Cisco Unified Communications Manager Administration Guide, Release 10.0(1)

First Published: December 03, 2013

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-29000-01

CONTENTS

Preface

This preface describes 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 doc accessing Cisco's product documentation page at this URL:

`http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series`

Purpose

The Cisco Unified Communications Manager Administration Guide provides instructions for administering the Cisco Unified Communications Manager (formerly Cisco Unified CallManager) system. This guide includes descriptions of procedural tasks that you complete by using Cisco Unified Communications Manager Administration. The Cisco Unified Communications Manager Administration Guide also provides references for commands to assist you in using Cisco Unified Communications Manager. This book acts as a companion to the Cisco Unified Communications Manager System Guide, which provides conceptual information about Cisco Unified Communications Manager and its components as well as tips for setting up features by using Cisco Unified Communications Manager Administration.

Audience

The *Cisco Unified Communications Manager Administration 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.

Organization

The following table provides the organization of this guide.

Part	Description
Part 1	"Cisco Unified Communications Manager" Contains information about general topics that are related to the configuration and operation of Cisco Unified Communications Manager.
Part 2	“System Configuration” Contains information on how to configure the items in the Cisco Unified Communications Manager Administration System menu.
Part 3	“Call Routing Configuration” Contains information on how to configure call routing functions and features in Cisco Unified Communications Manager Administration.
Part 4	“Media Resource Configuration” Contains information on how to configure media resources that are used in conjunction with Cisco Unified Communications Manager.
Part 5	“Advanced Features Configuration” Contains information on how to configure the following features in Cisco Unified Communications Manager Administration: • Voice mail and messaging • Service Advertisement Framework (SAF) • Cisco Extension Mobility Cross Cluster (EMCC) • Cisco Intercompany Media Engine • Fallback • Virtual Private Network (VPN)
Part 6	“Device Configuration” Contains information on how to configure devices in Cisco Unified Communications Manager Administration.

Part	Description
Part 7	“Application Configuration” Contains information on how to configure plugin applications and application interfaces to work with Cisco Unified Communications Manager.
Part 8	“User Management Configuration” Contains information on how to configure application users, end users, roles, user groups, user-related CAPF profiles, and SIP realms in Cisco Unified Communications Manager Administration.
Part 9	"Cisco Unified Communications Manager Bulk Administration" Contains information about Cisco Unified Communications Manager Bulk Administration.
Part 10	“Appendixes” Contains information about dependency records and configuration of non-Cisco phones that are running SIP.

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 Features and Services 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.

Notes use the following conventions:

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

Timesavers use the following conventions:

Timesaver 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 conventions:

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.

Obtain Documentation and Submit Service Request

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.

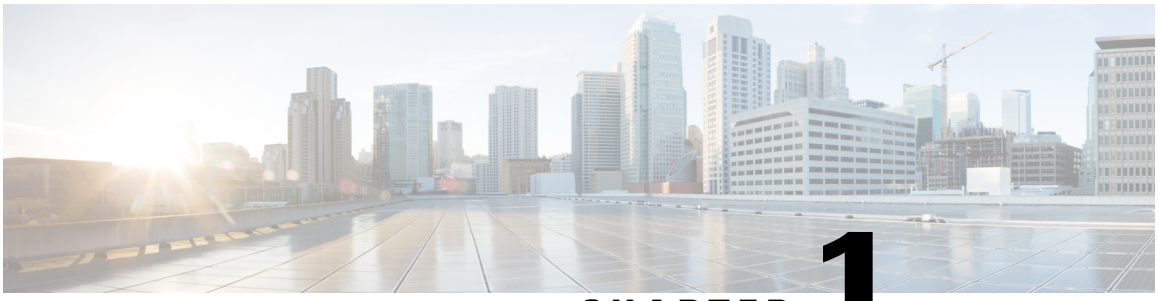
Cisco Product Security Overview

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`.

PART I

Cisco Unified Communications Manager



CHAPTER 1

Introduction

This chapter provides information about Cisco Unified Communications Manager (formerly Cisco Unified CallManager).

About Cisco Unified Communications Manager

Cisco Unified Communications Manager (formerly Cisco Unified CallManager) serves as the software-based call-processing component of the Cisco Unified Communications family of products. In Release 10.0(1) and later, Cisco only supports virtualized deployments of Cisco Unified Communications Manager (Unified Communications Manager) on Cisco Unified Computing System servers, or on a Cisco-approved third-party server configuration. In Release 10.0(1) and later, Cisco does not support deployments of Unified Communications Manager on Cisco Media Convergence Server servers.

For more information about the deployment of Unified Communications Manager in a virtualized environment, see:

http://docwiki.cisco.com/wiki/Unified_Communications_in_a_Virtualized_Environment.

The Cisco Unified Communications Manager system extends enterprise telephony features and functions to packet telephony network devices such as IP phones, media processing devices, voice-over-IP (VoIP) gateways, and multimedia applications. Additional data, voice, and video services, such as unified messaging, multimedia conferencing, collaborative contact centers, and interactive multimedia response systems, interact through Cisco Unified Communications Manager open telephony application programming interface (API).

Cisco Unified Communications Manager provides signaling and call control services to Cisco integrated telephony applications as well as third-party applications. Cisco Unified Communications Manager performs the following primary functions:

- Call processing

- Signaling and device control
- Dial plan administration
- Phone feature administration
- Directory services
- Operations, administration, maintenance, and provisioning (OAM&P)
- Programming interface to external voice-processing applications such as Cisco IP Communicator, Cisco Unified IP Interactive Voice Response (IP IVR).

Key Features and Benefits

The Cisco Unified Communications Manager system includes a suite of integrated voice applications that perform voice-conferencing and manual attendant console functions. This suite of voice applications means that no need exists for special-purpose voice-processing hardware. Supplementary and enhanced services such as hold, transfer, forward, conference, multiple line appearances, automatic route selection, speed dial, last-number redial, and other features extend to IP phones and gateways. Because Cisco Unified Communications Manager is a software application, enhancing its capabilities in production environments requires only upgrading software on the server platform, thereby avoiding expensive hardware upgrade costs.

Distribution of Cisco Unified Communications Manager and all Cisco Unified IP Phones, gateways, and applications across an IP network provides a distributed, virtual telephony network. This architecture improves system availability and scalability. Call admission control ensures that voice quality of service (QoS) is maintained across constricted WAN link and automatically diverts calls to alternate public switched telephone network (PSTN) routes when WAN bandwidth is not available.

A web-browsable interface to the configuration database provides the capability for remote device and system configuration. This interface also provides access to HTML-based online help for users and administrators.

Cisco Unified Communications Manager, designed to work like an appliance, refers to the following functions:

- Cisco Unified Communications Manager servers can get preinstalled with software to ease customer and partner deployment and automatically search for updates and notify administrators when key security fixes and software upgrades are available for their system.This process comprises Electronic Software Upgrade Notification.
- You can upgrade Cisco Unified Communications Manager servers while they continue to process calls, so upgrades take place with minimal downtime.
- Cisco Unified Communications Manager supports the Asian and Middle Eastern markets by providing support for Unicode on higher resolution phone displays.
- Cisco Unified Communications Manager provides Fault, Configuration, Accounting, Performance, and Security (FCAPS).

Cisco Unified Communications Manager Administration Web Browsers

You access the Cisco Unified Communications Manager Administration program from a PC that is not the web server or has Cisco Unified Communications Manager installed. No browser software exists on the server.

Related Topics

Web Browser Support, on page 5

Web Browser Support

Cisco Unified Communications Manager Administration supports the following operating system browsers:

- On Microsoft Windows XP, Vista, and 7:
  - Microsoft Internet Explorer (IE) 8, IE 9
  - Mozilla Firefox 4.x, Firefox 10.x
  - Google Chrome 8.x (only Self Care Portal page)
- On Apple OS X and later:
  - Apple Safari 5.x
  - Firefox 4.x, 10.x
  - Google Chrome 8.x (only Self Care Portal page)

From any user PC in your network, browse into a server that is running Cisco Unified Communications Manager Administration and log in with administrative privileges.

Note Simultaneous login to Cisco Unified Communications Manager Administration by a large number of users can cause performance to suffer. Try to limit the number of users and administrators that are logged on simultaneously.

Note Cisco Unified Communications Manager Administration does not support the buttons in your browser. Do not use the browser buttons (for example, the Back button) when you perform configuration tasks.

Note If you receive the following error message upon saving a configuration, entered changes are not lost. Click **Save** again after seeing the error message.

Security Error : The attempted action was a violation of security protocols and will not be allowed. This may be caused by having multiple concurrent windows open or using browser buttons (back, refresh, etc). Please retry the operation

Related Topics

Introduction, on page 3

Log In to Cisco Unified Communications Manager Administration

Use the following procedure to log in to Cisco Unified Communications Manager Administration. After you log in to Cisco Unified Communications Manager Administration, messages may display that indicate the

current state of licenses for Cisco Unified Communications Manager in the main window. For example, Cisco Unified Communications Manager may identify the following situations:

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

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

Procedure

Step 1 Start your preferred operating system browser.

Step 2 In the address bar of the web browser, enter the following case-sensitive URL:
`https://<Unified CM-server-name>:{8443}/ccmadmin/showHome.do`

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

Note You can optionally specify a port number.

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

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

Note The window for entering username and password is not displayed if single sign- on is enabled for Cisco Unified Communications Manager Administration. For more information on single sign-on feature, see Single Sign On section in the *Cisco Unified Communications Manager Features and Services Guide*.

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

Log Out of Cisco Unified Communications Manager Administration

Use the following procedure to log out of Cisco Unified Communications Manager Administration.

Procedure

Step 1 From the main Cisco Unified Communications Manager Administration window, click the Logout link in the upper, right corner.

Step 2 The window redisplays with the login fields.

Hypertext Transfer Protocol Over Secure Sockets Layer (HTTPS) Support

HTTPS, or Hypertext Transfer Protocol over Secure Sockets Layer (SSL), secures communication between a browser and a web server for Microsoft Windows users. HTTPS uses certificates to ensure server identities and to secure the browser connection. HTTPS uses a public key to encrypt the data, including the user login and password, during transport over the Internet.

To enable HTTPS, you must download a certificate that identifies the server during the connection process. You can accept the server certificate for the current session only, or you can download the certificate to a trust folder (file) to secure the current session and future sessions with that server. The trust folder stores the certificates for all your trusted sites.

The following Cisco Unified Communications Manager applications support HTTPS:

- Cisco Unified Communications Manager Administration
- Cisco Unity Connection Administration
- Cisco Unified Serviceability
- Cisco Unified Communications Self Care Portal
- Trace Collection Tool
- Cisco Unified Real Time Monitoring Tool (Unified RTMT)
- The XML (AXL) application programming interface

A self-signed certificate gets generated on the web server at installation (the certificate also gets migrated during upgrades).

Web Interface Timeout

Using the Command Line Interface (CLI), you can configure time, in minutes, after which the web interface times out and logs off the user. The default timeout value is 30 minutes. For more information, see the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*.

Import Cisco Certificate for Internet Explorer 7

Internet Explorer (IE) 7 adds security features that change the way that the browser handles Cisco certificates for website access. Because Cisco provides a self-signed certificate for the Cisco Unified Communications Manager server, Internet Explorer 7 flags the Cisco Unified Communications Manager Administration website as untrusted and provides a certificate error, even when the trust store contains the server certificate.

Note Cisco Unified Communications Manager Administration supports IE 7 when it is running on Microsoft Windows XP SP3.

Be sure to import the Cisco Unified Communications Manager certificate to Internet Explorer 7 to secure access without having to reload the certificate every time that you restart the browser. If you continue to a website that has a certificate warning and the certificate is not in the trust store, Internet Explorer 7 remembers the certificate for the current session only.

After you download the server certificate, Internet Explorer 7 continues to display certificate errors for the website. You can ignore the security warnings when the Trusted Root Certificate Authority trust store for the browser contains the imported certificate.

The following procedure describes how to import the Cisco Unified Communications Manager certificate to the root certificate trust store for Internet Explorer 7.

Procedure

Step 1 Browse to the application on the Tomcat server (for example, enter the hostname, localhost, or IP address for Cisco Unified Communications Manager Administration in the browser).
The browser displays a Certificate Error: Navigation Blocked page to indicate this website is untrusted.

Step 2 Click **Continue to this website (not recommended)** to access the server.
The Cisco Unified Communications Manager Administration window displays, and the browser displays the address bar and Certificate Error status in red.

Step 3 To import the server certificate, click the Certificate Error status box to display the status report. Click the **View Certificates** link in the report.

Step 4 Verify the certificate details.
The Certification Path tab displays "This CA Root certificate is not trusted because it is not in the Trusted Root Certification Authorities store."

Step 5 Select the General tab in the Certificate window and click **Install Certificate**.
The Certificate Import Wizard launches.

Step 6 To start the Wizard, click **Next**.
The Certificate Store window displays.

Step 7 Verify that the Automatic option, which allows the wizard to select the certificate store for this certificate type, is selected and click **Next**.

Step 8 Verify the setting and click **Finish**.
A security warning displays for the import operation.

Step 9 To install the certificate, click **Yes**.
The Import Wizard displays "The import was successful."

Step 10 Click **OK**. The next time that you click the View certificates link, the Certification Path tab in the Certificate window displays "This certificate is OK."

Step 11 To verify that the trust store contains the imported certificate, click **Tools** > **Internet Options** in the Internet Explorer toolbar and select the Content tab. Click **Certificates** and select the Trusted Root Certifications Authorities tab. Scroll to find the imported certificate in the list.
After importing the certificate, the browser continues to display the address bar and a Certificate Error status in red. The status persists even if you reenter the hostname, localhost, or IP address or refresh or relaunch the browser.

What to Do Next

You can copy the certificate to a file and store it locally so that you can restore the certificate whenever necessary.

Related Topics

Copy Web Browser Certificates to File , on page 13

Import Cisco Certificate for Internet Explorer 8

Note Cisco Unified Communications Manager Administration supports IE 8 when it is running on Microsoft Windows XP SP3 or Microsoft Vista SP2.

Be sure to import the Cisco Unified Communications Manager certificate to Internet Explorer 8 to secure access without having to reload the certificate every time that you restart the browser. If you continue to a website that has a certificate warning and the certificate is not in the trust store, Internet Explorer 8 remembers the certificate for the current session only.

