisco Unified Communications Manager Administration, Cisco Unified Serviceability, and Cisco Unified Reporting
- Cisco Unified Communications Self Care Portal - Enables SSO for Cisco Unified Communications Self Care Portal
- Cisco Unified Operating System Administration - Enables SSO for Cisco Unified Operating System Administration and Disaster Recovery System
- Cisco Unified Data Service - Enables SSO for Cisco UC Integration for Microsoft Office Communicator
- RTMT - Enables the web application for Real-Time Monitoring Tool

Server Settings

The server settings are editable only when SSO is disabled for all applications.

Use the following procedure:

Procedure

Step 1 Enter the following URL of the Open Access Manager (OpenAM) server:

http://opensso.sample.com:443/opensso

Step 2 Enter the relative path where the policy agent should be deployed. The relative path must be alphanumeric.

Step 3 Enter the name of the profile that is configured for this policy agent.

Step 4 Enter the password of the profile name.

Step 5 Enter the login Module instance name that is configured for Windows Desktop SSO.

Step 6 Click **Save.**

Step 7 Click **OK** on the confirmation dialog box to restart Tomcat.

CLI Commands for Single Sign-On

This section describes the CLI commands for single sign-on.

- utils sso enable
- utils sso disable
- utils sso status

utils sso enable

This command is not supported in Release 10.0(1). If you execute this command, the system prompts you to enable SSO using the GUI.

utils sso disable

This command disables SSO based authentication. This command lists the web applications for which SSO is enabled. Enter Yes when prompted to disable single sign-on for the specified application.

Command Syntax

utils sso disable

Usage Guidelines

Caution Disabling single sign-on restarts the Cisco Unified Communications Manager web server (Tomcat).

Note If OpenAM is not accessible, then Tomcat takes more time to appear. This is due to a Servm limitation. In this scenario, the approximate time for Tomcat to appear is 10 minutes.

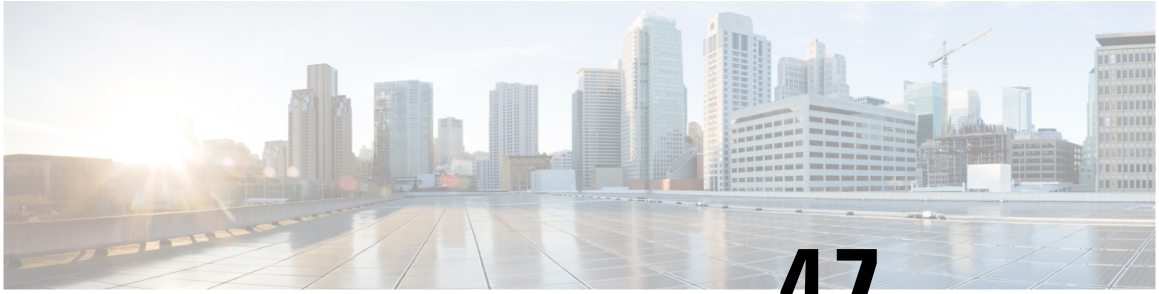
You must run this command on all nodes in a cluster.

utils sso status

This command displays the status and configuration parameters of single sign-on.

Command Syntax

utils sso status



CHAPTER 47

SAML Single Sign-On

This chapter provides information about the Security Assertion Markup Language (SAML) Single Sign-On feature, which allows administrative users to access certain Cisco Unified Communications Manager and IM and Presence Service applications without logging in again.

After you enable SAML Single Sign-On (SSO), users will be able to access the following web applications without logging in again:

- Cisco Unified Communications Manager Administration
- Cisco Unified Reporting
- Cisco Unified Serviceability
- Cisco Unified CM IM and Presence Administration
- Cisco Unified IM and Presence Serviceability
- Cisco Unified IM and Presence Reporting

Note Only LDAP-synchronized users can access SAML SSO-enabled web applications. Local end users and applications users cannot access them.

System Requirements for SAML SSO

The SAML Single Sign-On feature requires the following software components:

- Cisco Unified Communications Manager Release 10.0(1) or later.

Note Ensure that DNS is configured for the Cisco Unified Communications Manager cluster.

- IM and Presence Service Release 10.0(1) or later
- An Identity Provider (IdP) Server.
- An LDAP server that is trusted by the IdP server and supported by Cisco Unified Communications Manager.

The following IdPs using SAML 2.0 are supported:

- Microsoft Active Directory Federation Services (ADFS)
- Oracle Identity Manager
- Ping Federate
- Open Access Manager (OpenAM)

The third-party applications must meet the following configuration requirements:

- The mandatory attribute "uid" must be configured on the IdP. This attribute must match the attribute that is used for the LDAP-synchronized user ID in Cisco Unified Communications Manager.

  Note Cisco Unified Communications Manager currently supports only sAMAccountName option as the LDAP attribute for user ID settings.

  For information about configuring mandatory attribute mapping, see the IdP product documentation.

- The clocks of all the entities participating in SAML SSO must be synchronized. For information about synchronizing clocks, see the "NTP Settings" section in the *Cisco Unified Communications Operating System Administration Guide*.

Install SAML SSO

After you install Cisco Unified Communications Manager 10.0(1) and IM and Presence Service 10.0(1), you can use the SAML Single Sign-On feature if you perform the necessary configuration tasks. For information about configuration tasks that you must perform, see Enable SAML SSO, on page 1075.

SAML SSO Settings

In Cisco Unified Communications Manager Administration, use the **System** > **SAML Single Sign-On** menu path to configure SAML SSO. The table below describes the settings that are displayed on the **SAML Single Sign-On** window.

Note If you log in to Cisco Unified Communications Manager Administration as an end user without administrative privileges and attempt to access the **SAML Single Sign-On** window, a 403 error is displayed. After that, if you log in as an end user with administrative privileges in the same browser window, a 403 error is still displayed. In such a case, you must clear the browser cache and try logging in again.

Setting	Description
Server Name	Specifies the names of all the servers in the cluster.
SSO Status	Displays one of the following statuses: **SAML** Indicates that the SAML SSO is enabled on the server. **Disabled** Indicates that SAML SSO is disabled on the server. **OpenAM** Indicates that OpenAM SSO is enabled on the server. Cisco Unified Communications Manager: **Cisco Unified OS Administration** > **Security** > **Single Sign On** IM and Presence Service: **Cisco Unified IM and Presence OS Administration** > **Security** > **Single Sign On**
Re-import Metadata	Click the **Re-import Metadata** icon to import IdP metadata file from the publisher to the subscribers. **Note** This option is displayed as N/A (Not Applicable) for the publisher node.
Last Metadata Import	Specifies the time when the IdP metadata was last imported on the server. This field displays “Never” if you are running the SAML SSO setup for the first time.

Setting	Description
Export Metadata	Click the **Export Metadata** icon to download the server metadata file. A SAML metadata file must be generated for the specified server, and downloaded using the browser. You must then import this metadata file to the IdP server. **Important** If you change the hostname or domain of a node, ensure that you download the metadata from that node and upload the file to the IdP server again. For more information, see Update Server Metadata After Domain or Hostname Change, on page 1078. The **Export All Metadata** button is enabled by default, regardless of whether the SAML SSO state set to active.
Last Metadata Export	Specifies the time when the SAML metadata file of the specified server was last exported. This field displays “Never” if you are running the SAML SSO setup for the first time.
SSO Test	Displays the test results of the SAML configuration with the IdP. The test ensures that the specified server trusts the IdP, and that the IdP trusts the specified server. The trust relationship between the server and the IdP depends on the success of exporting and importing of SAML metadata files. Displays one of the following values: **Never** Indicates that a test has not been performed on this server. **Passed** Indicates that a test has been successfully run on this server, and that the server and the IdP trust one another. **Failed** Indicates that a test was attempted on the specified server, but that either the server does not trust the IdP, or the IdP does not trust the server, or some other network or IdP issue prevented the test from passing.

Setting	Description
Run Test	Click **Run Test** to run the SSO test. You must run this test before enabling SAML SSO. The SAML SSO setup cannot be completed until this test is successful. To run this test, there must be at least one LDAP synchronized user with administrator rights. You must also know the password for that user ID. **Note** You cannot run this test until the IdP metadata file is imported to the server, and the server metadata file is exported to the IdP server. **Note** If you are using OpenAM as the IdP, you must log out of the IdP before running this test.
Enable SAML SSO	Click **Enable SAML SSO** to start the SAML SSO configuration.
Update IdP Metadata File	Click **Update IdP Metadata File** to update IdP metadata on all the servers in the cluster.
Export All Metadata	Click **Export All Metadata** to export the SAML metadata files from each server. These files are converted to a compressed file (.zip) for easy download. You must extract the file and then import each file to the IdP.
Fix All Disabled Servers	Click **Fix All Disabled Servers** to enable SAML SSO on the servers on which it is disabled.
View IdP Trust Metadata File	Click **View IdP Trust Metadata File** to download a copy of the IdP metadata file.