After you download the server certificate, Internet Explorer 8 continues to display certificate errors for the website. You can ignore the security warnings when the Trusted Root Certificate Authority trust store for the browser contains the imported certificate.

The following procedure describes how to import the Cisco Unified Communications Manager certificate to the root certificate trust store for Internet Explorer 8.

Procedure

Step 1 Browse to application on the Tomcat server (for example, enter the hostname, localhost, or IP address for Cisco Unified Communications Manager Administration in the browser).
The browser displays a Certificate Error: Navigation Blocked message to indicate that this website is untrusted.

Step 2 Click **Continue to this website (not recommended)** to access the server.
The Cisco Unified Communications Manager Administration window displays, and the browser displays the address bar and Certificate Error status in red.

Step 3 To import the server certificate, click the Certificate Error status box to display the status report. Click the **View Certificates** link in the report.

Step 4 Verify the certificate details.

Step 5 Select the **General** tab in the Certificate window and click **Install Certificate**.
The Certificate Import Wizard launches.

Step 6 To start the Wizard, click **Next**.
The Certificate Store window displays.

Step 7 Verify that the Automatic option, which allows the wizard to select the certificate store for this certificate type, is selected and click **Next**.

Step 8 Verify the setting and click **Finish**.
A security warning displays for the import operation.

Step 9 To install the certificate, click **Yes**.
The Import Wizard displays “The import was successful.”

Step 10 Click **OK**. The next time that you click the View certificates link, the **Certification Path** tab in the Certificate window displays "This certificate is OK."

Step 11 To verify that the trust store contains the imported certificate, click **Tools** > **Internet Options** in the Internet Explorer toolbar and select the Content tab. Click **Certificates** and select the **Trusted Root Certifications Authorities** tab. Scroll to find the imported certificate in the list.
After importing the certificate, the browser continues to display the address bar and a Certificate Error status in red. The status persists even if you reenter the hostname, localhost, or IP address or refresh or relaunch the browser.

What to Do Next

You can copy the certificate to a file and store it locally so that you can restore the certificate whenever necessary.

Related Topics

Copy Web Browser Certificates to File , on page 13

Import Cisco Certificate for FireFox 3.x

Note Cisco Unified Communications Manager Administration supports FireFox 3.x when it is running on Microsoft Windows XP SP3, Microsoft Vista SP2 or Apple MAC OS X.

The first time that you (or a user) accesses Cisco Unified Communications Manager Administration or other Cisco Unified Communications Manager SSL-enabled virtual directories (after the Cisco Unified Communications Manager installation/upgrade) from a browser client, a Security Alert dialog box asks whether you trust the server.

When the dialog box displays, you must perform one of the following tasks:

- By clicking **I Understand The Risks**, you choose to trust the certificate for the current web session only. If you trust the certificate for the current session only, the Security Alert dialog box displays each time that you access the application; that is, until you install the certificate in the trusted folder.
- By clicking **Get Me Out Of Here**, you cancel the action. No authentication occurs, and you cannot access the web application. To access the web application, you must click **I Understand The Risks**.

The following procedure describes how to import the Cisco Unified Communications Manager certificate to the root certificate trust store for FireFox 3.x.

Procedure

Step 1 Access the Tomcat server (for example, enter the hostname, localhost, or IP address for Cisco Unified Communications Manager Administration in the browser).

Step 2 When the Security Alert dialog box displays, click **I Understand The Risks**.

Step 3 Click **Add Exception**.
The Add Exception dialog box displays.

Step 4 Click **Get Certificate**.

Step 5 Check the Permanently store this exception check box.

Step 6 Click **Confirm Security Exception**.

Step 7 To view the details of the certificate by performing the following steps:

a) From the FireFox browser, click **Tools** > **Options**.
The Options dialog box displays

b) Click **Advanced.**

c) Click **View Certificates**.
The Certificate Manager dialog box displays.

d) Highlight the certificate that you want to view and click **View**.
The Certificate Viewer dialog box displays.

e) Click the **Details** tab.

f) In the Certificate Fields field, highlight the field that you want to view.
Details display in the Field Values field.

g) From the Certificate Viewer dialog box, click **Close.**

h) From the Certificate Manager dialog box, click **OK.**

Related Topics

Copy FireFox Certificate to File , on page 13

Import Cisco Certificate for Safari 4.x

Note Cisco Unified Communications Manager Administration supports Safari 4.x when it is running on Apple MAC OS X.

The first time that you (or a user) accesses Cisco Unified Communications Manager Administration or other Cisco Unified Communications Manager SSL-enabled virtual directories (after the Cisco Unified Communications Manager installation/upgrade) from a browser client, a Security Alert dialog box asks whether you trust the server.

When the dialog box displays, you must perform one of the following tasks:

- By clicking **Yes**, you choose to trust the certificate for the current web session only. If you trust the certificate for the current session only, the Security Alert dialog box displays each time that you access the application; that is, until you install the certificate in the trusted folder.
- By clicking **Show Certificate** > **Install Certificate**, you intend to perform certificate installation tasks, so you always trust the certificate. If you install the certificate in the trusted folder, the Security Alert dialog box does not display each time that you access the web application.
- By clicking **No**, you cancel the action. No authentication occurs, and you cannot access the web application. To access the web application, you must click **Yes** or install the certificate via the **Show Certificate** > **Install Certificate** options.

Note The address that you use to access Cisco Unified Communications Manager must match the name on the certificate or a message will appear by default. If you access the web application by using the localhost or IP address after you install the certificate in the trusted folder, a security alert indicates that the name of the security certificate does not match the name of the site that you are accessing.

The following procedure describes how to import the Cisco Unified Communications Manager certificate to the root certificate trust store for Safari 4.x.

Procedure

Step 1 Access the Tomcat server (for example, enter the hostname, localhost, or IP address for Cisco Unified Communications Manager Administration in the browser).

Step 2 When the Security Alert dialog box displays, click **Show Certificate**.
You can click the Details tab to view the details of the certificate if you choose to verify the certificate data. To display a subset of settings, if available, choose one of the following options:

a) All—All options display in the Details pane.
b) Version 1 Fields Only—Version, Serial Number, Signature Algorithm, Issuer, Valid From, Valid To, Subject, and the Public Key options display.
c) Extensions Only—Subject Key Identifier, Key Usage, and the Enhanced Key Usage options display.
d) Critical Extensions Only—Critical Extensions, if any, display
e) Properties Only—Thumbprint algorithm and the thumbprint options display.

Step 3 In the Certificate pane, click **Install Certificat**e.

Step 4 When the Certificate Import Wizard displays, click **Next**.

Step 5 Click the **Place all certificates in the following store** radio button; click **Browse**.

Step 6 Browse to Trusted Root Certification Authorities; select it and click **OK.**

Step 7 Click **Next**.

Step 8 Click **Finish**.
A Security Warning Box displays the certificate thumbprint for you.

Step 9 To install the certificate, click **Yes**.
A message states that the import was successful. Click **OK**.

Step 10 In the lower, right corner of the dialog box, click **OK**.

Step 11 To trust the certificate, so you do not receive the dialog box again, click **Yes**.

Tip You can verify the certificate was installed successfully by clicking the Certification Path tab in the Certificate pane.

What to Do Next

You can copy the certificate to a file and store it locally so that you can restore the certificate whenever necessary.

Related Topics

Copy Web Browser Certificates to File , on page 13

Copy Web Browser Certificates to File

You can copy certificates to local files and restore the certificates later whenever necessary.

Performing the following procedure copies the certificate using a standard certificate storage format for the following browsers:

- Internet Explorer 7
- Internet Explorer 8
- Safari 4.x

Procedure

Step 1 View the certificate.

a) For Internet Explorer, click the Certificate Error status box, then click **View Certificates**.

b) For Safari 4.x, click **Show Certificate** in the Security Alert dialog box.

Tip In Safari, click the Certificate Error status box to display the Show Certificate option.

Step 2 Click the **Details** tab.

Step 3 Click the **Copy to File** button.

Step 4 The Certificate Export Wizard displays. Click **Next**.

Step 5 The following list defines the file formats from which you can choose. Choose the file format that you want to use for the exported file; click **Next**.

a) DER encoded binary X.509 (.CER)—Uses DER to transfer information between entities.

b) Base-64 encoded X.509 (.CER)—Sends secure binary attachments over the internet; uses ASCII text format to prevent corruption of file.

c) Cryptographic Message Syntax Standard-PKCS #7 Certificates (.P7B)—Exports the certificate and all certificates in the certification path to the chosen PC.

Step 6 Browse to the location to which you want to export the file copy and name the file. Click **Save**.

Step 7 The file name and path display in the **Certificate Export Wizard** pane. Click **Next**.

Step 8 Your file and settings display. Click **Finish**.

Step 9 When the successful export dialog box displays, click **OK**.

Copy FireFox Certificate to File

You can copy the certificate to a local file and restore the certificate later whenever necessary.

Performing the following procedure copies the certificate by using a standard certificate storage format. To copy the certificate contents to file, perform the following procedure.

Procedure

Step 1 From the FireFox browser, click **Tools** > **Options**.
The Options dialog box displays.

Step 2 If it is not already selected, click **Advanced**.

Step 3 Click the Encryption tab and click **View Certificates**.
The Certificate Manager dialog box displays.

Step 4 Click the **Servers** tab.

Step 5 Highlight the certificate you want to copy and click **Export**.
The Save Certificate to File dialog box displays.

Step 6 Browse to the location to which you want to copy the file.

Step 7 From the Save as type drop-down list, choose the file type from the following options:

a) X.509 Certificate (PEM)—Uses PEM to transfer information between entities.

b) X.509 Certificate with chain (PEM)—Uses Privacy Enhanced Mail to verify the certificate chain and transfer information between entities.

- X.509 Certificate (DER)—Uses DER to transfer information between entities.
- X.509 Certificate (PKCS#7)—PKCS#7 is a standard for signing or encrypting data. Since the certificate is needed to verify signed data, it is possible to include it in the SignedData structure. A .P7C-file is just a degenerated SignedData structure, without any data to sign.
- X.509 Certificate with chain (PKCS#7)—Uses PKCS#7 to verify the certificate chain and transfer information between entities.

Step 8 Click **Save**.

Step 9 Click **OK**.

What to Do Next

You can copy the certificate to a file and store it locally so that you can restore the certificate whenever necessary.

Cisco Unified Communications Manager Administration Application

You use Cisco Unified Communications Manager Administration, a web-based application, to perform configuration tasks for Cisco Unified Communications Manager servers. This section describes basic elements of the graphical user interface, including the navigation menus and the documentation search feature that allows you to search Cisco Unified Communications Manager documentation on Cisco.com.

Cisco Unified Communications Manager Administration Graphical User Interface

After you log in, the main Cisco Unified Communications Manager Administration window redisplays. The window includes the drop-down list box in the upper, right corner called Navigation. To access the applications in the drop-down list box, choose the program that you want and click **Go**.

Note The minimum supported screen resolution specifies 1024x768. Devices with lower screen resolutions may not display the applications correctly.

Related Topics

Introduction, on page 3
Navigation Drop-Down List Box , on page 15
Links to Search documentation, About, and Logout, on page 15
Menu Bar , on page 16
Shared Login, on page 16

Navigation Drop-Down List Box

The choices in the Navigation drop-down list box include the following Cisco Unified Communications Manager applications:

- Cisco Unified Communications Manager Administration—Shows as default when you access Cisco Unified Communications Manager. Use Cisco Unified Communications Manager Administration to configure system parameters, route plans, devices, and much more.
- Cisco Unified Serviceability—Takes you to the main Cisco Unified Serviceability window that is used to configure trace files and alarms and to activate and deactivate services.
- Cisco Unified OS Administration—Takes you to the main Cisco Unified OS Administration window, so you can configure and administer the Cisco Unified Communications Manager platform. You must log out from any other application before you can log in to this application.
- Disaster Recovery System—Takes you to the Cisco Disaster Recovery System, a program that provides full data backup and restore capabilities for all servers in a Cisco Unified Communications Manager cluster. You must log out from any other application before you can log in to this application.
- Cisco Unified Reporting—Takes you to the main Cisco Unified Reporting window where you can generate system reports.

Links to Search documentation, About, and Logout

The following links display on the main Cisco Unified Communications Manager Administration window directly below the Navigation drop-down list box:

- Search Documentation—Click this link to search Cisco Unified Communications Manager documentation on Cisco.com for the current release. The Cisco Unified CM Documentation Search window displays. Type the word or words for which you want to search and click the Search button. The search results display. You can narrow the search results by choosing a documentation type modifier button that

displays above your search result; for example, Unified CM Install/Upgrade or Unified CM Release Notes.

- About—Click this link to display the Cisco Unified Communications Manager Administration main window where you can view the system software version.
- Logout—Click this link to log out of the Cisco Unified Communications Manager Administration application. The window redisplays with the login fields.

Menu Bar

The horizontal bar located across the top of the interface contains the names of the menus. Click the menu options to display the Cisco Unified Communications Manager Administration windows. Menu items in this document appear in boldface font. A > (greater than) symbol separates menu item selections. In the browser, this indicates a menu item selection; for example: Choose **Advanced Features** > **Intercompany Media Services** > **Service**.

Shared Login

After you log in to Cisco Unified Communications Manager Administration, you can access all applications that display in the Navigation drop-down list box, except the Cisco Unified Operating System Administration and Disaster Recovery System, without needing to log in to each application. You cannot access the Cisco Unified Operating System Administration or Disaster Recovery System GUIs with the same username and password that you use to access Cisco Unified Communications Manager Administration. To access these applications from Cisco Unified Communications Manager Administration, you must first click the **Logout** link in the upper, right corner of the Cisco Unified Communications Manager Administration window; then, choose the application from the Navigation drop-down list box and click **Go**.

If you have already logged in to one of the applications that display in the Navigation drop-down list box (other than Cisco Unified Operating System Administration or Disaster Recovery System), you can access Cisco Unified Communications Manager Administration without logging in. From the Navigation drop-down list box, choose Cisco Unified Communications Manager Administration and click **Go**.