Enable SAML SSO

Note The Cisco CallManager Admin, Cisco Unified CM IM and Presence Administration, Cisco CallManager Serviceability, and Cisco Unified IM and Presence Serviceability services are restarted after enabling or disabling SAML SSO.

Perform the following steps to enable SAML SSO:

Before you begin

Ensure that the following prerequisites are met before proceeding with the steps:

- The end-user data is synchronized to the Cisco Unified Communications Manager database.

- Verify that the Cisco Unified CM IM and Presence Cisco Sync Agent service has completed data synchronization successfully. Check the status of this test by choosing **Cisco Unified CM IM and Presence Administration** > **Diagnostics** > **System Troubleshooter**. The “Verify Sync Agent has sync'ed over relevant data (e.g. devices, users, licensing information)” test indicates a "Test Passed" outcome if data synchronization has completed successfully.
- At least one LDAP synchronized user is added to the Standard CCM Super Users group to enable access to Cisco Unified Administration.

Note For more information about synchronizing end-user data and adding LDAP-synchronized users to a group, see the "System setup" and "End user setup" sections in the *Cisco Unified Communications Manager Administration Guide*.

- OpenAM SSO (**Cisco Unified OS Administration** > **Security** > **Single Sign On** or **Cisco Unified IM and Presence OS Administration** > **Security** > **Single Sign On**) is disabled on all the nodes.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, click **System** > **SAML Single Sign-On**.

Step 2 Click **Enable SAML SSO**.

A warning message is displayed to notify you that all server connections will be restarted.

Step 3 Click **Continue**.

A dialog box that allows you to import IdP metadata displays. To configure the trust relationship between the IdP and your servers, you must obtain the trust metadata file from your IdP and import it to all your servers.

Step 4 Click **Browse** to locate and upload the IdP metadata file.

Step 5 Click **Import IdP Metadata**.

Step 6 Click **Next**.

Note The **Next** button is enabled only if the IdP metadata file is successfully imported on at least one node in the cluster.

A new status message is added in the **SAML Single Sign-On Configuration** window. It provides optional information to either skip or continue further with steps to upload the server metadata to the IdP.

Step 7 Click **Download Trust Metadata Fileset** to download server metadata to your system.

Step 8 Upload the server metadata on the IdP server.

After you install the server metadata on the IdP server, you must run an SSO test to ensure that the metadata files are correctly configured.

Step 9 Click **Next** to continue.

Step 10 Select an LDAP-synced user with administrator rights from the list of valid administrator IDs.

Step 11 Click **Run Test**.

The IdP login window displays.

Note You cannot enable SAML SSO until the Run Test succeeds.

Step 12 Enter a valid username and password.

After successful authentication, the following message is displayed:

```
SSO Test Succeeded
```

Close the browser window after you see this message.

If the authentication fails or takes more than 60 seconds to authenticate, a "Login Failed" message is displayed on the IdP login window. The following message is displayed on the SAML Single Sign-On window:

```
SSO Metadata Test Timed Out
```

To attempt logging in to the IdP again, repeat Steps 11 and 12.

Step 13 Click **Finish** to complete the SAML SSO setup.

SAML SSO is enabled and all the web applications participating in SAML SSO are restarted. It may take one to two minutes for the web applications to restart.

Enable SAML SSO on Cisco Web Dialer after an Upgrade

If Cisco Web Dialer is activated before SAML SSO is enabled, after an upgrade, SAML SSO is not enabled on Cisco Web Dialer by default. Follow this procedure to enable SAML Single Sign-On (SSO) on Cisco Web Dialer after an upgrade.

Procedure

Step 1 Deactivate the Cisco Web Dialer web service if it is already activated.

Step 2 Disable SAML SSO if it is already enabled.

Step 3 Activate the Cisco Web Dialer web service.

Step 4 Enable SAML SSO.

Recovery URL

The recovery URL allows you to bypass SAML Single Sign-On and log in to the Cisco Unified Communications Manager Administration and Cisco Unified CM IM and Presence interfaces for troubleshooting. For example, enable the recovery URL before you change the domain or hostname of a server. Logging in to the recovery URL facilitates an update of the server metadata. The recovery URL is https://hostname:8443/ssosp/local/login.

Note You can also access the recovery URL from the home page of the Cisco Unified Communications Manager and IM and Presence Service nodes, that is, the web page that displays when you enter the hostname or IP address of the server into the web browser.

Note Only application users with administrative privileges can access the recovery URL.

If SAML SSO is enabled, the recovery URL is enabled by default. You can enable and disable the recovery URL from the CLI. For more information about the CLI commands to enable and disable the recovery URL, see *Command Line Interface Guide for Cisco Unified Communications Solutions, Release 10.0(1)*.

Update Server Metadata After Domain or Hostname Change

Use the following procedure to update server metadata after you change domain or hostname of a server.

Caution SAML SSO will not be functional after domain or hostname change until you perform this procedure.

Note If you are unable to log in to SAML Single Sign-On window even after performing this procedure, clear the browser cache and try logging in again.

Procedure

Step 1 In the address bar of the web browser, enter the following URL:

```
https://<Unified CM-server-name>
```

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

Step 2 Select **Recovery URL to bypass Single Sign-On (SSO)** from the main window that displays.

The **Cisco Single Sign-On Recovery Administration** window is displayed.

Note If the recovery URL is disabled, you will not see the Recovery URL to bypass Single Sign-On link. To enable the recovery URL, log into the CLI and execute the following command: **utils sso recovery-url enable**.

Step 3 Enter the credentials of an application user with administrator role and click **Login**.

The Cisco Unified CM Administration window is displayed.

Step 4 From Cisco Unified CM Administration, choose **System** > **SAML Single Sign-On**.

Step 5 Click **Export Metadata** to download the server metadata.

Step 6 Upload the server metadata file to the IdP.

Step 7 Click **Run Test**.

The IdP login window displays.

Note You cannot enable SAML SSO until the Run Test succeeds.

Step 8 Enter a valid User ID and password.

After successful authentication, the following message is displayed:

```
SSO Test Succeeded
```

Close the browser window after you see this message.

If the authentication fails or takes more than 60 seconds to authenticate, a "Login Failed" message is displayed on the IdP login screen. The following message is displayed on the SAML Single Sign-On window:

```
SSO Metadata Test Timed Out
```

To attempt logging in to the IdP again, repeat Steps 7 and 8.

Manual Provisioning of Server Metadata

If you want to provision a single connection in your Identity Provider for multiple UC applications, you must manually provision the server metadata while configuring the Circle of Trust between the Identity Provider and the Service Provider. For information about configuring the Circle of Trust, refer the IdP product documentation.

To provision the server metadata manually, you must use the Assertion Customer Service (ACS) URL.

Sample ACS URL

```
<md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://cucm.ucsso.cisco.com:8443/ssosp/saml/SSO/alias/cucm.ucsso.cisco.com"
index="0"/>
```

General URL syntax

```
https://<SP FQDN>:8443/ssosp/saml/SSO/alias/<SP FQDN>
```

CLI Commands for SAML SSO

This section lists the CLI commands for SAML Single Sign-On.

- utils sso enable
- utils sso disable
- utils sso status
- utils sso recovery-url enable
- utils sso recovery-url disable
- show samltrace level

- set samltrace level

For more information about the CLI commands, see the *Command Line Interface Guide for Cisco Unified Communications Solutions, Release 10.0(1)*.

CHAPTER 48

URI Dialing

Cisco Unified Communications Manager supports dialing using directory URIs for call addressing. Directory URIs look like email addresses and follow the username@host format where the host portion is an IPv4 address or a fully qualified domain name. A directory URI is a uniform resource identifier, a string of characters that can be used to identify a directory number. If that directory number is assigned to a phone, Cisco Unified Communications Manager can route calls to that phone using the directory URI. URI dialing is available for SIP and SCCP endpoints that support directory URIs.

This chapter contains the following topics:

Set Up URI Dialing

The following steps describe how to set up URI dialing in your network:

Before you begin

If you want to configure URI dialing between clusters, you must set up an ILS network and enable Global Dial Plan Replication in the ILS network . See topics related to setting up the ILS network and the Global Dial Plan replication for details.