Cisco Unified Communications Manager Administration Help

To access Help, click the Help menu in the Cisco Unified Communications Manager Administration navigation menu, and choose one of the following options:

- Contents—Opens a new browser window and displays the home page for the Cisco Unified Communications Manager Administration Help system. The links in the left pane of the Help window allow you to access all topics in the Help system.
- This Page—Opens a new browser window for the Cisco Unified Communications Manager Administration Help system. The right pane of the window contains definitions for each field in the current window in Cisco Unified Communications Manager Administration. In most cases, cross-references point to additional topics that relate to the current window.
- About—Displays the Cisco Unified Communications Manager Administration main window where you can view the system software version.

The left pane of the Help system provides a table of contents for all of the product guides that the Help system includes. The table of contents expands to show the location within the hierarchy of the Help topic that displays on the right.

To learn more about the Cisco Unified Communications Manager Administration system, including instructions on how to search Help, click the **Using Help** link at the top of any Help window.

Find and Delete Records

You can search Cisco Unified Communications Manager for any records that you have added to the database through the Cisco Unified Communications Manager Administration windows or for records that exist as default entries. To find records, you navigate to the Find and List window for the record that you want to locate, such as Find and List Phones (**Device** > **Phone**). You can search for all records or enter search criteria to narrow your search. The search parameters vary, depending on the records for which you are searching. For example, when searching for a phone, you can search for phones with certain digits in the directory number or certain characters in the device name. When searching for an end user, you can search for first names or last names that contain certain letters.

Once you have found records, you can delete them from the Find and List window that contains your records. You can delete individual records or delete all records that display in the window.

Note During your work in a browser session, the cookies on the client machine store your find/list search preferences. If you navigate to other menu items and return to this menu item, or if you close the browser and then reopen a new browser window, your Cisco Unified Communications Manager search preferences get retained until you modify your search.

Use the following procedure to find or delete records from Cisco Unified Communications Manager Administration.

Procedure

Step 1 Navigate to the Find and List window in Cisco Unified Communications Manager Administration for the component that you want to find. For example, if you want to find a phone, choose **Device** > **Phone** to display the Find and List Phones window.

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

Step 3 To filter or search records

a) From the first drop-down list box, select a search parameter. The search parameter represents the field on which you want to search. The search parameters vary, depending on the records type.

b) From the second drop-down list box, select a search pattern. The search pattern defines how the system searches the records. For example, you might want to search for records (or search parameters) that contain a certain value that you specify in the search text field.

c) Specify the appropriate search text, if applicable. The search text allows you to specify values for which you want to search. Use this field in conjunction with the search parameter and search pattern fields. For example, if you choose “Directory Number” from the search parameter drop-down list box, choose “contains” from the search pattern drop-down list box, and enter 5551212 as the search text, the system searches for a directory number that contains the digits 5551212.

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 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.

You can reverse the sort order, by clicking the Up Arrow or Down Arrow, if available, in the list header.

Note You can delete multiple records from the database by checking the check boxes next to the appropriate record(s) and clicking **Delete Selected**. You can delete all configurable records for this selection by clicking the check box at the top of the column of check boxes 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.
The window displays the item that you choose.

Related Topics

GUI Buttons and Icons , on page 19

Add and Copy Records

You can add items to the Cisco Unified Communications Manager by creating new records in Cisco Unified Communications Manager Administration and sometimes by copying existing records. Use the following procedure to add or copy records to the database.

Procedure

Step 1 Navigate to the Find and List window in Cisco Unified Communications Manager Administration for the component that you want to add or copy. For example, if you want to add a transcoder, choose **Media Resources** > **Transcoder** to display the Find and List Transcoders window.

Step 2 To add a new record, click the **Add New** button.
The window refreshes with a new record. Make the necessary changes, and click **Save**.

Step 3 To copy an existing record, do one of the following:

a) Use the Find and List window to display a set of records. From the list of records, click the **Copy** icon for a particular record, if the icon is available.

b) Locate the record that you want to copy. Choose the record, which causes the complete record to display. Click the **Copy** icon in the configuration window. For example, find the transcoder that you want to copy, and click the **Copy** icon in the Transcoder Configuration window.
The window refreshes with a new record. Make the necessary changes, and click **Save**.

Note You must make a change to the copied record before you save the copy. If you do not, the system does not save the copy.

Step 4 To copy an existing record and populate a new record with all of the associated information from the existing record:

a) Use the Find and List window to display a set of records. From the list of records, click the Super Copy icon for a particular record, if the icon is available.

b) Locate the record that you want to copy. Choose the record, which causes the complete record to display. Click the **Super Copy** button in the configuration window. For example, find the phone record that you want to copy, and click the **Super Copy** button in the Phone Configuration window.

The window refreshes with a new Device Name field. Make the necessary changes, and click **Save**.

Related Topics

Find and Delete Records , on page 17
GUI Buttons and Icons , on page 19

GUI Buttons and Icons

The Cisco Unified Communications Manager Administration windows use a common set of buttons and icons across the GUI. In general, icons display in a row that follows the window name, and a matching set of buttons displays near the bottom of the window.

Note Not all buttons and icons display on all windows. For those buttons that are not listed here, the individual configuration settings tables for each record type describe buttons that pertain to particular record types.

The Cisco Unified Communications Manager Administration GUI has the following groups of buttons and icons:

- Buttons and Icons on Find and List Windows
- Buttons and Icons on Configuration Windows

Find and List Window Buttons and Icons

The following icons and buttons are found in the Find and List windows of the Cisco Unified Communications Manager Administration GUI:

- Add New—Opens a blank window of the same record type. Add configuration details to the new record and click **Save**, or choose an option in the Related Links drop-down list box.
- Select All—Chooses all of the records of a particular type that you are displaying. The check boxes to the left of each record get checked.

Note This button selects only the records on the particular page that you are displaying.

Note Example: Your search for partitions yielded 300 partitions, but you are only displaying 50 rows per page. If you click **Select All** while displaying any set of 50 partitions, only those 50 partitions get checked.

- Clear All—Deselects all of the records of a particular type that you are displaying. The check boxes to the left of each record get unchecked.

- Delete Selected—After you display a set of records, deletes the records for which you have checked the check boxes at left. You must confirm the deletion before the deletion takes place.
- Reset Selected—After you display a set of records, resets the records for which you have checked the check boxes at left. A popup window opens and offers the following choices:
  - Reset—Shuts down the device(s) and then restarts it (them).
  - Restart—Restarts the device(s) without shutting it (them) down.
  - Close—Closes the popup window without taking any action.
- Apply Config to Selected—When you change the configuration settings of a record, you may receive a message that directs you to click the **Apply Config** button to have the changes take effect. You can wait until you finish configuring multiple devices, then return to the Find and List window. Select the reconfigured devices and click the **Apply Config** to Selected button. A popup window advises of the possible actions that will take place when you click **OK**.
- 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.
- Find—Initiates a search for all records that match the criteria that you entered.
- Clear Filter—Removes all added search criteria from a search.
- + (Plus button)—To add additional search criteria to a search, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify.
- **–** (Minus button)—To remove criteria from a search, click the **–** button to remove the last added criterion.
- First-page Arrow—In a multipage list of records, click the First-page Arrow to display the first page of records.
- Left Arrow—In a multipage list of records, click the Left Arrow to display the preceding page of records.
- Right Arrow—In a multipage list of records, click the Right Arrow to display the following page of records.
- Last-page Arrow—In a multipage list of records, click the Last-page Arrow to display the last page of records.
- Go—In a multipage list of records, enter a value for the page of records to display; then, click Go.

Configuration Windows Buttons and Icons

The following icons and buttons are found in the Configuration windows of the Cisco Unified Communications Manager Administration GUI:

- Save—Saves the current record.
- Delete—Deletes the current record after requesting confirmation of the deletion.
- Copy—Refreshes the window with a copy of the current record. You must change at least one value (usually, the record name) before you can save the copied record by clicking **Save**.
- Reset—Opens a popup window that offers the following choices:

- Reset—Shuts down the device and then restarts it.
- Restart—Restarts the device without shutting it down.
- Close—Closes the popup window without taking any action.

- Apply Config—When you change the configuration settings of a record, you may receive a message that directs you to click the **Apply Config** button to have the changes take effect. When you click the **Apply Config** button, a popup window advises of the possible actions that will take place when you click **OK**.
- Add New—Opens a blank window of the same record type. Add configuration details to the new record and click **Save**, or choose an option in the Related Links drop-down list box.
- Next—For record types that require multiple steps to add a new record, the Next button takes you from one step to the next.

Cisco Unified Presence Server Access

If you have configured a Cisco Unified Presence server, the Cisco Unified Communications Manager Administration main window provides a link directly to the associated Cisco Unified Presence server. To access Cisco Unified Presence Administration, click the Cisco Unified Presence address link.

Clustered Cisco Unified Presence Server Access

If you have a Cisco Unified Presence server configured as part of the Cisco Unified Communications Manager cluster, the main Cisco Unified Communications Manager Administration window displays a link to the Cisco Unified Presence publisher server.

To access Cisco Unified PresenceAdministration, click the link to the Cisco Unified Presence publisher server.

Login Message Customization

You can upload a text file that contains a customized login message that displays in the main Cisco Unified Communications Manager Administration window.

For more information and the procedure for uploading your customized login message, see the *Cisco Unified Communications Operating System Administration Guide*.

Last Successful Login Message

When you log in to Cisco Unified Communications Manager Administration, the main Cisco Unified Communications Manager Administration window displays the date and time of the last successful system login.

When you log in to Cisco Unified Communications Manager for the first time, the system displays the last successful login time as the current time.

Accessibility

Cisco Unified Communications Manager Administration and Cisco Unified Communications Self Care Portal provide functionality for users that allows them to access buttons on the window without using a mouse. You can perform the following procedures from any point on the window, so the user does not have to scroll or tab through various fields.

Access Icons

Many of the windows in Cisco Unified Communications Manager include icons that display at the top of the window; for example, an icon of a disk for Save, an icon that is a plus sign (+) for Add, and so on. To access these icons, perform the following procedure.

Procedure

Step 1 Press **Alt**, press **1**; then, press **Tab**.
The cursor will highlight the first icon from the left. To move to the next icon, press **Tab** again.

Step 2 Press **Enter**.
The system performs the function of the icon; for example, Add.

Access Buttons

Many of the windows in Cisco Unified Communications Manager and Cisco PCA have buttons that display at the bottom of the window; for example, a button for Save, a button for Add, and so on. To access these buttons, perform the following procedure.

Procedure

Step 1 Press **Alt**, press **2**, and then press **Tab**.
The cursor will highlight the first button from the left. To move to the next button, press **Tab** again.

Step 2 Press **Enter**.
The function of the button gets performed; for example, Save.

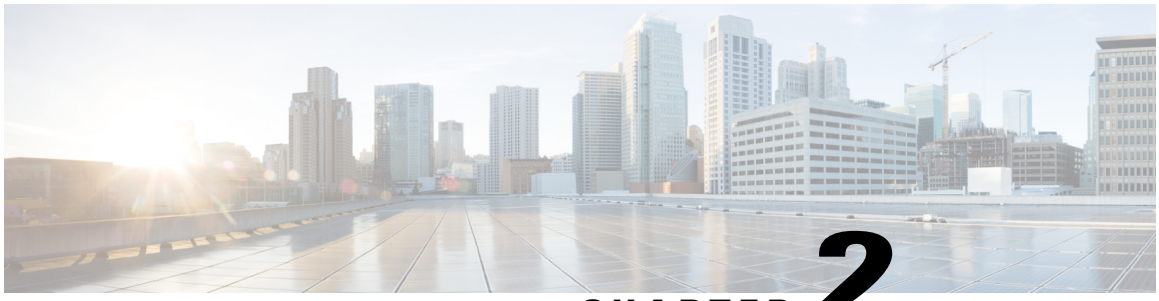
Where to Find More Information

- *Cisco Unified Communications Manager System Guide*
- *Cisco Unified Communications Manager Features and Services Guide*
- *Cisco Unified Serviceability Administration Guide*

- *Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide*
- *Installing Cisco Unified Communications Manager*
- *Upgrading Cisco Unified Communications Manager*
- *Cisco Unified Communications Manager Security Guide*
- *Cisco Unified Communications Operating System Administration Guide*
- *Disaster Recovery System Administration Guide*
- *Cisco Unified Communications Solution Reference Network Design (SRND)*

PART II

System Setup



CHAPTER 2

Server Setup

This chapter provides information about server configuration.

See also Internet Protocol Version 6 (IPv6) in *Cisco Unified Communications Manager Features and Services Guide* and *Changing the IP Address and Host Name for Cisco Unified Communications Manager*.

About Server Setup

In Cisco Unified Communications Manager Administration, use the **System** > **Server** menu path to add and configure a server.

Use the Server Configuration window to specify the address of the server where Cisco Unified Communications Manager or Cisco Unified Communications Manager IM and Presence Service is installed.

You must add and configure new servers using Cisco Unified Communications Manager Administration prior to their installation. The server type you configure must match the server type you install. To install a node on a cluster, see the *Cisco Unified Communications Manager Installation Guide*.

Server Setup Tips

Before you configure a server, review the following information:

- Make sure that you only add each server once in the Server Configuration window. If you add a server by using the hostname and add the same server again by using the IP address, Cisco Unified Communications Manager cannot accurately determine component versions for the server after a Cisco Unified Communications Manager upgrade. If you have two entries in Cisco Unified Communications Manager Administration for the same server, delete one of the entries before you upgrade.

- When you perform a fresh installation of Cisco Unified Communications Manager, you must define any subsequent servers (nodes) in the Server Configuration window using Cisco Unified Communications Manager Administration before you can install Cisco Unified Communications Manager or IM and Presence Service on each subsequent server. To define a subsequent node, click Add New and proceed to configure the server. After you add the subsequent server, you can then install the Cisco Unified Communications Manager or IM and Presence Service software on that server.
- If you use IPv4 in your network, you must update the DNS server with the appropriate Cisco Unified Communications Manager name and address information before you use that information to configure the Cisco Unified Communications Manager server.
- For DNS, make sure that you map the IP addresses of all servers, including dummy nodes, to the host names on the DNS server. If you do not perform this task, Cisco Unified Communications Manager generates alarms that inform you that the License Manager service is down.
- Cisco Unified Communications Manager Administration does not prevent you from updating the Host Name/IP Address field under any circumstances.
- When you attempt to change the IP address in the Server Configuration window, the following message displays after you save the configuration: "Changing the host name/IP Address of the server may cause problems with Cisco Unified Communications Manager. Are you sure that you want to continue?" Before you click OK, make sure that you understand the implications of updating the Host Name/IP Address field; for example, incorrectly updating this setting may cause Cisco Unified Communications Manager to become inoperable; that is, the database may not work, you may not be able to access Cisco Unified Communications Manager Administration, and so on. In addition, updating this field without performing other related tasks may cause problems for Cisco Unified Communications Manager.
- Changes to the server configuration do not take effect until you restart Cisco Unified Communications Manager. For information about restarting the Cisco CallManager service, see the *Cisco Unified Serviceability Administration Guide*.
- For additional information on changing the IP address or host name, see the document *Changing the IP Address and Host Name for Cisco Unified Communications Manager*.

Related Topics

Server Deletion , on page 28

Server Deletion

This section describes how to delete a server from the Cisco Unified Communications Manager database and how to add a deleted server back to the Cisco Unified Communications Manager cluster.

In Cisco Unified Communications Manager Administration, you cannot delete the first node of the cluster, but you can delete subsequent nodes. Before you delete a subsequent node in the Find and List Servers window, Cisco Unified CM Administration displays the following message: “You are about to permanently delete one or more servers. This action cannot be undone. Continue?”. If you click OK, the server gets deleted from the Cisco Unified CM database and is not available for use.

Tip When you attempt to delete a server from the Server Configuration window, a message that is similar to the one in the preceding paragraph displays. If you click OK, the server gets deleted from the Cisco Unified CM database and is not available for use.

Before you delete a server, consider the following information:

- Cisco Unified Communications Manager Administration does not allow you to delete the first node in the cluster, but you can delete any subsequent node.
- Cisco recommends that you do not delete any node that has Cisco Unified Communications Manager running on it, especially if the node has devices, such as phones, registered with it.
- Although dependency records exist for the subsequent nodes, the records do not prevent you from deleting the node.
- If any call park numbers are configured for Cisco Unified Communications Manager on the node that is being deleted, the deletion fails. Before you can delete the node, you must delete the call park numbers in Cisco Unified Communications Manager Administration.
- If a configuration field in Cisco Unified Communications Manager Administration contains the IP address or host name for a server that you plan to delete, update the configuration before you delete the server. If you do not perform this task, features that rely on the configuration may not work after you delete the server; for example, if you enter the IP address or host name for a service parameter, enterprise parameter, service URL, directory URL, IP phone service, and so on, update this configuration before you delete the server.
- If an application GUI, for example, Cisco Unity, Cisco Unity Connection, and so on, contains the IP address or host name for the server that you plan to delete, update the configuration in the corresponding GUIs before you delete the server. If you do not perform this task, features that rely on the configuration may not work after you delete the server.
- The system may automatically delete some devices, such as MOH servers, when you delete a server.
- Before you delete a node, Cisco recommends that you deactivate the services that are active on the subsequent node. Performing this task ensures that the services work after you delete the node.
- Changes to the server configuration do not take effect until you restart Cisco Unified Communications Manager. For information on restarting the Cisco CallManager service, see the *Cisco Unified Serviceability Administration Guide*.
- To ensure that database files get updated correctly, you must reboot the cluster after you delete a server, Presence, or application server.
- After you delete the node, access Cisco Unified Reporting to verify that Cisco Unified Communications Manager removed the node from the cluster. In addition, access Cisco Unified Reporting, RTMT, or the CLI to verify that database replication is occurring between existing nodes; if necessary, repair database replication between the nodes by using the CLI.

Remove Node From Cluster

Follow this procedure if you need to safely remove an IM and Presence Service node from its presence redundancy group.

Caution Removing a node will cause a service interruption to users on the remaining node(s) in the presence redundancy group. This procedure should only be performed during a maintenance window.

Procedure

Step 1 On the **Cisco Unified CM Administration > System > Presence Redundancy Groups** page, disable High Availability if it is enabled.

Step 2 On the **Cisco Unified CM Administration > User Management > Assign Presence Users** page, unassign or move all the users off the node that you want to remove.

Step 3 To remove the node from its presence redundancy group, choose **Not-Selected** from the Presence Server drop down list on the presence redundancy group's Presence Redundancy Group Configuration page. Select **OK** when a warning dialog box indicates that services in the presence redundancy group will be restarted as a result of unassigning the node.

Step 4 Delete the unassigned node from the **Cisco Unified CM Administration > System > Server** page. Select **OK** when a warning dialog box indicates that this action cannot be undone.

Step 5 Shut down the host VM or server for the node you have unassigned.

Add Deleted Server Back in to Cluster

If you delete a subsequent node (subscriber) from Cisco Unified Communications Manager Administration and you want to add it back to the cluster, perform the following procedure.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, add the server by choosing **System** > **Server**.

Step 2 After you add the subsequent node to Cisco Unified Communications Manager Administration, perform an installation on the server by using the disk that Cisco provided in your software kit.

Tip For example, if you have a version 8.5(1) disk, perform a 8.5(1) installation on the node. If you have a disk with a compatible version of 6.1(3) on it, for example, use the disk to install Cisco Unified CM on the subsequent node; during the installation, choose the Upgrade During Install option when the installation displays the options.

Make sure that the version that you install on the subsequent node matches the version that runs on the first node (publisher) in the cluster.

If the first node in the cluster runs Cisco Unified Communications Manager 8.5(1) version and a service update (or engineering special), you must choose the Upgrade During Install option when the installation displays the installation options; before you choose this option, ensure that you can access the service update (or engineering special) image on DVD or a remote server. For more information on how to perform an installation, see the installation documentation that supports your version of Cisco Unified Communications Manager.

Step 3 After you install Cisco Unified CM, configure the subsequent node, as described in the installation documentation that supports your version of Cisco Unified CM.

Step 4 Access the Cisco Unified Reporting, RTMT, or the CLI to verify that database replication is occurring between existing nodes; if necessary, repair database replication between the nodes.

Server Settings

The following table describes the server configuration settings.

Table 1: Server Settings

Field	Description
Server Information	
Server Type	From the drop-down list box, select the server type that suits your network configuration. The following are the available server types: • CUCM Voice/Video • CUCM IM and Presence **Note** You can only change the server type when you add a new server. If you want to make a change to the server, you must delete it, then add it again from this window.
CUCM Voice/Video	
Host Name/IP Address	If your network uses DNS that can map to IPv4 addresses, you can enter the host name of the Cisco Unified Communications Manager server. Otherwise, you must enter the full IPv4 address of the server. **Tip** To avoid errors, Cisco recommends that you add a server to the system with a name that has less than 47 characters. Then, update the server name to the target length. **Tip** If your network supports IPv6 (or IPv4 and IPv6), configure the IPv6 Name field in addition to the Hostname/IP Address field. **Note** You must update the DNS server with the appropriate Cisco Unified Communications Manager name and address information before you enter that information in this field.

Field	Description
IPv6 Address (for dual IPv4/IPv6)	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 server. Otherwise, enter the non-link-local IP address of the Cisco Unified Communications Manager server; for information on how to obtain the non-link local IP address, see the *Cisco Unified Communications Manager Features and Services Guide*. This field, which gets included in the TFTP configuration file, gets used by phones that run SCCP to retrieve the IPv6 address of the Cisco Unified Communications Manager server, so phone registration occurs. **Tip** Remember to update the DNS server with the appropriate Cisco Unified Communications Manager name and address information. **Tip** In addition to configuring the IPv6 Name field, you must configure the IP Address/Hostname field, so Cisco Unified Communications Manager can support features/devices that use IPv4 (or IPv4 and IPv6).
MAC Address	This field is optional. It exists only to give you a place to note the server MAC address. It does not impact the system at all. Enter the media access control (MAC) address of the network interface card (NIC) in the Cisco Unified Communications Manager server. The MAC address specifies the permanent hardware address of the NIC. **Tip** If you plan to move the server periodically to different locations on the network, you must enter the MAC address, so other devices on the network can always identify the server. If you do not plan to relocate the server, consider entry of the MAC address as optional.
Description	Consider this entry as optional. Enter a description of the server. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
Location Bandwidth Management Information	
LBM Intercluster Replication Group	Select an LBM Intercluster Replication Group from the drop-down list. You may also click **View Details** to display the settings for this LBM Intercluster Replication Group.
CUCM IM and Presence	
Fully Qualified Domain Name/IP Address	Enter the Fully Qualified Domain Name (FQDN) or IP address of the node, up to a maximum of 255 characters. By default, the name for a node is the FQDN of the IM and Presence Service server. Note that the hostname of the node can be entered but Cisco recommends that you use the FQDN or the IP address.

Field	Description
IM and Presence Domain	Provide a valid domain that specifies the IM and Presence domain name of the IM and Presence server. Typically this parameter should be an enterprise top-level domain name (for example, example.com). The parameter that you enter allows the IM and Presence server to identify which URIs are to be treated as local and managed by this installation. Instant Messaging (IM) or availability status requests addressed to other domains must be forwarded via federation. Other SIP requests may be proxied. **Note** This value does not have to be the same as the DNS network domain of the IM and Presence server.
Description	Consider this entry as optional. Enter a description of the server. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).

Related Topics

Server Setup , on page 27

View Presence Server Status

Use Cisco Unified CM Administration to view the status of critical services and self-diagnostic test results for the IM and Presence Service node.

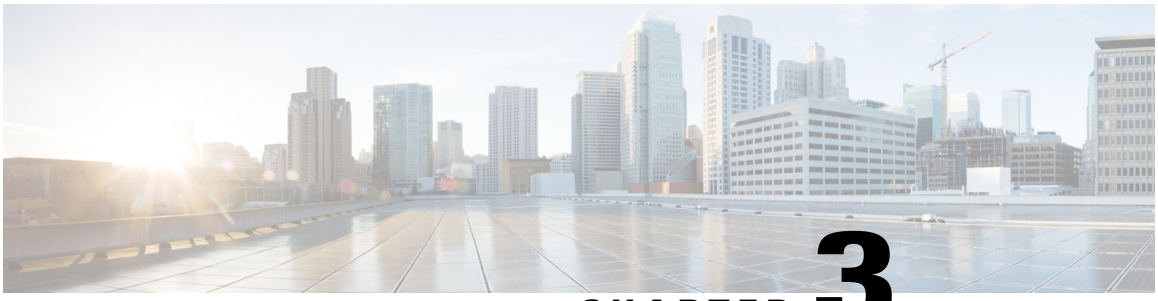
Procedure

Step 1 Select **System** > **Server**.
The **Find and List Servers** window appears.

Step 2 Select the server search parameters, and then click **Find**.
Matching records appear.

Step 3 Select the IM and Presence server that is listed in the **Find and List Servers** window.
The **Server Configuration** window appears.

Step 4 Click on the Presence Server Status link in the IM and Presence Server Information section of the **Server Configuration** window.
The **Node Details** window for the server appears.



CHAPTER 3

Cisco Unified Communications Manager Setup

This chapter provides information to find and update a Cisco Unified Communications Manager configuration or to view system component version information.

See also *Cisco Unified Serviceability Administration Guide*.

About Cisco Unified Communications Manager Setup

In Cisco Unified Communications Manager Administration, use the **System** > **Cisco Unified CM** menu path to configure Cisco Unified Communications Managers.

Use Cisco Unified Communications Manager configuration to specify the ports and other properties.

Cisco Unified Communications Manager Settings

The following table describes the Cisco Unified Communications Manager settings.

Table 2: Cisco Unified Communications Manager Settings

Field	Description
Server Information	
CTI ID	This read-only field displays the computer telephony integration (CTI) identification.
Cisco Unified Communications Manager Server	This read-only field displays the server where this Cisco Unified Communications Manager is installed.

Field	Description
Cisco Unified Communications Manager Name	Enter the name that you want to assign to this Cisco Unified Communications Manager.
Description	Enter a description of the Cisco Unified Communications Manager.The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
Location Bandwidth Manager Group	Select a Location Bandwidth Manager Group from the drop-down list.
Auto-registration Information You must configure the Universal Device Template and Universal Line Template before you configure auto-registration settings.	
Universal Device Template	Select the required Universal Device Template from the drop-down list. If no Universal Device Template is created, you can select the Default Universal Device Template.
Universal Line Template	Select the required Universal Line Template from the drop-down list. If no Universal Line Template is created, you can select the Default Universal Line Template.
Starting Directory Number	Enter the first directory number to use for autoregistration of devices. Do not begin the Starting Directory Number with a zero (0).
Ending Directory Number	Enter the last directory number to use for autoregistration of devices. Do not begin the Ending Directory Number with a zero (0). **Note** The Ending Directory Number must be greater than the Starting Directory Number which automatically enables autoregistration. Setting the starting and ending directory numbers to the same value disables autoregistration.

Field	Description
Auto-registration Disabled on this Cisco Unified Communications Manager	Cisco Unified Communications Manager disables the autoregistration by default to prevent unauthorized connections to the network. You can choose to enable or disable autoregistration by one of the following options: • To enable autoregistration for this Cisco Unified Communications Manager, uncheck the Auto-registration Disabled check box. • To disable autoregistration for this Cisco Unified Communications Manager, check the Auto-registration Disabled check box. ◦ When autoregistration is disabled, you must configure the directory numbers manually whenever you add new devices to your network. ◦ Setting the Starting Directory Number and Ending Directory Number to the same value also disables autoregistration. ◦ If starting and ending directory numbers are currently specified when you disable autoregistration by checking this option, Cisco Unified Communications Manager sets the starting and ending directory numbers to the same value. Cisco Unified Communications Manager resets the UDT and ULT information when autoregistration is disabled.
Cisco Unified Communications Manager TCP Port Settings for this Server	
Ethernet Phone Port	Cisco Unified Communications Manager uses this TCP port to communicate with the Cisco Unified IP Phones (SCCP only) on the network. • Accept the default port value of 2000 unless this port is already in use on your system. Choosing 2000 identifies this port as non-secure. • Ensure all port entries are unique. • Valid port numbers range from 1024 to 49151. • See the *Cisco Unified Communications Manager Security Guide* for information about security configurations.
MGCP Listen Port	Cisco Unified Communications Manager uses this TCP port to detect messages from its associated MGCP gateway. • Accept the default port of 2427 unless this port is already in use on your system. • Ensure all port entries are unique. • Valid port numbers range from 1024 to 49151.