Procedure

Step 1 Assign directory URIs to the users in your network.

Step 2 Associate the directory URIs to directory numbers by assigning both a primary extension and phone to the users in your network.

Step 3 If you want to configure PSTN failover numbers for intercluster URI dialing, set up PSTN failover numbers for the directory URIs in your ILS network by doing the following:

a) In Directory Number Configuration, assign an enterprise alternate number or +E.164 alternate number to the same directory number on which the directory URI associates.
b) In the PSTN failover drop-down list box, choose the alternate number as the PSTN failover.

Step 4 Assign the default directory URI partition to an existing partition that is located in a calling search space by doing the following:

a) In Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**
b) For the Directory URI Alias Partition enterprise parameter, choose an existing partition that is in an existing calling search space.
c) Set the **URI Dialing Display Preference** service parameter for URI dialing as **URI** for calling display in call park display URI of the calling party. **DN** is the default setting for the service parameter.

Step 5 Configure the SIP profiles in your network by configuring the following fields in the SIP Profile Configuration window:

- Configure a setting for the Dial String Interpretation drop-down list box and apply the setting for all the SIP profiles in your network.
- Check the **Use Fully Qualified Domain Name in SIP Requests** check box for all the SIP profiles in your network.

Note At this point, intracluster URI dialing is configured. The remaining steps are used to configure intercluster URI dialing.

Step 6 For all the SIP trunks in your network, configure whether the network uses blended addressing by configuring the Calling and Connected Party Info Format drop-down list box in the Trunk Configuration window.

Step 7 Configure the case setting for the user portion of your directory URIs by setting the URI Lookup Policy enterprise parameter.

Step 8 Enable ILS support for Global Dial Plan Replication of directory URIs by doing the following:

a) In Cisco Unified CM Administration, choose **Advanced Features** > **ILS Configuration**.
b) Check the **Exchange Global Dial Plan Replication with Remote Clusters** check box.
c) In the Advertised Route String text box, assign a route string for the local cluster and click **Save**.

Step 9 If your deployment uses digit transformations to transform calling party directory numbers, do the following:

a) Configure calling party transformation patterns and apply them to the Inbound Call Settings for the phone or device pool. This configuration is used to apply digit transformations for intercluster calls.
b) Configure calling party transformation patterns that remove the digit transformations from the previous step and apply them to the Outbound Call Settings for the phone or device pool. This configuration removes the digit transformations on calls that remain in the local cluster.

Step 10 Configure SIP route patterns to route intercluster directory URI calls:

a) Create SIP route patterns that match the ILS-learned route strings for the remote clusters in your ILS network.
b) Point those SIP route patterns to SIP trunks or route lists that route to the next hop clusters in your ILS network.

Step 11 Repeat the previous steps for all the clusters in your ILS network.

Step 12 If you want to place directory URI calls to a Cisco TelePresence Video Communications Server, or a third-party call control system, import directory URI catalogs from a CSV file for the other system into any hub cluster in the ILS network.

Related Topics

Directory URI and Directory Number Dial String Interpretation, on page 1085
Set Up Global Dial Plan Replication, on page 597
Set Up ILS Network, on page 675
Set Up PSTN Failover for Directory URIs and Alternate Numbers, on page 605
Set Up Digit Transformations for URI Dialing, on page 1090

Directory URI Format

Directory URIs are alphanumeric strings consisting of a user and a host address separated by the @ symbol. Cisco Unified Communications Manager supports the following formats for directory URIs:

- user@domain (for example, joe@cisco.com)
- user@ip_address (for example, joe@10.10.10.1)

Cisco Unified Communications Manager supports the following formats in the user portion of a directory URI (the portion before the @ symbol):

- Accepted characters are a-z, A-Z, 0-9, !, $, %, &, *, _, +, ~, -, =, \, ?, \, ‘, ,, ., /.
- The user portion has a maximum length of 47 characters.
- The user portion accepts percent encoding from %2[0-9A-F] through %7[0-9A-F]. For some accepted characters, Unified CM automatically applies percent encoding. See below for more information on percent encoding.
- The user portion is case-sensitive or case-insensitive depending on the value of the URI Lookup Policy enterprise parameter. The default value is case-sensitive.

Cisco Unified Communications Manager supports the following formats in the host portion of a directory URI (the portion after the @ symbol):

- Supports IPv4 addresses or fully qualified domain names.
- Accepted characters are a-z, A-Z ,0-9, hyphens, and dots.
- The host portion cannot start or end with a hyphen.
- The host portion cannot have two dots in a row.
- Minimum of two characters.
- The host portion is not case sensitive.

Due to database restrictions, the Directory URI field has a maximum length of 254 characters.

Note You can also enter a directory number in the user portion of a directory URI. However, Cisco Unified Communications Manager may treat the directory URI as a directory number depending on which Dial String Interpretation option you choose for the SIP Profile.

Note For compatibility with third party call control systems, Cisco recommends setting the value of the URI Lookup Policy enterprise parameter to case insensitive.

Percent Encoding of Directory URIs

In the user portion of a directory URI, Unified CM automatically applies percent encoding to the following characters when the directory URI is saved in the database:

% ^ ` { } | \ : ” < > [ ] \ ‘ and spaces

When percent encoding is applied, the digit length of the directory URI increases. For example, if you input joe smith#@cisco.com (20 characters) as a directory URI, Cisco Unified Communications Manager stores the directory URI in the database as joe%20smith%23@cisco.com (24 characters). Due to database restrictions, Cisco Unified Communications Manager rejects any attempt to save a directory URI of greater than 254 characters.

Directory URI Format Exception for Bulk Administration

Within Cisco Unified CM Administration, you can enter directory URIs with embedded double quotes or commas. However, when you use Bulk Administration to import a CSV file that contains directory URIs with embedded double quotes and commas, you must use enclose the entire directory URI in double quotes and escape the embedded double quotes with a double quote. For example, the Jared, "Jerry",Smith@test.com directory URI must be input as "Jared,""Jerry"",Smith@test.com" in the CSV file.

Directory URI Provisioning

In Cisco Unified CM Administration, you can assign directory URIs in the local cluster in the following ways:

- End User Configuration—In End User Configuration, you can create end users and assign a phone, primary extension, and directory URI to that end user. Alternatively, If you synchronize your corporate LDAP directory with Cisco Unified Communications Manager, the LDAP data automatically populates for your end users. If the users in your LDAP directory have a phone, primary extension, and directory URI, they will automatically have directory URIs in Cisco Unified Communications Manager End User Configuration after the LDAP synchronization.
- Directory Number Configuration—In Directory Number Configuration, you can configure a directory number and associate a directory URI to that directory number. If that directory number is assigned to a phone, Cisco Unified Communications Manager allows you to dial that phone using the directory URI.

For both end user configuration and directory number configuration, you can also use Bulk Administration to import end users, directory URIs, directory numbers, and phones into Cisco Unified Communications Manager by bulk. See the *Cisco Unified Communications Manager Bulk Administration Guide* for more information.

For intracluster URI dialing, you must assign your directory URIs to a partition and calling search space. See Set Up URI Dialing, on page 1081 for more information.

For intercluster URI dialing, Cisco Unified Communications Manager uses the Intercluster Lookup Service (ILS) to replicate directory URIs to other clusters in the ILS network. If ILS is configured to support Global Dial Plan Replication, each cluster advertises its catalog of known directory URIs to the other clusters in the ILS network. See Global Dial Plan Replication, on page 597 for more information.

Directory URI and Directory Number Dial String Interpretation

Each phone that registers with Cisco Unified Communications Manager registers to its directory number. If a directory URI is associated with that directory number, users can dial that phone using the directory number or the directory URI—either will reach the same destination. However, because directory numbers and directory URIs are saved in different lookup tables in the database, Cisco Unified Communications Manager must be able to determine which dialing format is used, or it will not be able to route the call.

The Dial String Interpretation field that appears in the SIP Profile Configuration window allows you to set the rules that Cisco Unified Communications Manager uses to examine the user portion of a dial string and determine whether to route the call as a directory URI or a directory number. Because directory URIs can use both alpha and numeric characters, many dial strings are arbitrary and could be configured as either a directory URI or directory number. For example, you can configure Cisco Unified Communications Manager to route a dial string of 1234ABCD@10.10.10.1 as a directory number or as a directory URI. To ensure that calls are not dropped, you must configure a consistent policy for your network.