Field	Description
MGCP Keep-alive Port	Cisco Unified Communications Manager uses this TCP port to exchange keepalive messages with its associated MGCP gateway. • Accept the default port of 2428 unless this port is already in use on your system. • Ensure all port entries are unique. • Valid port numbers range from 1024 to 49151.
SIP Phone Port	This field specifies the port number that Cisco Unified Communications Manager uses to listen for SIP line registrations over TCP and UDP.
SIP Phone Secure Port	This field specifies the port number that Cisco Unified Communications Manager uses to listen for SIP line registrations over TLS. See the Cisco Unified Communications Manager Security Guide for information about security configurations.
Reset button	Click this button to reset all devices that belong to the same Cisco Unified CM Group as this Cisco Unified Communications Manager server. **Note** All devices in the Cisco Unified CM Group of which this server is a member get reset, not just those devices that are registered with this server.

Related Topics

Cisco Unified Communications Manager Setup , on page 35

Synchronize Cisco Unified Communications Manager with Devices

To synchronize a Cisco Unified Communications Manager that has undergone configuration changes with its corresponding registered devices, perform the following procedure, which applies 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 **System** > **Cisco Unified CM**.
The Find and List Cisco Unified CMs window displays.

Step 2 Choose the search criteria to use.

Step 3 Click **Find**.
The window displays a list of Cisco Unified CMs that match the search criteria.

Step 4 Click the Cisco Unified Communications Manager that you want to synchronize with its devices.

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**.

Related Topics

Cisco Unified Communications Manager Setup , on page 35

Activate Cisco CallManager Service

When you perform a new Cisco Unified Communications Manager installation, you must follow these steps in sequence:

1. Add the server. Cisco Unified Communications Managers automatically get added when a server gets configured.
2. Activate the Cisco CallManager service, as described in the *Cisco Unified Serviceability Administration Guide*.

A message displays if you do not follow this sequence.

Related Topics

Cisco Unified Communications Manager Setup , on page 35

Deactivate Cisco CallManager Service

You can deactivate the Cisco CallManager service in Cisco Unified Serviceability. When you deactivate the Cisco CallManager service, the Cisco Unified Communications Manager where you deactivated the service becomes inactive for use.

Note From Cisco Unified Serviceability, you can view the status of the Cisco Unified Communications Manager by accessing **Tools** > **Service Activation**.

Note When the Cisco CallManager service is deactivated, no one can make calls on that Cisco Unified Communications Manager.

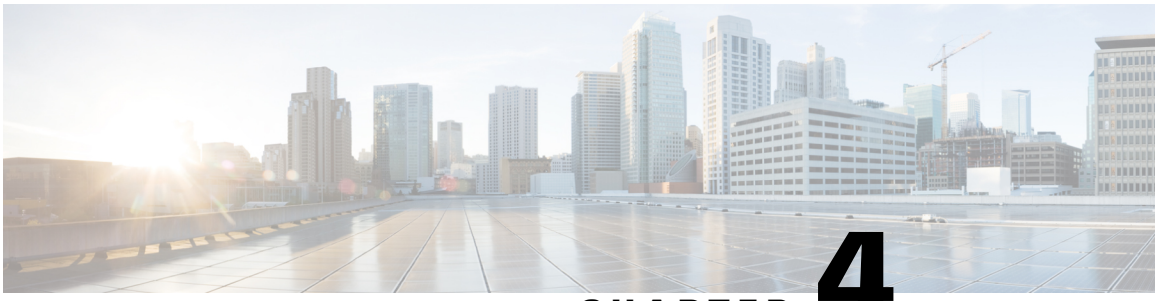
You may still be able to perform configuration operations on a deactivated Cisco Unified Communications Manager if the Cisco Communications Manager Administration web service is active and the database is up and running.

When you reactivate the Cisco CallManager service on the Cisco Unified Communications Manager, the database automatically re-creates the Cisco Unified Communications Manager by retaining the original configuration (server name or IP address). This Cisco Unified Communications Manager then becomes active; you can verify that the Cisco CallManager service is running by accessing **Tools** > **Control Center - Feature Services** in Cisco Unified Serviceability.

For more information about Service Activation, see the *Cisco Unified Serviceability Administration Guide*.

Related Topics

Cisco Unified Communications Manager Setup , on page 35



CHAPTER 4

Cisco Unified Communications Manager Group Setup

This chapter provides information to configure a Cisco Unified Communications Manager group.

About Cisco Unified Communications Manager Group Setup

In Cisco Unified Communications Manager Administration, use the **System** > **Cisco Unified CM Group** menu path to configure Cisco Unified Communications Manager groups.

A Cisco Unified Communications Manager Group specifies a prioritized list of up to three Cisco Unified Communications Managers. The first Cisco Unified Communications Manager in the list serves as the primary Cisco Unified Communications Manager for that group, and the other members of the group serve as secondary and tertiary (backup) Cisco Unified Communications Managers.

Each device pool has one Cisco Unified Communications Manager Group that is assigned to it. When a device registers, it attempts to connect to the primary (first) Cisco Unified Communications Manager in the group that is assigned to its device pool. If the primary Cisco Unified Communications Manager is not available, the device tries to connect to the next Cisco Unified Communications Manager that is listed in the group, and so on.

Cisco Unified Communications Manager Groups provide important features for your system:

- Redundancy—This feature enables you to designate a primary and backup Cisco Unified Communications Managers for each group.
- Call processing load balancing—This feature enables you to distribute the control of devices across multiple Cisco Unified Communications Managers.

For most systems, you need to have multiple groups, and you need to assign a single Cisco Unified Communications Manager to multiple groups to achieve better load distribution and redundancy.

Cisco Unified Communications Manager Group Configuration Considerations

Before configuring a Cisco Unified Communications Manager group, you must configure the Cisco Unified Communications Managers that you want to assign as members of that group.

After you have configured the Cisco Unified Communications Manager group, you can use it to configure device pools. Devices obtain their Cisco Unified Communications Manager Group list setting from the device pool to which they are assigned.

Related Topics

About Cisco Unified Communications Manager Setup , on page 35

Cisco Unified Communications Manager Group Deletion

Note You cannot delete a Cisco Unified Communications Manager group if it is assigned to any device pools or MGCP gateways or if it is the current Auto-registration Cisco Unified Communications Manager Group for the cluster.

To find out which devices are using the Cisco Unified Communications Manager group, choose Dependency Records from the Related Links drop-down list box on the Cisco Unified Communications Manager Group Configuration window and click **Go**.

If the dependency records feature is not enabled for the system, the dependency records summary window displays a message that shows the action that you can take to enable the dependency records; the message also displays information about high CPU consumption that is related to the dependency records feature.

If you attempt to delete a Cisco Unified Communications Manager group that is in use, a message displays. Before deleting a Cisco Unified Communications Manager group that is currently in use, you must perform some or all of the following tasks:

- Assign a different Cisco Unified Communications Manager group to the device pools or MGCP gateways that currently use this Cisco Unified Communications Manager group.
- Create or choose a different Cisco Unified Communications Manager group to be the Auto-registration Cisco Unified Communications Manager Group.

Related Topics

About Device Pool Setup , on page 79
Access Dependency Records , on page 982

Cisco Unified Communications Manager Group Settings

The following table describes the settings for Cisco Unified Communications Manager groups.

Table 3: Cisco Unified Communications Manager Group Settings

Field	Description
Cisco Unified Communications Manager Group Settings	

Field	Description
Name	Enter the name of the new group.
Auto-registration Cisco Unified Communications Manager Group	Check the Auto-registration Cisco Unified Communications Manager Group check box if you want this Cisco Unified Communications Manager group to be the default Cisco Unified Communications Manager group when auto-registration is enabled. Leave this check box unchecked if you do not want devices to auto-register with this Cisco Unified Communications Manager group. **Tip** Each Cisco Unified Communications Manager cluster can have only one default auto-registration group. If you choose a different Cisco Unified Communications Manager group as the default auto-registration group, that is, you check the Auto-registration Cisco Unified Communications Manager Group check box for a different Cisco Unified Communications Manager group, the previously chosen auto-registration group no longer serves as the default for the cluster; the Auto-registration Cisco Unified Communications Manager check box displays for the previously chosen group (the original default), and the check box gets disabled for the group that now serves as the default.
Cisco Unified Communications Manager Group Members	
Available Cisco Unified Communications Managers	This field displays the list of available Cisco Unified Communications Manager that are not a part of the Cisco Unified Communications Manager group. Choose the Cisco Unified Communications Manager names and use the up and down arrows to move Cisco Unified Communications Managers between the Selected list and the Available list.
Selected Cisco Unified Communications Managers	This field displays the Cisco Unified Communications Managers that are in the Cisco Unified Communications Manager group. The Selected list, which can contain up to three Cisco Unified Communications Managers, lists the Cisco Unified Communications Managers in order by highest priority. Cisco Unified Communications Managers in the Selected list become members of the group when you click **Save**. Choose the Cisco Unified Communications Manager names and use the up and down arrows to move Cisco Unified Communications Managers between the Selected list and the Available list. Within the Selected list, use the up and down arrows to arrange the groups in the Selected list in the order that you want.

Synchronize Cisco Unified Communications Manager Group Settings with Devices

To synchronize a Cisco Unified Communications Manager Group that has undergone recent configuration changes to their associated registered devices, perform the following procedure, which applies any outstanding configuration settings in the least-intrusive manner possible. (For example, a reset or restart may not be required on some affected devices.)

Procedure

Step 1 Choose **Media Resources** > **Cisco Unified CM Group**.
The Find and List Cisco Unified CM Groups window displays.

Step 2 Choose the search criteria to use.

Step 3 Click **Find**.
The window displays a list of Cisco Unified CM Groups that match the search criteria.

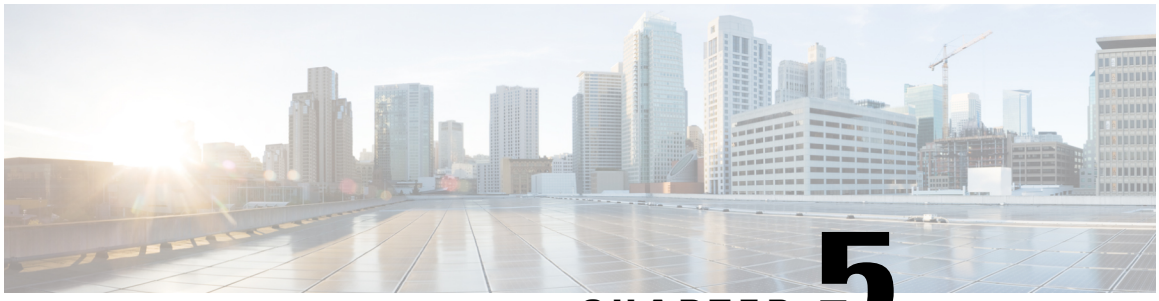
Step 4 Click the Cisco Unified CM Group that you want to synchronize with affected devices. The Cisco Unified CM Group Configuration window displays.

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**.



CHAPTER 5

Presence Redundancy Group Setup

This chapter provides information to configure a presence redundancy group for IM and Presence Service nodes in a cluster.

About Presence Redundancy Group Setup

In Cisco Unified Communications Manager Administration, use the **System** > **Presence Redundancy Groups** menu path to create a presence redundancy group consisting of two IM and Presence Service nodes from the same cluster.

For information about how to enable high availability for the presence redundancy group, or to initiate a manual node failover, fallback, and recovery, see the *Cisco Unified Communications Manager Features and Services Guide*.

Related Topics

Presence Redundancy Groups and High Availability, on page 45
Presence Redundancy Group Settings, on page 47
Set Up Presence Redundancy Groups, on page 48

Presence Redundancy Groups and High Availability

A presence redundancy group is comprised of two or more 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.

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.

Presence Redundancy Groups and High Availability Considerations

Presence Redundancy Group Interactions and Limitations

Consider the following when configuring presence redundancy groups using Cisco Unified Communications Manager 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.

Presence Redundancy Group Settings

The following table describes the settings for presence redundancy groups.

Table 4: Presence Redundancy Group Settings

Field	Description
Status	Displays the success or failure messages for save, delete, failover, fallback, and recover operations for the presence redundancy group.
Presence Redundancy Group Configuration	
Name	Enter a name for the presence redundancy group using up to 128 alphanumeric characters including underscore (_) and dash (-).
Description	(Optional) Enter a description for the presence redundancy group using up to 128 alphanumeric characters including symbols, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), forward slash (\), or angle brackets (<>).
Presence Redundancy Group Configuration	
Presence Server*	This field displays the FQDN, hostname, or IP address of the selected IM and Presence Service node that is a member of the presence redundancy group. At least one node must be selected to created a presence redundancy group. This first Presence Server field is a mandatory field that must be populated. Click the arrow to expand the drop-down list of available nodes, and use the up and down arrows to navigate the list. Only IM and Presence Service nodes that are available and are not already a part of a presence redundancy group are listed. The IM and Presence Service server must also be installed before it will display in the list. **Note** An IM and Presence Service database publisher node is automatically assigned to the DefaultCUPSubcluster group.
Presence Server	This field displays the hostname or IP address of the selected IM and Presence Service node that is a member of the presence redundancy group. You can have up to two IM and Presence Service nodes in a presence redundancy group. Click the arrow to expand the drop-down list of available nodes, and use the up and down arrows to navigate the list. Only IM and Presence Service nodes that are available and are not already a part of a presence redundancy group are listed. The IM and Presence Service server must also be installed before it will display in the list. **Note** An IM and Presence Service database publisher node is automatically assigned to the DefaultCUPSubcluster group.

Field	Description
High Availability	
Enable High Availability	When checked, this check box indicates that high availability is enabled for this presence redundancy group. Uncheck this check box to disable high availability for this group.
Monitored Server	Lists the hostnames or IP addresses of the member nodes of this presence redundancy group.
Assigned Users	Displays the number of users who are assigned to this IM and Presence Service node.
Active Users	Displays the number of users that are homed to this IM and Presence Service node in any given High Availability state. This number only changes when a High Availability event occurs in the redundancy group. In the Normal state, the active user count equals the assigned users count.
Server State	The current state of the IM and Presence Service server. For more details about presence redundancy group node states, see topics related to node state definitions, causes, and recommended actions.
Reason	The reason for the current state of the IM and Presence Service server. For more details about presence redundancy group node states, see topics related to node state definitions, causes, and recommended actions.
ServerAction	The Failover button displays if the server is in the Normal state. The Fallback button displays if the server is in the Idle or Failed Over state.
Recover	If both servers are in a failed state, the Recover button is available.
Save	Click to save the presence redundancy group with the current settings.
Delete	Click to delete the presence redundancy group.
Add New	Click to create a new presence redundancy group.

Set Up Presence Redundancy Groups

Use Cisco Unified Communications Manager Administration to assign IM and Presence Service nodes to presence redundancy groups. An IM and Presence Service node can be assigned to only one presence redundancy group. For high availability, you must assign two nodes from the same cluster to the presence redundancy group and enable high availability for the group.

Before You Begin

- At least two IM and Presence Service nodes must be configured on the same cluster for high availability.

- Make sure critical services are running on both nodes before assigning them to a presence redundancy group. You can check the IM and Presence Service server status from the Server window. If one or more critical services are not running and you checked the Enable High Availability check box for the presence redundancy group, the node will immediately fail over. If one or more critical services are not running on one of the nodes and all critical services are running on the other node, the cluster will go into a failed state as soon as you configure a presence redundancy group with high availability enabled.
- For deployments over the Wide Area Network (WAN), 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.

Procedure

Step 1 Select **System** > **Presence Redundancy Groups**.
The **Find and List Presence Redundancy Groups** window displays.

Step 2 Click **Add New**.
The **Presence Redundancy Group Configuration** window displays.

Step 3 In the **Presence Redundancy Group Configuration** panel, perform the following actions:

a) Enter a unique name for the presence redundancy group in the Name field. You can enter a maximum of 128 alphanumeric characters, including underscore (_) and dash (-).
b) (Optional) Enter a description of the group in the Description field. You can enter a maximum of 128 alphanumeric characters including symbols, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), forward slash (\), or angle brackets (<>).
c) Select two different IM and Presence Service nodes in the Presence Server fields to assign them to the group.
Only servers that are installed and unassigned display in the Presence Server fields.

Note (Optional) You can check the Enable High Availability check box to enable high availability for the presence redundancy group. See topics related to enabling high availability for more information.

Step 4 Click **Save**.

Related Topics

Presence Redundancy Group Settings, on page 47

Enable or Disable High Availability

Use Cisco Unified Communications Manager Administration 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 will fail 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 will not move these users back to the primary node; they remain on the backup node.
- See the *Deployment Guide for 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 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 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**.

Delete Presence Redundancy Group

Use Cisco Unified Communications Manager Administration to delete an existing presence redundancy group from the cluster.

Observe the following restrictions:

- You cannot remove a server from a presence redundancy group if users are assigned to the server.
- You cannot delete a presence redundancy group if there are servers assigned to the presence redundancy group.

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 Choose one of the following delete procedures:

a) Check the check box beside the presence redundancy group that is listed in the search results, and then click **Delete Selected**.

b) Select the presence redundancy group that is listed in the search results. The **Presence Redundancy Group Configuration** window appears.
Click **Delete**.

c) Click **OK** to delete this presence redundancy group or click **Cancel** continue without deleting the presence redundancy group.

View Presence Redundancy Group Node Status

Use Cisco Unified Communications Manager Administration to view the status of IM and Presence Service nodes that are members of a presence redundancy group.

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 a presence redundancy group that is listed in the search results.
The **Presence Redundancy Group Configuration** window appears. If two servers are configured in that group and high availability is enabled, then the status of the nodes within that group are displayed in the High Availability panel.

Node State Definitions

The following table describes the different states for IM and Presence Service nodes in a presence redundancy group.

Table 5: 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 Cisco Unified Communications Manager Administration.
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 Cisco Unified Communications Manager Administration.
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 Cisco Unified Communications Manager Administration.
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.

State	Description
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 nodes in a presence redundancy group on the **Presence Redundancy Group Configuration** window when you select a group using Cisco Unified Communications Manager Administration.

The following table lists the high-availability states for both IM and Presence Service nodes in a presence redundancy group and describes the reasons for the state, the state causes, and recommended actions.

Table 6: Node High-Availability States, Causes and Recommended Actions

Node 1		Node 2		
State	**Reason**	**State**	**Reason**	**Cause/Recommended Actions**
Normal	Normal	Normal	Normal	High Availability is running on both nodes in the presence redundancy group. The presence redundancy group is operating normally and is not in failover mode. Critical services on both nodes are running.
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.

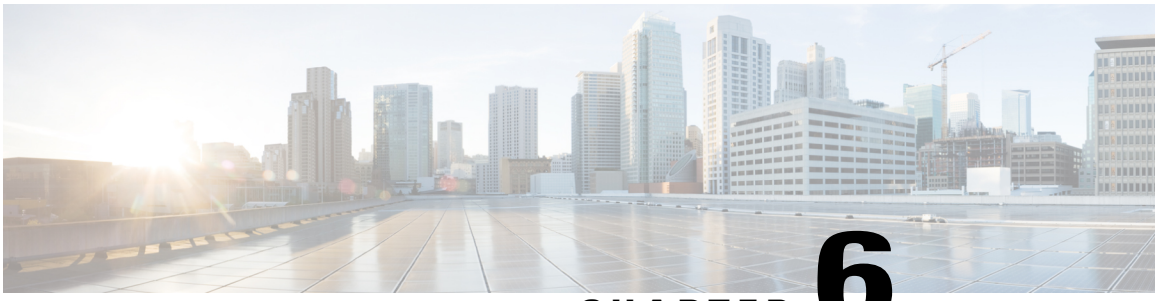
Node 1		Node 2		
State	**Reason**	**State**	**Reason**	**Cause/Recommended Actions**
Idle	On Admin Request	Running in Backup Mode	Initialization	The administrator restarts the SRM service on node 2 while node 2 is running in backup mode, but before the heartbeat on node 1 times out.
Failing Over	On Admin 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.

Node 1		Node 2		
State	**Reason**	**State**	**Reason**	**Cause/Recommended Actions**
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.
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, select **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.

Node 1		Node 2		
State	**Reason**	**State**	**Reason**	**Cause/Recommended Actions**
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, select **Recovery** in the Presence Redundancy Group Configuration window. **2** If the critical services do not start, reboot the node.
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. Select **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		Node 2		
State	**Reason**	**State**	**Reason**	**Cause/Recommended Actions**
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.
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. Select **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. Select **Recovery** in the Presence Redundancy Group Configuration window. If the problem persists, then reboot the nodes.

Node 1		Node 2		
State	**Reason**	**State**	**Reason**	**Cause/Recommended Actions**
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:** Select **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.
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.



CHAPTER 6

Phone NTP Reference Setup

This chapter provides information to configure phone NTP references.

About Phone NTP Reference Setup

In Cisco Unified Communications Manager Administration, use the **System** > **Phone NTP Reference** menu path to configure phone NTP references.

If you want to do so, you can configure phone Network Time Protocol (NTP) references in Cisco Unified Communications Manager Administration to ensure that a phone that is running SIP gets its date and time from the NTP server. If all NTP servers do not respond, the phone that is running SIP uses the date header in the 200 OK response to the REGISTER message for the date and time.

After you add the phone NTP reference to Cisco Unified Communications Manager Administration, you must add it to a date/time group. In the date/time group, you prioritize the phone NTP references, starting with the first server that you want the phone to contact.

The date/time group configuration gets specified in the device pool, and the device pool gets specified on the phone page.

Phone NTP References Setup Tips

After you add a new phone NTP reference to the Cisco Unified Communications Manager database, assign it to a date/time group.

Related Topics

About Date and Time Group Setup , on page 63

Phone NTP Reference Deletion

Before you can delete the phone NTP reference from Cisco Unified Communications Manager Administration, you must delete the phone NTP reference from the date/time group. To find which date/time groups use the phone NTP reference, choose **Dependency Records** from the Related Links drop-down list box in the Phone NTP Reference Configuration window and click **Go**. When you know which date/time groups use the phone NTP reference, you can then remove that phone NTP reference from that group.

If the dependency records feature is not enabled for the system, the dependency records summary window displays a message that shows the action that you can take to enable the dependency records; the message also displays information about high CPU consumption that is related to the dependency records feature.

Related Topics

Access Dependency Records , on page 982

Phone NTP Reference Settings

The following table describes the phone NTP reference settings.

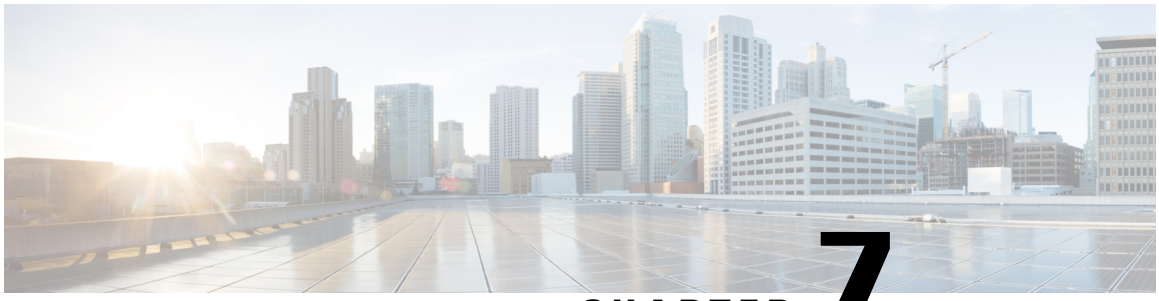
Table 7: Phone NTP Reference Settings

Field	Description
IP Address	Enter the IP address of the NTP server that you want the phone that is running SIP to use to get its date and time. **Note** Cisco Unified Communications Manager cannot be configured as Phone NTP References.
Description	Enter a description for the phone NTP reference. Cisco Unified Communications Manager Administration automatically propagates the information in the IP Address field to the Description field. If you want to do so, you can change the information.

Field	Description
Mode	From the drop-down list box, choose the mode for the phone NTP reference. The values from which you can choose follow: • Directed Broadcast—If you choose this default NTP mode, the phone accesses date/time information from any NTP server but gives the listed NTP servers (1st = primary, 2nd = secondary) priority. For example, if the phone configuration contains NTP servers where A = primary NTP server and B = secondary/backup NTP server, the phone uses the broadcast packets (derives the date/time) from NTP server A. If NTP server A is not broadcasting, the phone accesses date/time information from NTP server B. If neither NTP server is broadcasting, the phone accesses date/time information from any other NTP server. If no other NTP server is broadcasting, the phone will derive the date/time from the Cisco Unified Communications Manager 200 OK response to the REGISTER message. • Unicast—If you choose this mode, the phone will send an NTP query packet to that particular NTP server. If the phone gets no response, the phone will access date/time information from any other NTP server. If no other NTP servers respond, the phone will derive the date/time from the Cisco Unified Communications Manager 200 OK response to the REGISTER message. **Note** Cisco Unified Communications Manager currently does not support the Multicast and Anycast modes. If you choose either of these modes, Cisco Unified Communications Manager will default to the Directed Broadcast mode.

Related Topics

Phone NTP Reference Setup , on page 59



CHAPTER 7

Date and Time Group Setup

This chapter provides information to add, update, or delete Date/Time Groups, and to synchronize configuration changes with affected devices.

About Date and Time Group Setup

In Cisco Unified Communications Manager Administration, use the **System** > **Date/Time Group** menu path to configure date and time groups.

Use Date/Time Groups to define time zones for the various devices that are connected to Cisco Unified Communications Manager. Each device exists as a member of only one device pool, and each device pool has only one assigned Date/Time Group.

Installing Cisco Unified Communications Manager automatically configures a default Date/Time Group that is called CMLocal. CMLocal synchronizes to the active date and time of the operating system on the server where Cisco Unified Communications Manager is installed. After installing Cisco Unified Communications Manager, you can change the settings for CMLocal as desired. Normally, adjust server date/time to the local time zone date and time.

Note CMLocal resets to the operating system date and time whenever you restart Cisco Unified Communications Manager or upgrade the Cisco Unified Communications Manager software to a new release. Do not change the name of CMLocal.

Tip For a worldwide distribution of Cisco Unified IP Phones, create one named Date/Time Group for each of the time zones in which you will deploy endpoints.

Add Phone NTP Reference to SIP Phones in Date and Time Group

Use the following procedure to add a phone NTP reference to a date/time group for a phone that is running SIP.

Procedure

Step 1 To add a phone NTP reference to a date/time group for a phone that is running SIP, perform the following tasks:

Note To get its date and time, a phone that is running SIP can use NTP server(s) that exist in Cisco Unified Communications Manager Administration.

a) Click the **Add Phone NTP References** button.

b) Find the phone NTP reference(s) that you want to add.
Only phone NTP references that exist in the Cisco Unified Communications Manager database display.

c) After the search results display, check the check boxes for any phone NTP references that you want to add to the date/time group or click **Select All**.

d) Click **Add Selected**.

Tip After you add the phone NTP reference(s) to the date/time group, you can prioritize them, starting with the first server that you want the phone that is running SIP to contact. For example, to move a server to the top of the list, highlight the entry in the pane and click the Up arrow. To move a server to the bottom of the list, highlight the entry in the pane and click the Down arrow.

Step 2 To remove a phone NTP reference from the date/time group, highlight the reference in the pane and click **Remove Phone NTP References**.
Removing the phone NTP reference from the date/time group does not remove the phone NTP reference from the Cisco Unified Communications Manager database.

Step 3 To save the new date/time group in the database, click the **Save** icon that displays in the tool bar in the upper, left corner of the window (or click the **Save** button that displays at the bottom of the window).

Note See the procedure to synchronize a Date/Time group with affected devices before deciding on whether to proceed to the next step.

Step 4 To reset the devices that use the date/time group, click **Reset**.

What to Do Next

After adding a new date/time group to the database, you can assign it to a device pool to configure the date and time information for that device pool.

Related Topics

Phone NTP Reference Setup , on page 59
About Phone NTP Reference Setup , on page 59
Synchronize Date and Time Group Settings with Devices , on page 66
About Device Pool Setup , on page 79

Date and Time Group Deletion

Note You cannot delete a date/time group that any device pool uses.

To find out which device pools use the date/time group, choose **Dependency Records** from the Related Links drop-down list box on the Date/Time Group Configuration window and click **Go**.