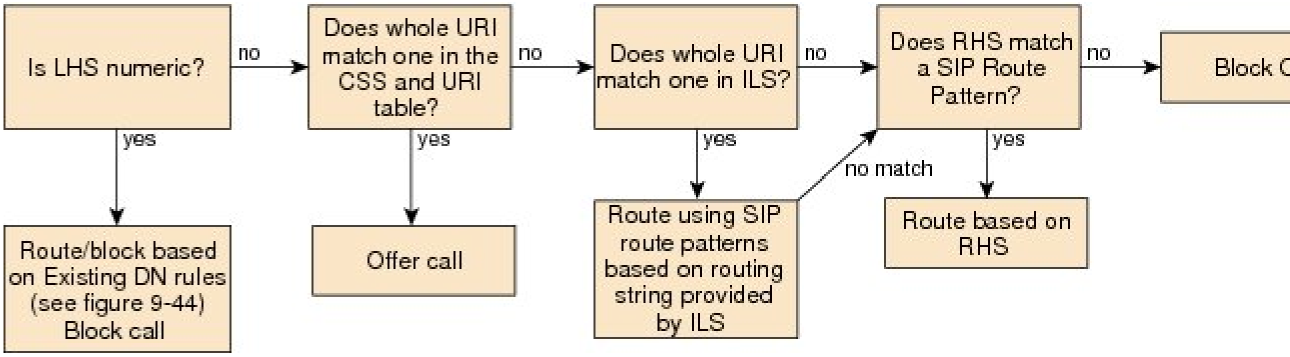
For more information on the Dial String Interpretation field, see topics related to SIP profile settings in the *Cisco Unified Communications Manager Administration Guide*.

Directory URI Call Routing

Cisco Unified Communications Manager uses the following logic to route calls that are placed to a directory URI:

- Cisco Unified Communications Manager checks if the dial string is numeric according to the Dial String Interpretation policy. If the dial string is numeric, Cisco Unified Communications Managerroutes the call as a directory number.
- Else, Cisco Unified Communications Manager checks local calling search spaces and the local directory URI lookup table to see if the directory URI is in the local cluster. If the directory URI is on cluster, Cisco Unified Communications Manager routes the call to the appropriate endpoint.
- Else, Cisco Unified Communications Manager checks if the directory URI exists in a learned or imported catalog. If the directory URI is in a URI catalog,Cisco Unified Communications Manager tries to match the route string for the catalog to a SIP route pattern. If a matching SIP route pattern is found, Cisco Unified Communications Manager routes the call to the trunk that is associated with that route pattern.
- Else, if a matching SIP route pattern was found, and the route fails, Cisco Unified Communications Manager checks if a PSTN failover exists for the directory URI. If a PSTN failover exists,Cisco Unified Communications Manager uses the calling party's AAR CSS to route the call to the PSTN failover number.

- Else, Cisco Unified Communications Manager tries to match the host portion of the directory URI to a SIP route pattern. If the host portion matches a SIP route pattern, Cisco Unified Communications Manager routes the call to the SIP trunk that is associated to that route pattern.
- Else, Cisco Unified Communications Manager blocks the call.


Is LHS numeric?
no
yes
Route/block based on Existing DN rules (see figure 9-44) Block call
Does whole URI match one in the CSS and URI table?
no
yes
Offer call
Does whole URI match one in ILS?
no
yes
Route using SIP route patterns based on routing string provided by ILS
no match
Does RHS match a SIP Route Pattern?
no
yes
Route based on RHS
Block C

Intercluster URI Dialing

Cisco Unified Communications Manager provides support for intercluster URI dialing through ILS and Global Dial Plan Replication.

When Global Dial Plan Replication is enabled in an ILS network, each cluster in the ILS network advertises its global dial plan data, which includes directory URIs, route strings, and PSTN failover numbers to the rest of the ILS network. As a result of Global Dial Plan Replication, each cluster in the ILS network learns the directory URIs that are known by all the other clusters in the ILS network, the route string for the directory URI home cluster, and any PSTN failover numbers.

Cisco Unified Communications Manager routes intercluster directory URI calls by matching the route string that is associated to the dialed directory URI to a SIP route pattern. As a fallback, if Cisco Unified Communications Manager is unable to route the call over a SIP trunk, Cisco Unified Communications Manager can reroute the call to the called party's associated PSTN failover number.

Directory URI Types

Within an individual cluster, directory URIs can be categorized as follows:

- Local directory URIs—Directory URIs that are configured in the local cluster. By default, ILS advertises all local directory URIs to the ILS network. However, you can exclude a local directory URI from being advertised to the ILS network by unchecking the Advertise Globally via ILS check box for that directory URI in the Directory Number Configuration window.
- Learned directory URIs—Directory URIs that were configured in a remote cluster and learned by this cluster.
- Imported Directory URIs—Third-party directory URIs that were manually imported into this cluster.

Route Strings

In most cases, the host portion of a directory URI is not granular enough for Cisco Unified Communications Manager to locate the home cluster on which the directory URI is configured. Cisco Unified Communications

Manager uses route strings in combination with a SIP route pattern in order to route directory URI calls across clusters.

When you configure Global Dial Plan Replication, you must assign a distinct route string for each cluster in the ILS network. Cisco Unified Communications Manager associates all local directory URIs in a given cluster to the advertised route string for that cluster and ILS advertises those directory URIs, and their associated route string, to the rest of the ILS network.

When a user dials a learned directory URI that is registered to a remote cluster, Cisco Unified Communications Manager pulls the route string that is associated to that directory URI, matches that route string to a SIP route pattern, and routes the call to the outbound trunk that is specified by the SIP route pattern. In order for Cisco Unified Communications Manager to route calls to a route string, you must configure SIP route patterns that route the destination route strings to the next-hop clusters in your ILS network.

For more detailed information on route strings, see Route Strings, on page 605.

PSTN Failover for Directory URIs

Global Dial Plan Replication allows you to configure a PSTN failover for directory URIs and replicate that PSTN failover to remote clusters. If a remote cluster is unable to route an intercluster call over a SIP trunk to a learned directory URI, Cisco Unified Communications Manager can use the calling party's AAR CSS to reroute the call to the PSTN failover number.

You can configure PSTN failover information in the Directory Number Configuration window by creating an alternate number for the directory number and then assigning that alternate number as the PSTN failover. If Global Dial Plan Replication is enabled, ILS advertises that alternate number as the PSTN failover for each directory URI and alternate number that is associated to that directory number.

For details on how to set up a PSTN failover number for directory URIs, see Set Up PSTN Failover for Directory URIs and Alternate Numbers, on page 605.

PSTN failover example

Alice in New York has a primary extension of 2000, a directory URI of alice@cisco.com, and an +E.164 alternate number of +19725552000. Alice's +E.164 alternate number is assigned as the PSTN failover and Global Dial Plan Replication is enabled.

If Bob in Los Angeles dials alice@cisco.com from another cluster in the ILS network and the SIP trunk that connects the two clusters is down, Cisco Unified communications Manager uses Bob's AAR CSS to reroute the call to +19725552000 and sends the call to a PSTN gateway. Alice's extension in New York rings. Because the call was routed over a PSTN gateway, the final call is audio only.

Directory URI Interoperability with VCS or Third Party System

Cisco Unified Communications Manager gives users with a supported endpoint the ability to place calls to alphanumeric URIs such as johnsmith@acme.com. The simplest way to route directory URI calls from a supported endpoint on Cisco Unified Communications Manager to an endpoint on a Cisco TelePresence Video Communications Server (VCS) or a third party call control system is to configure a domain-based SIP route pattern. For example, you can configure a SIP route pattern of acme.com to route calls addressed to the acme.com domain out a SIP trunk that is configured for the Cisco TelePresence VCS or a third party call control system.

In situations where you have more than one Cisco TelePresence VCS or third party call control systems that use the same domain name, Cisco Unified Communications Manager can use the Intercluster Lookup Service

(ILS) to provide URI dialing interoperability. For each Cisco TelePresence VCS, or third party system, you must manually create a csv file with the directory URIs that are registered to that call control system.

On a Cisco Unified Communications Manager cluster that is set up as a hub cluster in an ILS network, you can create an Imported directory URI catalog for each Cisco TelePresence VCS, or third party system, and assign a unique route string for each catalog. After you import the csv files into their corresponding Imported directory URI catalog, ILS replicates the imported directory URI catalog and route string to the other clusters in the ILS network.