If the dependency records feature is not enabled for the system, the dependency records summary window displays a message that shows the action that you can take to enable the dependency records; the message also displays information about high CPU consumption that is related to the dependency records feature.

If you attempt to delete a date/time group that is in use, Cisco Unified Communications Manager displays a message. Before deleting a date/time group that is currently in use, you must perform either or both of the following tasks:

- Assign a different date/time group to any device pools that use the date/time group that you want to delete.
- Delete the device pools that use the date/time group that you want to delete.

Related Topics

About Device Pool Setup , on page 79
Device Pool Deletion , on page 80
Access Dependency Records , on page 982

Date and Time Group Settings

The following table describes the date/time group settings.

Table 8: Date/Time Group Settings

Field	Description
Date/Time Group Information	
Group Name	Enter the name that you want to assign to the new date/time group.
Time Zone	From the drop-down list box, choose the time zone for the group that you are adding. The default setting for new Cisco Unified Communications Manager installations equals (GMT) Monrovia, Casablanca. If you upgrade from a compatible Cisco Unified Communications Manager release and you use “local time zone of Communications Manager” in the configuration, the Cisco Unified Communications Manager database determines the appropriate time zone for the database server and then displays that time zone as replacement for the Communications Manager time zone.

Field	Description
Separator	Choose the separator character to use between the date fields.
Date Format	Choose the date format for the date that displays on the Cisco Unified IP Phones.
Time Format	Choose a 12-hour or 24-hour time format.
Phone NTP References for this Date/Time Group	
Selected Phone NTP References (ordered by highest priority)	To ensure that a phone that is running SIP gets its date and time configuration from an NTP server, add the phone NTP reference(s) to the date/time group. To add a phone NTP reference to the date/time group, perform the following tasks: **1** Click the **Add Phone NTP References** button. **2** Find the phone NTP reference(s) that you want to add. Only phone NTP references that exist in the Cisco Unified Communications Manager database display. **3** After the search results display, check the check boxes for the phone NTP references or click **Select All**. **4** Click **Add Selected**. After you add the phone NTP reference(s) to the date/time group, you can prioritize them, starting with the first reference that you want the phone to contact. For example, to move a reference to the top of the list, highlight the entry in the pane and click the Up arrow. To move a reference to the bottom of the list, highlight the entry in the pane and click the Down arrow. **Tip** To remove a phone NTP reference from the date/time group, highlight the server in the pane and click **Remove Phone NTP References**. Removing the phone NTP reference from the date/time group does not remove the phone NTP reference from the Cisco Unified Communications Manager database.

Related Topics

About Phone NTP Reference Setup , on page 59
Date and Time Group Setup , on page 63

Synchronize Date and Time Group Settings with Devices

To synchronize devices to a date/time group that has undergone configuration changes, perform the following procedure, which applies 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 **System** > **Date/Time Group**.
The Find and List Date/Time Groups window displays.

Step 2 Choose the search criteria to use.

Step 3 Click **Find**.
The window displays a list of Date/Time Groups that match the search criteria.

Step 4 Click the Date/Time Group to which you want to synchronize applicable devices.
The Date/Time Group Configuration window displays.

Step 5 Make any additional configuration changes.

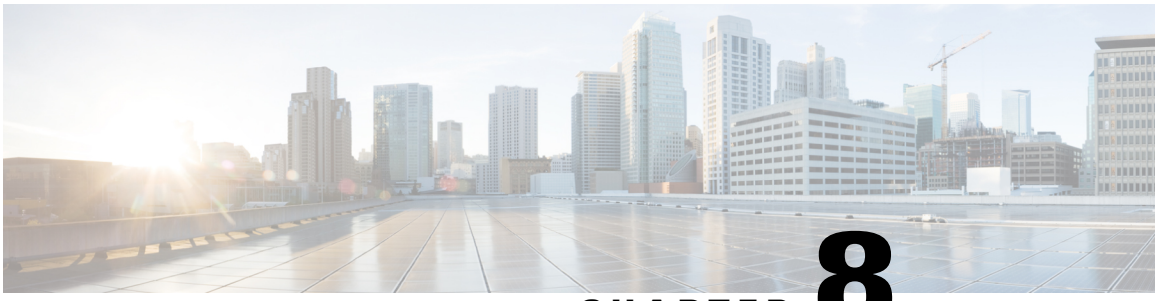
Step 6 Click **Save**.

Step 7 Click **Apply Config**.
The **Apply Configuration Information** dialog displays.

Step 8 Click **OK**.

Related Topics

Date and Time Group Setup , on page 63



CHAPTER 8

Region Setup

This chapter provides information to add, update, or delete regions, and synchronize configuration changes with affected devices.

For additional information, see topics related to regions in the *Cisco Unified Communications Manager System Guide*, as well as topics related to Call Admission Control in the *Cisco Unified Communications Manager System Guide*.

Audio Codec Preference List

In Cisco Unified Communications Manager (Unified CM) Administration, use the **System > Region Information > Audio Codec Preference** menu path to configure the order of audio codec preference, both for calls within a region and for between regions.

Unified CM has two default Audio Codec Preference lists, one for lossy regions and another for low-loss regions. These are the Factory Default lossy, and the Factory Default low loss. Start with a default Audio Codec Preference list to create a custom list.

With the Audio Codec Preference feature, you can:

- Change the relative priorities of audio codecs.
- Save the custom Audio Codec Preference list with a unique name.
- Assign custom codec preference lists for use within a region or between regions.

- Create multiple custom codec preference list.

Related Topics

Create New Audio Codec Preference List , on page 70
Edit Audio Codec Preference List , on page 70
Delete Audio Codec Preference List , on page 71

Create New Audio Codec Preference List

Procedure

Step 1 Click **Add New** from the **Find and List Audio Codec Preference lists** page.
The **Audio Codec Preference List Configuration** page is displayed.

Step 2 Choose an Audio Codec Preference list from the dropdown list.

Step 3 Click **Copy**.

Step 4 In the **Audio Codec Preference List Information** section, enter a Name and Description.

Step 5 Place the codecs in the preferred order by using the up and down arrows.

Step 6 Click **Save**.

Related Topics

Edit Audio Codec Preference List , on page 70
Delete Audio Codec Preference List , on page 71

Edit Audio Codec Preference List

Procedure

Step 1 In the **Audio Codec Preference** lists section, click the list to be edited.
The **Audio Codec Preference List Configuration** page is displayed.

Step 2 Reorder the audio codecs using the up and down arrows.

Step 3 Click **Save**.

Related Topics

Create New Audio Codec Preference List , on page 70
Delete Audio Codec Preference List , on page 71

Delete Audio Codec Preference List

Note You cannot delete the Factory Default lossy or low loss audio codec preference lists.

Procedure

Step 1 Select the list to be deleted from the **Audio Codec Preference lists** section.

Step 2 Click **Delete Selected**.
A message box appears "You are about to permanently delete one or more Audio Codec Preference Lists. This action cannot be undone. Continue?"

Step 3 Click **OK**.

Related Topics

Create New Audio Codec Preference List , on page 70
Edit Audio Codec Preference List , on page 70

About Region Setup

In Cisco Unified Communications Manager Administration, use the **System** > **Region** menu path to configure regions.

You use regions to limit the bandwidth that is used for audio and video calls within a region and between existing regions by specifying the transport-independent maximum bit rates for audio and for video calls. You can specify the maximum bit rates for audio and video calls within a region and between existing regions.

- The maximum audio bit rate determines the codecs that are allowed for calls by filtering out codecs with bit rates that exceed the specified limit.
- The maximum video call bit rate comprises the sum of the audio and video bit rates, but does not include transport overhead.

Cisco Unified Communications Manager supports up to 2000 regions. The following limitations and restrictions apply:

- Configure as many regions as possible to Use System Default for the audio bit rate and video call bit rate fields.
- This enhancement requires a virtual machine OVA with a capacity of 7500 users or larger.
- See the "Regions" subtopic under the "Administration Considerations" topic of the "IP Video Telephony" chapter of the *Cisco Unified Communications Solution Reference Network Design (SRND)* for the current release, which provides recommendations as to how the video bandwidth should be set for regions and locations, so the video portion of video calls will succeed, and the video calls will not get rejected nor set up as audio-only calls.

Regions Setup Tips

For every region, an association exists with that region in other regions; therefore, the addition of regions occurs in a matrixlike fashion. For example, if you add regions A, B, and C, a matrix with region A, region B, and region C as both columns and rows results, as shown in the following matrix:

	Region A	Region B	Region C
Region A			
Region B			
Region C			

If you assign 20 regions, the database adds 400 entries (20 x 20). Some performance limitations exist when large numbers of regions are assigned.

Note Cisco Unified Communications Manager allows you to add up to 2000 regions.

Note Cisco recommends that you reset devices after changing a region name.

Set Up Regions

Follow these additional steps when configuring regions.

Procedure

Step 1 To configure the settings to use within a particular region, click the name of this region to highlight it in the Regions window pane; then, configure the settings, as described in Table 9: Region Settings , on page 73.

Step 2 To configure the default codecs to use between this region and other regions, click another region name (other than this region) to highlight it in the Regions window pane. Then, configure the settings, as described in Table 9: Region Settings , on page 73.

Tip For enhanced scalability and to conserve resources, Cisco recommends that you properly set the default values in the Clusterwide Parameters (System - Location and Region) section of the Cisco Unified Communications Manager Administration Service Parameters Configuration window for the audio codec, video call bandwidth, and link loss type values and then choose the Use System Default entries in the Cisco Unified Communications Manager Administration Region Configuration window for these fields.

Step 3 To save the new region in the database, click **Save**.

Tip The Find and List Regions window displays an Rows per page drop-down list box that allows you to list 25, 50, 100, 150, 200, or 250 configured regions. If you choose to display 100 or more regions, Cisco Unified Communications Manager may experience performance degradation.

What to Do Next

After you configure a region, you can use it to configure device pools. Devices acquire a region setting from the device pool to which they are assigned.

Related Topics

Audio and Video Call Bit Rate Settings , on page 73
About Device Pool Setup , on page 79

Region Deletion

Note You cannot delete a region that any device pools are using.

To find out which device pools use the region, choose Dependency Records from the Related Links drop-down list box on the Region Configuration window and click Go.

If the dependency records feature is not enabled for the system, the dependency records summary window displays a message that shows the action that you can take to enable the dependency records; the message also displays information about high CPU consumption that is related to the dependency records feature.

If you attempt to delete a region that is in use, Cisco Unified Communications Manager displays a message. Before deleting a region that is currently in use, you must perform either or both of the following tasks:

- Update the device pools to use a different region.
- Delete the device pools that use the region that you want to delete.

Tip The Find and List Regions window displays an Items per page drop-down list box that allows you to list 25, 50, 100, 150, 200, or 250 configured regions. If you choose to display 100 or more regions, Cisco Unified Communications Manager may experience performance degradation.

Related Topics

About Device Pool Setup , on page 79
Device Pool Deletion , on page 80
Access Dependency Records , on page 982

Audio and Video Call Bit Rate Settings

The following table summarizes the audio bit rate and video call bit rate settings that can be specified for regions.

Table 9: Region Settings

Field	Description
Region Information	

Field	Description
Name	Enter a unique name for this region. This name can comprise up to 30 characters. Valid characters include letters, numbers, dashes, dots (periods), blanks, and underscores. **Note** Cisco recommends that you reset devices after changing a region name.
Region Relationships	
Region	The entries in this column display all regions for which non-default relationships have been configured. **Note** If the relationships between the region that you are configuring and this region specify only default values, this region does not display in this column.
Audio Codec Preference List	The entries in this column specify the audio codec preference relationship between the region that you are configuring and the region that displays in the corresponding row.
Maximum Audio Bit Rate	The entries in this column specify the maximum audio bit rate between the region that you are configuring and the region that displays in the corresponding row.
Maximum Session Bit Rate for Video Calls	The entries in this column specify the maximum video bit rate (including audio) between the region that you are configuring and the region that displays in the corresponding row.
Maximum Session Bit Rate for Immersive Video Calls	The entries in this column specify the maximum immersive video bit rate (including audio) between the region that you are configuring and the region that displays in the corresponding row.
Modify Relationship to other Regions	
Regions	The entries in this window pane specify all existing regions, including the Default region, the region that you are configuring, and all other regions. Choose a region in this pane prior to configuring the relationships between the region that you are configuring and the chosen region.

Field	Description
Audio Codec Preference List	For each region that is specified in the Regions window pane, choose the corresponding value from the drop-down list box in this column to set the Audio Codec Preference list describing the network conditions between this region and the specified region. The Audio Codec Preference list determines the relative preferences for certain audio codecs, optimizing the audio quality based on whether or not the network conditions are lossy. Certain audio codecs are more robust when faced with packet loss, jitter, and delay. Choose from the following values: • Keep Current Setting—Choose this value to keep the link loss type between the region that you are configuring and the region that you specified in the Regions window pane. • Use System Default—Choose this value to use the system default value for link loss type between the region that you are configuring and the region that you specified in the Regions window pane. (System default is set in the Service Parameters Configuration window.) • Factory Default Low Loss—Choose this value to specify a low-loss link loss type between the region that you are configuring and the region that you specified in the Regions window pane. • Factory Default Lossy—Choose this value to specify a lossy link loss type between the region that you are configuring and the region that you specified in the Regions window pane. • <Custom Audio Codec Preference list>—Choose a custom Audio Codec Preference list that you have created. **Caution** Custom audio codec preferences must be configured identically in both clusters for H.323 Intercluster Trunks (ICTs). Inconsistent audio codec preferences may result in calls with no audio.