On each Cisco Unified Communications Manager cluster, configure SIP Route Patterns that match the route string assigned to each Imported directory URI catalog in order to allow Cisco Unified Communications Manager to route directory URIs to an outbound trunk that is destined for the Cisco TelePresence VCS or third party system.

For more information on how to import directory URIs from a VCS into Cisco Unified Communications Manager, see the "Import directory URIs from a non-ILS system" procedure in the Global Dial Plan Replication chapter of the *Cisco Unified Communications Manager Features and Services Guide*.

Cisco Unified Communications Manager also provides directory URI export functionality. You can export all directory URIs that were configured in the local cluster, including those that were imported from an LDAP directory, to a csv file that you can import into the other call control system. For more information on how to export directory URIs from Cisco Unified Communications Manager to a csv file, see the "Export Local Directory URIs to a CSV File" section in the Directory URIs chapter of the *Cisco Unified Communications Manager Bulk Administration Guide*.

Directory URI LDAP Integration

Cisco Unified Communications Manager supports synchronization of directory URI fields in Cisco Unified CM Administration with data from a corporate LDAP directory.

When you synchronize with an LDAP directory, Cisco Unified Communications Manager automatically assigns the directory URI value that you choose from the LDAP directory as the primary directory URI for that end user. Even if you have already configured a directory URI as the primary directory URI for that end user's primary extension, the LDAP value overrides the value that is configured in Cisco Unified CM Administration

Note Under the default setting, the user portion of a directory URI is case-sensitive and whatever case the directory URI has in the LDAP directory is the case in Cisco Unified Communications Manager. For example, if the directory URI value in LDAP is JOE@cisco.com, calls to joe@cisco.com will fail. You can change this setting by changing the value of the URI Lookup Policy enterprise parameter to case-insensitive.

Note For compatibility with third party call control systems, Cisco recommends that you set the value of the URI Lookup Policy enterprise parameter to case-insensitive.

Note For Cisco Unified Communications Manager systems where LDAP synchronization was configured prior to Release 9.0, the directory URI field is not automatically enabled for synchronization. You must create a new LDAP synchronization agreement.

Directory URI and Directory Number Blended Address

Cisco Unified Communications Manager supports blended addressing of directory URIs and directory numbers. When blended addressing is enabled across the network, Cisco Unified Communications Manager inserts both the directory URI and the directory number of the sending party in outgoing SIP Invites, or responses to SIP Invites. The destination endpoint has the option of using either the directory URI or the directory number for its response—both will reach the same destination.

Cisco Unified Communications Manager uses the x-cisco-number tag in the SIP identity headers to communicate a blended address. When both a directory URI and directory number are available for the sending phone and blended addressing is enabled, Cisco Unified Communications Manager uses the directory URI in the From fields of the SIP message and adds the x-cisco-number tag with the accompanying directory number to the SIP identity headers. The x-cisco-number tag identifies the directory number that is associated with the directory URI.

For Cisco Unified Communications Manager to deliver a SIP message with blended addressing, the following conditions must be true:

- For all SIP trunks between the phones, the Calling and Connected Party Info Format drop-down list box must be set to **Deliver URI and DN in connected party**.
- Both a directory URI and a directory number must be configured for the phone that is sending the SIP message.
- The destination endpoint must support blended addressing.

For SIP trunks, blended addressing is enabled in the Trunk Configuration window of Cisco Unified CM Administration by setting the Calling and Connected Party Info Format drop-down list box to **Deliver URI and DN in connected party**. When Cisco Unified Communications Manager receives a SIP message with a blended address that is to be forwarded out a trunk, Cisco Unified Communications Manager checks whether blended addressing is enabled on the trunk before forwarding the message. If blended addressing is not enabled on the trunk, Cisco Unified Communications Manager removes the x-cisco-number tag before forwarding the SIP message.

For SIP lines, blended addressing is enabled by default. However, if a SIP message with a blended address is being forwarded out a SIP line to the destination endpoint, Cisco Unified Communications Manager checks whether the endpoint supports blended addressing. If the destination endpoint does not support blended addressing, Cisco Unified Communications Manager removes the x-cisco-number tag before forwarding the SIP message to the endpoint.

Blended addressing can be applied to the RPID, PAI, PPI, and Diversion headers.

Example 1

Bob at Cisco makes a call from extension 2100. The Calling and Connected Party Info Format field in the Trunk Configuration window is set to **Deliver DN only in connected party**. Blended addressing is not applied and the x-cisco-number tag is not added to the outgoing SIP message.

```
From:<sip:2100@10.10.10.1>
Remote-Party-ID:<sip:2100@10.10.10.1>;party=calling
```

Example 2

Jill at Cisco makes a call from extension 2030. The Calling and Connected Party Info Format field in the Trunk Configuration window is set to **Deliver URI only in connected party**. Blended addressing is not applied and the x-cisco-number tag is not added to the outgoing SIP message.

```
From:<sip:jill@cisco.com>
Remote-Party-ID:<sip:jill@cisco.com>;party=calling
```

Example 3

Alice at Cisco makes a call from extension 2000. The Calling and Connected Party Info Format field in the Trunk Configuration window is set to **Deliver DN and URI in connected party**. Blended addressing is applied. Cisco Unified Communications Manager adds the x-cisco-number tag to the SIP identity header.

```
From:<sip:alice@cisco.com>
Remote-Party-ID:<sip:alice@cisco.com;x-cisco-number=2000>;party=calling
```

John at Cisco extension 4003 receives Alice’s call, but John has his office phone set to forward calls to his home phone. If blended addressing is enabled, Cisco Unified Communications Manager adds a Diversion header with the x-cisco-number tag, and forwards the SIP INVITE to John’s home phone.

```
From:<sip:alice@cisco.com>
Diversion: <sip:john@cisco.com;x-cisco.number=4003>reason=no-answer
Remote-Party-ID:<sip:alice@cisco.com;x-cisco-number=2000>;party=calling
```

Set Up Digit Transformations for URI Dialing

If your network applies digit transformation patterns to calling party directory numbers and you are implementing URI dialing across clusters, you can apply calling party transformation patterns against the Inbound Call Settings of the phone or device pool. This is required because if the called number is a directory URI, Cisco Unified Communications Manager cannot perform calling party transformations where the transformation is applied based on the called directory number or pattern.

For intercluster calls, you can apply a digit transformation pattern against a Calling Search Space (CSS) and apply that CSS transformation to the Inbound Call Settings for the phone or device pool. Before routing the call, whether the dialed number is a directory URI or a directory number, Cisco Unified Communications Manager applies the transformation pattern to the calling directory number.

For intracluster calls, if you don’t want the calling party transformation to be applied for calls that remain in the local cluster, you can also apply a CSS transformation pattern that strips the digits that were added by the Inbound Call Settings and apply that pattern to the Outbound Call Settings for the phone or device pool. For the device pool, the Calling Party Transformation CSS for outbound calls appears under Device Mobility Related Information.

To apply calling party digit transformations when URI dialing is implemented, do the following:

Procedure

Step 1 In Cisco Unified CM Administration, chooseCall Routing > **Class of Control** > **Partition** and create a new partition (for example, Change Calling Party XXXX to 8XXXXXXX).

Step 2 Choose**Call Routing** > **Class of Control** > **Calling Search Space** and do the following:

- Create a calling search space (for example, Change Calling Party XXX to 8XXXXXXX).
- In the Available Partitions list box, add the newly created partition (for example, Change Calling Party XXXX to 8XXXXXXX).

Step 3 In Cisco Unified CM Administration, choose **Call Routing** > **Transformation** > **Transformation Pattern** > **Calling Party Transformation Pattern**.

- Create a transformation pattern (for example, XXXX)
- Set the partition to the partition that you created in the previous steps (for example Change Calling Party XXXX to 8XXXXXXX).
- Set the Calling Party Transformation Mask to the desired mask (for example, 8265XXXX).

Step 4 In Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **Partition** and create a new partition (for example, Change Calling Party 8XXXXXXX to XXXX).

Step 5 Choose**Call Routing** > **Class of Control** > **Calling Search Space** and do the following:

- Create a calling search space (for example, Change Calling Party 8XXXXXXX to XXXX).
- In the Available Partitions list box, add the newly created partition (for example, Change Calling Party 8XXXXXXX to XXXX).

Step 6 In Cisco Unified CM Administration, choose **Call Routing** > **Transformation** > **Transformation Pattern** > **Calling Party Transformation Pattern**.

- Create a transformation pattern (for example, 8265XXXX)
- Set the partition to the partition that you created in the previous steps (for example, Change Calling Party 8XXXXXXX to XXXX).
- Set the Calling Party Transformation Mask to the desired mask (for example, XXXX).

Step 7 To assign your transformation patterns to an individual phone, choose **Device** > **Phone** and apply the following settings to the phone:

- For patterns that apply to inbound settings, choose the CSS that contains the pattern from the Calling Party Transformation CSS drop-down list box that appears under Inbound Calls.
- For patterns that apply to outbound settings, choose the CSS that contains the pattern from the Calling Party Transformation CSS drop-down list box that appears under Outbound Calls.

Step 8 Click **Save**.

Note You can also apply the digit transformation patterns to a device pool by choosing**System** > **Device Pool** from Cisco Unified CM Administration. For device pool configuration, the Calling Party Transformation CSS for outbound calls appears under Device Mobility Related Information.

Directory URI Troubleshooting Tips

This section describes some basic troubleshooting scenarios for URI dialing.

Directory URI Has Been Dialed, but the Call Fails

Check the following:

- Check the setting of the URI Lookup Policy enterprise parameter. Make sure that the dialed directory URI and the provisioned directory URI use the same case setting for the user portion of the directory URI.
- Check the partition, directory URI partition, and calling search space of the called party. For intracluster calls, make sure the destination phone is in the same calling search space.
- Check the Dial String Interpretation policy against the dialed directory URI. If the implemented dial string interpretation policy interprets the directory URI as a directory number, Cisco Unified Communications Manager may not be able to route the call.
- For intercluster calls, check the local cluster for the directory URI and make sure the Advertise Globally via ILS check box is checked for that directory URI.
- Use the Dialed Number Analyzer tool to determine if Cisco Unified Communications Manager can route a call to that directory URI.

Note The Dialed Number Analyzer can only be used to test routing for intracluster calls.

Directory URI Has Been Dialed, but the Call Display Shows a Directory Number

Check the following:

- Check to see whether the phone model supports blended addressing. If the phone model does not support blended addressing, the directory number is displayed.
- Check to see whether the Alerting Name is configured. The Alerting Name overrides the dial string.
- If the incorrect display is on the called phone, check to see whether the calling phone has a primary directory URI configured.

CHAPTER 49

Web Dialer

This chapter provides information about Cisco Web Dialer, used in conjunction with Cisco Unified Communications Manager, which allows Cisco Unified IP Phone users to make calls from web and desktop applications.

Configure Cisco Web Dialer

Cisco Web Dialer, which is installed on a Cisco Unified Communications Manager server and used in conjunction with Cisco Unified Communications Manager, allows Cisco Unified IP Phone users to make calls from web and desktop applications. For example, Cisco Web Dialer 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.

Perform the following steps to configure Cisco Web Dialer.

Procedure

Step 1 Activate the Cisco Web Dialer service.

Step 2 Configure the Webdialer servlet.

Step 3 Configure Cisco Web Dialer as an application server in the Application Server window in Cisco Unified Communications Manager Administration.

Step 4 Add each user that you want to use Web Dialer to the Standard End User Group for Cisco Unified Communications Manager.

Step 5 Determine which language Web Dialer displays by setting the locale field in the Cisco Unified Communications Self Care Portal menu.

Step 6 (Optional) Configure the Redirector servlet.

Step 7 (Optional) Configure the application dial rules for multiple cluster applications.

Step 8 (Optional) Create a proxy user.

Step 9 (Optional) Configure Cisco Web Dialer trace settings.

Step 10 Configure Cisco Web Dialer alarms.

Related Topics

Web Dialer, on page 1093
Install and Activate Cisco Web Dialer, on page 1097
Set Service Parameters for the Web Dialer Servlet, on page 1098
Configure Cisco Web Dialer in the Application Server Window, on page 1099
Add Users to the Standard CUCM Users Group, on page 1102
Configure Web Dialer for the Local Language, on page 1101
Configure the Redirector Servlet, on page 1102
Configure Application Dial Rules, on page 1102
Create a Proxy User, on page 1103
Trace Settings, on page 1104

Cisco Web Dialer Feature

Cisco Web Dialer, which is installed on a Cisco Unified Communications Manager node and used in conjunction with Cisco Unified Communications Manager, allows Cisco Unified IP Phone users to make calls from web and desktop applications. For example, Cisco Web Dialer 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.

Cisco Web Dialer has two main components: Webdialer servlet and Redirector servlet.

Webdialer Servlet

The Webdialer servlet, a Java servlet, allows Cisco Unified Communications Manager users in a specific cluster to make and complete calls, as well as to access their phone and line configuration.

An application can interact with the Webdialer servlet through two interfaces:

- The SOAP over HTTPS interface - This interface that is based on the Simple Object Access Protocol (SOAP) gets used to develop desktop applications such as Microsoft Outlook Add-in and SameTime Client Plug-in. Developers can use the isClusterUserSoap interface to design multicluster applications that require functionality similar to a Redirector servlet.
- HTML over HTTPS interface - This interface that is based on the HTTPS gets used to develop web-based applications. Developers who use this interface can use the Redirector servlet for designing multicluster applications.

Redirector Servlet

The Redirector servlet, a Java-based Tomcat servlet, finds the Cisco Unified Communications Manager cluster for a request that a Cisco Web Dialer user makes. It redirects that request to the specific Cisco Web Dialer server that is located in that user Cisco Unified Communications Manager cluster. Availability of the Redirector servlet occurs only for multicluster applications and only for applications that are developed by using HTML over HTTPS interfaces.

Example of Cisco Web Dialer Using the Redirector Servlet

For example, consider three clusters, each one in a single city such as San Jose (SJ-CM), Dallas (D-CM), and New York (NY-CM). Each cluster contains three Cisco Unified Communications Manager servers with Webdialer servlets that have been configured for Cisco Unified Communications Manager servers SJ-CM1, D-CM2, and NY-CM3.

The system administrator configures the Webdialer servlets on any Cisco Unified Communications Manager server by entering the IP address of that specific Cisco Unified Communications Manager server in the List of Web Dialers service parameter (see the Set Service Parameters for the Web Dialer Servlet, on page 1098). For information on configuring the Webdialer servlet and the Redirector servlet, see the Configure the Webdialer Servlet, on page 1097 and the Configure the Redirector Servlet, on page 1102.

When a user who is located in San Jose clicks on a telephone number in the corporate directory search window that Cisco Web Dialer enables, the following actions happen:

1. The user application (client) sends an initial makeCall HTTPS request to the Redirector servlet.
2. If this request is received for the first time, the Redirector servlet reads the Cisco Web Dialer server cookie and finds it empty.

   For a repeat request, the Redirector servlet reads the IP address of the Cisco Web Dialer server that previously serviced the client and sends a isClusterUser HTTPS request only to that server.
3. The Redirector servlet sends a response that asks for information, which results in the authentication dialog box opening for the user.
4. The user enters the Cisco Unified Communications Manager user ID and password and clicks the Submit button.
5. The Redirector servlet reads only the user identification from this information and sends an isClusterUser HTTPS request to each Cisco Web Dialer server that the system administrator has configured.
6. The Redirector servlet redirects the original request from the user to SJ-CM1.

Redundancy

Because redundancy is important for applications that are running in a multicluster environment, this section describes one method to achieve that redundancy.

If a single Redirector servlet is supporting multiple Cisco Web Dialers in a multicluster environment, it provides a single point of failure. For example, in Configure Web Dialer for the Local Language, on page 1101, a Redirector servlet runs on the San Jose cluster and also services the New York and Dallas clusters. If this Redirector servlet fails to run on the San Jose cluster, the users who are serviced by all three clusters cannot use Cisco Web Dialer.

To avoid this single point of failure, configure Redirector servlets for each cluster. If the directory search window points to a URL such as https://sanjoseclustercompany.com:8443/webdialer/Redirector, change that URL to a virtual link such as https://webdialer-service.company.com/webdialer/Redirector. This virtual link points to a virtual machine that is using a Cisco DistributedDirector. All the Redirector servlets operate behind this virtual link.

For more information on installing and configuring Cisco DistributedDirector, see the suite of documents for Cisco DistributedDirector.

System Requirements for Cisco Web Dialer

Cisco Web Dialer requires the following software components:

- Cisco Unified Communications Manager 5.0(2) or later
- Cisco Unified IP Phones that CTI supports

To configure your company directory search window for Cisco Web Dialer or the Cisco Unified Communications Manager directory search window, you must

- Install and configure Cisco Unified Communications Manager.
- Configure Cisco Web Dialer.

You can launch Cisco Web Dialer from the Directory window, in Cisco Unified Communications Self Care Portal. For example, you could access a URL similar to the following one:

https://<IP address of Cisco Unified Communications Manager server>:8443/ccmuser/showhome.do.

Interactions and Restrictions

This section describes the interactions and restrictions for Cisco Web Dialer.

Interactions

The following interactions apply to Cisco Web Dialer:

- When using Client Matter Codes (CMC), the user must enter the proper code at the tone; otherwise, the IP phone disconnects, and the user receives reorder tone.
- When using Forced Authorization Codes (FAC), the user must enter the proper code at the tone; otherwise, the IP phone disconnects, and the user receives reorder tone.
- Cisco Web Dialer uses change notifications on the ApplicationDialRule database table to track and use the updated dial rules.

Restrictions

Cisco Web Dialer supports phones that run Skinny Client Control Protocol (SCCP) and Session Initiation Protocol (SIP) that Cisco Computer Telephony Integration (CTI) supports.

Note Cisco Web Dialer supports only the 7970/71 and 7961/41 IP phone models that run SIP.

Install and Activate Cisco Web Dialer

Cisco Web Dialer automatically installs on the server on which you installed Cisco Unified Communications Manager.

Perform the following procedure to activate Cisco Web Dialer on the Cisco Unified Communications Manager server.

Procedure

Step 1 From the navigation area of the Cisco Unified Communications Manager application, choose Cisco Unified Serviceability and click **Go.**

Step 2 Choose **Tools** > **Service Activation**.

Step 3 Choose the Cisco Unified Communications Manager server that is listed in the Servers drop-down list box.

Step 4 From CTI Services, check the check box next to Cisco Web Dialer Web Service.

Step 5 Click **Save.**

Note You must also activate and start the CTI Manager service for Cisco Web Dialer to function properly. To ensure that the CTI Manager service is started, from Cisco Unified Serviceability, choose **Tools** > **Control Center - Feature Services**.

Configure Cisco Web Dialer

This section provides information to configure Cisco Web Dialer.

Tip Before you configure Cisco Web Dialer, review the configuration summary task for Cisco Web Dialer.

Related Topics

Configure Cisco Web Dialer, on page 1093

Configure the Webdialer Servlet

To configure the Webdialer servlet

- Activate the Cisco Web Dialer service. See the Install and Activate Cisco Web Dialer, on page 1097.
- Set trace settings (optional). See the Trace Settings, on page 1104.
- Set the Cisco Web Dialer service parameters. See the Set Service Parameters for the Web Dialer Servlet, on page 1098.
- Configure application user.

Set Service Parameters for the Web Dialer Servlet

Cisco Unified Communications Manager provides the following service parameters for the Webdialer servlet:

- CAPF Profile Instance ID for Secure Connection to CTI Manager - This parameter specifies the Instance Id of the Application CAPF Profile for Application User WDSecureSysUser that this Cisco Web Dialer server will use to open a secure connection to CTI Manager.
- Primary Cisco CTIManager - Enter the IP address of the primary Cisco CTIManager.

  The default IP address of the Cisco CTI Manager specifies 127.0.0.1, which is the local host server that is used to set up Cisco Web Dialer.

  The maximum length specifies 15 digits.
- Backup Cisco CTIManager - Enter the IP address of the backup Cisco CTIManager. The maximum length specifies 15 digits. No IP address implies that no backup Cisco CTIManager exists.
- User Session Expiry (in hours) - Enter the duration, in hours, for which the user login session is valid.

  A default value of 0 indicates that the login session is valid for an indefinite time, until Cisco Web Dialer Web Service is restarted the next time.

  The minimum length specifies 0 hours, and the maximum length specifies 168 hours.
- Maximum Concurrent Call Requests - This parameter specifies the maximum number of concurrent WebDialer call requests that the WebDialer service can accept.

  For example:

  - –MCS 7825H2 supports a maximum of 2 calls per second. Cisco recommends setting the MaxConcurrentCallRequests (MCCR) value to 3 to allow callers to initiate and disconnect calls as needed.
  - MCS 7845H2 supports a maximum of 4 calls per second. Cisco recommends setting the MaxConcurrentCallRequests (MCCR) value to 8 to allow callers to initiate and disconnect calls as needed.

    Enter a lower value if RTMT alerts, alarms, or performance counters suggest the hardware associated with WebDialer is being overutilized (for example, spikes in CPU, entering Code Yellow). Enter a higher value to allow more simultaneous WebDialer call requests. Be aware that a higher value can add more load to the CPU.

    The maximum value specifies 8.

    The default value specifies 3.
- Duration of End Call Dialog (in seconds) - Enter the duration, in seconds, to display the dialog to end a call. This dialog indicates that the user must end the call if the user dialed out in error.

  The default value specifies 15 seconds, with a maximum value of 60 seconds and a minimum value of 10 seconds.

  To disable the Duration of End Call Dialog service parameter, the user checks the Disable Auto-Close check box in the Self Care Portal window. If the Disable Auto-Close check box is checked, the End Call dialog does not close automatically, and the Hangup button returns the user to the Make Call window.
- Apply Application Dial Rules on Dial - Default specifies True. If you do not need Cisco Web Dialer to use application dial rules, change the setting to False.

- CTI Manager Connection Security Flag - This clusterwide parameter indicates whether security for the Cisco Web Dialer service CTI Manager connection gets disabled or complies with the security mode of the cluster. If security is enabled, Cisco Web Dialer opens a secure connection to CTI Manager by using the Application CAPF profile that is configured in Application CAPF Profile Instance Id for Secure Connection to CTI Manager parameter.

Note All changes require a restart of the Cisco Web Dialer service for the changes to take effect.

Use the following procedure initially to set or modify existing service parameters for the Webdialer servlet.

Procedure

Step 1 Choose **System** > **Service Parameters**.

Step 2 From the Server drop-down list box, choose the Cisco Unified Communications Manager server on which you want to configure Cisco Web Dialer service parameters.

Step 3 From the Service drop-down list box, choose the Cisco Web Dialer Web Service.

Default values already exist for the parameters Primary Cisco CTIManager, Duration of End Call Dialog, User SessionExpiry (InHours), and Apply Application Dial Rules (True). Enter new values if your application requires them.

The parameter Backup Cisco CTIManager does not have any default values that are assigned to it. Enter values for this parameter if your application requires a backup Cisco CTIManager.

Step 4 For new parameter values to take effect, restart the Cisco Web Dialer Web Service.

Configure Cisco Web Dialer in the Application Server Window

Instead of configuring the List of WebDialers service parameter, which limits the number of characters that you can enter, you can configure the WebDialer servers in the Application Server Configuration window in Cisco Unified Communications Manager Administration. To access the Application Server Configuration window, choose **System** > **Application Server** in Cisco Unified Communications Manager Administration. Cisco Web Dialer appears as one of the options in the Application Server Type drop-down list box.

After you add a Cisco Web Dialer application server in the Application Server Configuration window, the server displays in the List of WebDialers field in the Service Parameter Configuration window for the Cisco WebDialer Web Service.

Tip You can configure either the List of WebDialers service parameter or the Cisco Web Dialer application server through the Application Server Configuration window. If you add a Cisco Web Dialer application server in the Application Server Configuration window, the server displays in the List of WebDialers field in the Service Parameter Configuration window for the Cisco WebDialer Web Service. You can access the Service Parameter Configuration window by choosing **System** > **Service Parameters** in Cisco Unified Communications Manager Administration.

If you configured the List of WebDialers field in the Service Parameter Configuration window for the Cisco WebDialer Web Service before the upgrade to Cisco Unified Communications Manager 8.0(2) (or higher), the configured list of Web Dialers gets automatically migrated during the upgrade.

If you install Cisco Unified Communications Manager and plan to use Cisco Web Dialer, configure the Cisco Web Dialer application server in the Application Server Configuration window. You do not need to configure the List of WebDialers field in the Service Parameter Configuration window if you configure the application server in the Application Server Configuration window.

Configure the Application User

The Web Dialer needs a CTI connection to make and end calls. The Web Dialer uses the application user and password that are required to create a CTI provider. (The database stores this value as application user and the system retrieves it from there.) To secure a TLS connection to CTI, see the Secure TLS Connection to CTI, on page 1100.

Secure TLS Connection to CTI

Cisco Web Dialer supports a secure (TLS) connection to CTI. Obtain the secure connection by using the “WDSecureSysUser” application user.

Note You must configure a CAPF profile, in the Application User CAPF Profile Configuration windows in **Cisco Unified Communications Manager Administration**, that is configured for the instance ID for application user WDSecureSysUser to obtain a secure connection. If you enable security from the service Service Parameter Configuration window, the **Cisco Web Dialer** will open a secure connection to CTI Manager by using the Application CAPF profile. You should configure both the “CTI Manager Connection Security Flag” and the “CAPF Profile Instance ID for Secure Connection to CTI Manager” service parameters for the secure connection to succeed. See the **Cisco Unified Communications Manager Administration Guide**.

Perform the following procedure to configure the application user.

Procedure

Step 1 Choose **User Management** > **Application User**.

The Find and List Application Users window displays.

Step 2 Click **Find.**

Step 3 From the Find and List Application Users Application window, click **WDSysUser** or **WDSecureSysUser.**

Note To configure a CAPF profile, see **Secure TLS Connection to CTI** in the **Cisco Unified Communications Manager Administration Guide** for general information and to the **Cisco Unified Communications Manager Security Guide** for details.

Note You can change the password that is associated with the WDSysUser. The application obtains the new password from the database.

Configure Web Dialer for the Local Language

Cisco Unified Communications Manager gives precedence to languages that are set up in the client browser; for example, Microsoft Internet Explorer (see the following figure). To change the language that the client displays, use the browser settings (not the Locale field in the Cisco Unified CM User Options menu).

Conversely, Cisco Web Dialer gives precedence to the locale that is configured in the Cisco Unified Communications Self Care Portal.

Cisco Web Dialer accesses locales in the following ways:

- You can configure a Cisco Web Dialer user for a locale from the Cisco Unified Communications Self Care Portal; for example, Japanese.

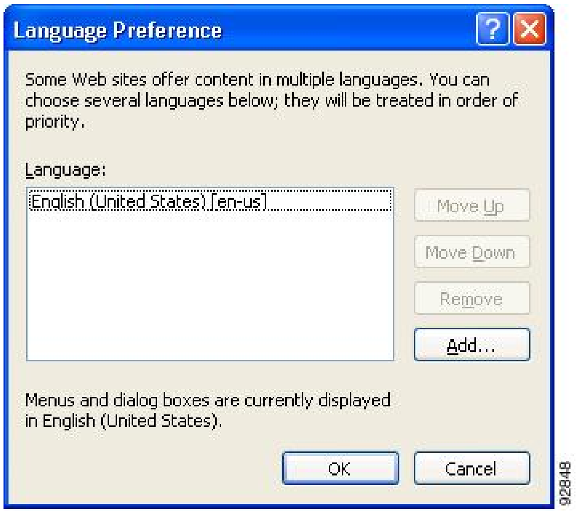
  When the user logs in to Web Dialer, the Web Dialer preferences window displays in Japanese. The user can change the language to the browser language; for example, by using Microsoft Internet Explorer. Cisco Web Dialer recognizes the browser language only in the format ll_CC. For example, the Japanese locale gets defined as ja_JP.

Note If the Japanese language displays incorrectly when you use Microsoft Windows, ensure that the Unicode font is installed on your machine.

- You can configure a Cisco Web Dialer (Locale field is set to None in the Cisco Unified Communications Self Care Portal).

  When the user logs in to Web Dialer, the Web Dialer preferences window displays in English. To change the language of the browser, the user must add a user-defined locale in the browser (using the format of ll_CC). For example, the Japanese locale gets defined as ja_JP.

Figure 174: Locale Settings in Microsoft Internet Explorer



Language Preference

Some Web sites offer content in multiple languages. You can choose several languages below; they will be treated in order of priority.

Language:

English (United States) [en-us]

Menus and dialog boxes are currently displayed in English (United States).

See the documentation that came with your browser for information on how to change a user-defined locale.

See Customizing Your Cisco Unified IP Phone on the Web for information on how to set the locale in the Cisco Unified CM User Options menu.

Partition Support

Cisco Web Dialer includes partition information, provided by JTAPI, as well as line information. The following list comprises the different available configurations:

- Lines with the same DN: Cisco Web Dialer handles different partition as different lines.
- Lines with the same DN: Cisco Web Dialer handles same partition and different devices as shared lines.
- Lines with the same DN: Cisco Web Dialer does not support same partition and in same device.

Configure the Redirector Servlet

Configure the Redirector servlet only if your applications require multiple clusters. Perform the following procedure to configure the Redirector servlet.

Procedure

Step 1 Choose **System** > **Service Parameters**.

Step 2 From the Server drop-down list box, choose the Cisco Unified Communications Manager server on which you want to configure the Redirector Servlet.

Step 3 From the Service drop-down list box, choose the Cisco Web Dialer Web Service.

Step 4 For the parameter, List of Web Dialers, enter new values that your application requires. See the Set Service Parameters for the Web Dialer Servlet, on page 1098 for a description of this service parameter.

Configure Application Dial Rules

Ensure that the application dial rules are configured for multiple cluster applications of Cisco Web Dialer.

For information on configuring these application dial rules, see the Cisco Unified Communications Manager Administration Guide for dial rule design and error checking.

Note Cisco Web Dialer must pick up the dial rule change without a restart.

Add Users to the Standard CUCM Users Group

For users to use the Cisco Web Dialer links in the User Directory windows in Cisco Unified Communications Manager, you must add each user to the Standard Cisco Unified Communications Manager End Users Group. The following procedure describes how to add users to this group.

Procedure

Step 1 Choose **User Management** > **User Group**.

The Find and List User Group window displays.

Click **Find.**

Step 2 Click the Standard CCM End Users link.

Step 3 The User Group Configuration window displays.

Step 4 Click **Add End Users to Group**.

The Find and List Users window displays.

Step 5 Click **Find**. You can enter criteria for a specific user.

Step 6 Check the check box next to the users that you want to add to the user group and click **Add Selected**.

Note If you want to add all users in the list of users, click **Select All** and then **Add Selected.**

The users display in the Users in Group table on the User Group Configuration window.

Create a Proxy User

Create a proxy user if you are using the makeCallProxy HTML over HTTP interface to develop an application for using Cisco Web Dialer. For information on the makeCallProxy interface, see the makeCallProxy section in the Cisco Web Dialer API Reference Guide.

You can enable authentication proxy rights for either an existing user or a new user.

Authentication Proxy Rights for Existing User

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 displays.

Click **Find.**

Step 2 Click the Standard EM Authentication Proxy Rights link.

The User Group Configuration window displays.

Step 3 Click **Add End Users to Group**.

The Find and List Users window displays.

Click **Find**. You can also add a criteria for a specific user.

Step 4 Choose the user to which you want to add proxy rights and click **Add Selected**.

Note If you want to add all the users in the list, click **Select All** and then click **Add Selected**.

The user displays in the Users in Group table on the User Group Configuration window.

Authentication Proxy Rights for New User

Perform the following procedure to enable authentication proxy rights for a new user.

Procedure

Step 1 Choose **User Management** > **End User**.

Step 2 Click **Add New**.

Step 3 Enter the following mandatory fields:

Last Name; User ID; Password; Confirm Password; PIN; and Confirm PIN.

Step 4 Click **Save**.

Step 5 Choose **User Management** > **User Group**.

The Find and List User Group window displays.

Step 6 Click the Standard EM Authentication Proxy Rights link.

The User Group Configuration window displays.

Step 7 Click **Add End Users to Group**.

The Find and List Users window displays.

Step 8 Click **Find**. You can also enter criteria for a specific user.

Step 9 Choose the user to which you want to add proxy rights and click **Add Selected**.

Note If you want to add all the users in the list, click **Select All** and then click **Add Selected**.

The user displays in the Users in Group table on the User Group Configuration window.

Trace Settings

You can configure trace settings from Cisco Unified Serviceability Administration. Use the following CLI commands to access the trace files:

file get activelog tomcat/logs/webdialer/log4j

file get activelog tomcat/logs/redirector/log4j

You can use the Real Time Monitoring Tool (RTMT) to collect traces.

Note The same trace settings apply to both Cisco Web Dialer and Redirector.

Perform the following procedure to enable debug traces for Cisco Web Dialer.

Procedure

Step 1 From the navigation drop-down list box 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 box, choose the server on which you want to enable traces for Cisco Web Dialer.

Step 4 From the Service drop-down list box, choose the Cisco Web Dialer Web Service.

Step 5 In the Trace Configuration window, change the trace settings according to your troubleshooting requirements. For more information on traces, see the Cisco Unified Serviceability Administration Guide.

Step 6 Click **Save.**