Field	Description
Maximum Audio Bit Rate	For each region that is specified in the Regions window pane, choose the value from the drop-down list box in this column to set the maximum bit rate to use for audio between this region and the specified region. This setting applies to both audio and video calls and serves as an upper limit for the audio bit rate, which means that audio codecs with higher bit rates than the one that you specify are not used for these calls. For example, if you choose 64 kbps (G.722, G.711), G.722 or G.711 may get negotiated for the calls because both codecs use 64 kb/s. G.722 has better audio quality than G.711, so it is preferred for a call. • Cisco recommends that you update the intraregion and interregion maximum audio bit rate service parameters. In addition, Cisco recommends that Use System Default option be chosen for this field. Configuring and using the service parameter values facilitates the modification of the Max Audio Bit Rate for many region pairs at one time. • Because of bandwidth constraints at most remote-site deployments, use 8 kb/s (G.729) as the recommended setting between a new region and existing regions. • If you choose Keep Current Setting, you keep the value that is specified in the Regions Relationships pane for the region pair that you are creating. • If you choose Use System Default, the value for the Intraregion or Interregion Max Audio Bit Rate service parameter gets used, depending on the region that is selected. This service parameter supports the Cisco CallManager service.
Maximum Session Bit Rate for Video Calls	For each region that is specified in the Regions window pane, click one radio button in this column as specified: • Keep Current Setting—Click this button to use the current setting for the video call bandwidth. • Use System Default—Click this button to use the default value. The default value normally specifies 384 kbps, unless the default value has been set to a different value in the Service Parameters Configuration window. • None—Click this radio button if no video call bit rate is allotted between this region and the specified region. If you choose this option, the system does not allow video calls. • kbps—Click this button to set the maximum video call bit rate between the region that you are configuring and the specified region. Enter the bit rate that is available for each video call between these two regions; remember that the audio bit rate is included. Valid values range from 1 to 32256.

Field	Description
Maximum Session Bit Rate for Immersive Video Calls	For each region that is specified in the Regions window pane, click one radio button in this column as specified: • Keep Current Setting—Click this button to use the current setting for the immersive video call bandwidth. • Use System Default—Click this button to use the default value. The default value normally specifies 2000000000 kbps, unless the default value has been set to a different value in the Service Parameters Configuration window. • None—Click this radio button if no immersive video call bit rate is allotted between this region and the specified region. If you choose this option, the system does not allow immersive video calls. • kbps—Click this button to set the maximum immersive video call bit rate between the region that you are configuring and the specified region. Enter the bit rate that is available for each immersive video call between these two regions; remember that the audio bit rate is included. Valid values range from 1 to 2147483647.

Related Topics

Region Setup , on page 69

Synchronize Region Settings with Devices

To synchronize devices with a Region that has undergone configuration changes, perform the following procedure, which applies 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 **System** > **Region**.
The Find and List Regions window displays.

Step 2 Choose the search criteria to use.

Step 3 Click **Find**.
The window displays a list of Regions that match the search criteria.

Step 4 Click the Region to which you want to synchronize applicable devices.
The Find and List Regions window displays.

Step 5 Make any additional configuration changes.

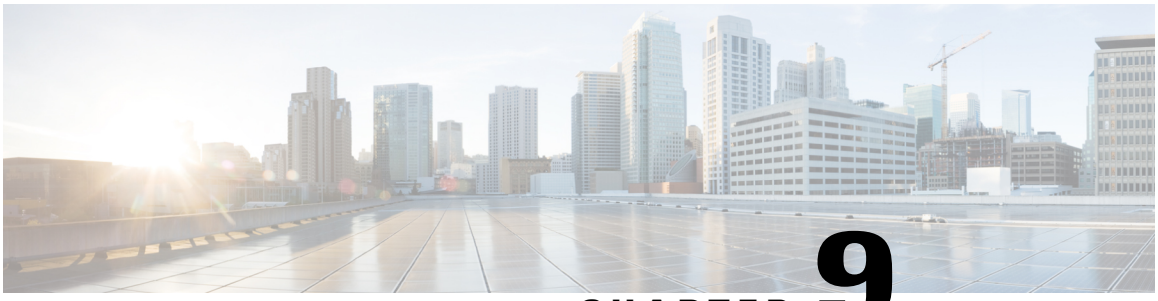
Step 6 Click **Save**.

Step 7 Click **Apply Config**.
The Apply Configuration Information dialog displays.

Step 8 Click **OK**.

Related Topics

Region Setup , on page 69



CHAPTER 9

Device Pool Setup

This chapter provides information to add, update, or delete a device pool.

See topics related to system-level configuration settings in the *Cisco Unified Communications Manager System Guide* for more information about device pools and the device settings that are assigned through device pools, as well as topics related to common device configuration.

About Device Pool Setup

In Cisco Unified Communications Manager Administration, use the **System** > **Device Pool** menu path to configure device pools.

Device pools define sets of common characteristics for devices. The device pool structure supports the separation of user and location information. The device pool contains system, device, and location-related information. The Common Device Configuration window under **Device** > **Device Settings** > **Common Device Configuration** records all the user-oriented information such as type of softkey template that is used and locale information. Ensure that each device is associated with a device pool and with a common device configuration for user-oriented information.

Device Pool Setup Tips

After adding a new device pool to the database, you can use it to configure devices such as Cisco Unified IP Phones, gateways, conference bridges, transcoders, media termination points, voice-mail ports, CTI route points, and so on.

Before you configure a device pool, you must configure the following items if you want to choose them for the device pool:

- Cisco Unified Communications Manager group (required).
- Date/time group (required).
- Region (required).

- SRST reference (optional).
- Media resource group list (optional).
- Calling search space for auto-registration (optional).
- Reverted call focus priority (optional).
- Device mobility group (optional).
- Wireless LAN Profile Group (optional).

Note You can specify the Wireless LAN Profile Group at the Device Pool level or the individual phone level.

- Wi-Fi Hotspot Profile (optional).

Note You can specify the Wi-Fi Hotspot Profile at the Device Pool level or the individual phone level.

- Device mobility calling search space.
- Physical location (optional). See topics related to configuring a device mobility group in the *Cisco Unified Communications Manager Features and Services Guide*.
- Location.
- AAR group.
- AAR calling search space.

Related Topics

About Cisco Unified Communications Manager Group Setup , on page 41
About Date and Time Group Setup , on page 63
About Region Setup , on page 71
About Location Setup , on page 127
About SRST Reference Setup , on page 135
About AAR Group Setup , on page 171
About Calling Search Space Setup , on page 273
About Media Resource Group List Setup , on page 399

Device Pool Deletion

You cannot delete a device pool if any devices are assigned to it, if it is used for Device Defaults configuration, or if it is the only device pool in the database. If you try to delete a device pool that is in use, a message displays. Before deleting a device pool that is currently in use, you must perform either or both of the following tasks:

- Update the devices to assign them to a different device pool.

- Delete the devices that are assigned to the device pool that you want to delete.

Related Topics

Phone Setup , on page 581

Device Pool Settings

The following table lists and describes device pool settings.

Table 10: Device Pool Settings

Field Name	Description
Device Pool Settings	
Device Pool Name	Enter the name of the new device pool that you are creating. You can enter up to 50 characters, which include alphanumeric characters, periods (.), hyphens (-), underscores (_), and blank spaces.
Cisco Unified Communications Manager Group	Choose the Cisco Unified Communications Manager group to assign to devices in this device pool. A Cisco Unified Communications Manager group specifies a prioritized list of up to three Cisco Unified Communications Managers. The first Cisco Unified Communications Manager in the list serves as the primary Cisco Unified Communications Manager for that group, and the other members of the group serve as backup Cisco Unified Communications Managers for redundancy.
Calling Search Space for Auto-registration	Choose the calling search space to assign to devices in this device pool that auto-register with Cisco Unified Communications Manager. The calling search space specifies partitions that devices can search when attempting to complete a call.
Adjunct CSS	From the drop-down list box, choose an existing Calling Search Space (CSS) to use for the devices in this device profile as an adjunct CSS for the Extension Mobility Cross Cluster (EMCC) feature. (To configure a new CSS or modify an existing CSS, choose **Call Routing** > **Class of Control** > **Calling Search Space** in Cisco Unified Communications Manager Administration.) Default value specifies None. When configuring the EMCC feature, the administrator must configure a device pool for each remote cluster. If the remote cluster is located in a different country, the adjunct CSS must embrace the partition with which the emergency patterns of that country associate. This configuration facilitates country-specific emergency call routing. For more information about the adjunct CSS, see topics related to EMCC call routing in the *Cisco Unified Communications Manager Features and Services Guide*.

Field Name	Description
Reverted Call Focus Priority	Choose a clusterwide priority setting for reverted calls that are invoked by the hold reversion feature. This setting specifies which call type, incoming calls or reverted calls, have priority for user actions, such as going off hook. • Default—If you choose this option, incoming calls have priority. • Highest—If you choose this option, reverted calls have priority. 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. **Note** This setting applies specifically to hold reverted calls; it does not apply to parked reverted calls. For more information, see topics related to hold reversion in the *Cisco Unified Communications Manager Features and Services Guide*.
Intercompany Media Services Enrolled Group	Select an Intercompany Media Services Enrolled Group from the drop-down list. For more information, see the *Cisco Intercompany Media Engine Installation and Configuration Guide*.

Field Name	Description
Local Route Group Settings The Local Route Group Settings enables you to associate the route groups that you add under **Call Routing** > **Route/Hunt** > **Route Group** with the local route groups that you configure on the Local Route Group Names window for any particular device pool. To associate a route group with the local route group for any particular device pool, choose the relevant route group from the drop-down list box. Select the default value <None> to prevent implementation of the Local Route Group feature. **Note** The Standard Local Route Group entry on the left is a default field entry which is populated from pre-10.0(1) release input. This field name may vary depending on the local route group name that you specify in the Local Route Group Names window under **Call Routing** > **Route/Hunt** > **Local Route Group Names** menu path in Cisco Unified Communications Manager Administration. You can add multiple local route group names in the Local Route Group Names window. The Local Route Group Settings window will display them as noneditable fields. **Tip** To configure the local route group names in the Local Route Group Names window, use the **Call Routing** > **Route/Hunt** > **Local Route Group Names** menu path in Cisco Unified Communications Manager Administration. You can define site-specific local route groups (like primary local route group, secondary local route group, tertiary local route group, and so on) when you configure multiple local route groups under **Call Routing** > **Route/Hunt** > **Local Route Group Names**. For example, you can add multiple local route groups such as Emergency Route Group, Primary Local Route Group (for site A), Secondary Local Route Group (for site A), Primary Local Route Group (for site B), and Secondary Local Route Group (for site B). The Local Route Group feature enables you to specify different route groups for each site (site A and site B) for the respective device pool. Also, you can define a separate call routing option for emergency calls when you associate the Emergency Route Group with a different route group. Hence you can easily define separate call routing options for emergency calls and PSTN calls. See the *Cisco Unified Communications Manager Features and Services Guide* for additional information about Local Route Group feature.	
Roaming Sensitive Settings	
Date/Time Group	Choose the date/time group to assign to devices in this device pool. The date/time group specifies the time zone and the display formats for date and time.
Region	Choose the Cisco Unified Communications Manager region to assign to devices in this device pool. The Cisco Unified Communications Manager region settings specify voice codec that can be used for calls within a region and between other regions.
Media Resource Group List	From the drop-down list box, choose a media resource group list. A media resource group list specifies a prioritized list of media resource groups. An application selects the required media resource (for example, a music on hold server, transcoder, or conference bridge) from the available media resource groups according to the priority order that is defined in a media resource group list.

Field Name	Description
Location	Use locations to implement call admission control (CAC) in a centralized call-processing system. CAC enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location. From the drop-down list box, choose the appropriate location for this device pool. A location setting of None or Hub_None means that the locations feature does not keep track of the bandwidth that the devices in this device pool consume. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the **System** > **Location** menu option. For an explanation of location-based CAC across intercluster trunks, see topics related to location-based CAC in the *Cisco Unified Communications Manager System Guide*.
Network Locale	From the drop-down list box, choose the locale that is associated with phones and gateways. The network locale contains a definition of the tones and cadences that the phones and gateways in the device pool in a specific geographic area use. Make sure that you select a network locale that is supported by all of the phones and gateways that use this device pool. **Note** If the user does not choose a network locale, the locale that is specified in the Cisco Unified Communications Manager clusterwide parameters as Default Network Locale applies. **Note** 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. If a device is associated with a network locale that it does not support in the firmware, the device will fail to come up.
SRST Reference	From the drop-down list box, choose a survivable remote site telephony (SRST) reference to assign to devices in this device pool. Choose from the following options: • Disable—If you choose this option, devices in this device pool will not have SRST reference gateways that are available to them. • Use Default Gateway—If you choose this option, devices in this device pool use the default gateway for SRST. • Existing SRST references—If you choose an SRST reference from the drop-down list, devices in this device pool will use this SRST reference gateway.

Field Name	Description
Connection Monitor Duration	This setting defines the time that the Cisco Unified IP Phone monitors its connection to Cisco Unified Communications Manager before it unregisters from SRST and reregisters to Cisco Unified Communications Manager. To use the configuration for the enterprise parameter, you can enter -1 or leave the field blank. The default value for the enterprise parameter equals 120 seconds. Change this setting if you need to disable the connection monitor or if you want to extend the connection monitor time. The maximum number of seconds that you can enter in the field equals 2592000. **Tip** When you change the value of the connection monitor duration, it applies only to the device pool that is being updated. All other device pools use the value in their own connection monitor duration fields or use the value that is configured in the enterprise parameter. For more information, see topics related to survivable remote site telephony in the *Cisco Unified Communications Manager System Guide*.
Single Button Barge	This setting determines whether the devices or phone users in this device pool have single-button access for barge and cBarge. From the drop-down list box, choose from the following options: • Off—If you choose this option, the devices in this device pool will have the Single Button Barge/cBarge feature disabled. • Barge—If you choose this option, the devices in this device pool will have the Single Button Barge feature enabled. • CBarge—If you choose this option, the devices in this device pool will have the Single Button cBarge feature enabled. • Default—If you choose this option, the devices in this device pool will use the service parameter setting for the Single Button Barge/cBarge feature.
Join Across Lines	This setting determines whether the Join Across Lines feature is enabled for the devices or phone users in this device pool. From the drop-down list box, choose from the following options: • Off—If you choose this option, the devices in this device pool will have the Join Across Lines feature disabled. • On—If you choose this option, the devices in this device pool will have the Join Across Lines feature enabled. • Default—If you choose this option, the devices in this device pool will use the service parameter setting for the Join Across Lines feature.
Physical Location	Select the physical location for this device pool. The system uses physical location with the device mobility feature to identify the parameters that relate to a specific geographical location.

Field Name	Description
Device Mobility Group	Device mobility groups represent the highest level geographic entities in your network and are used to support the device mobility feature.
Wireless LAN Profile Group	Select a wireless LAN profile group from the drop-down list box. You may also click **View Details** to display the settings for this wireless LAN profile group. **Note** You can specify the Wireless LAN Profile Group at the Device Pool level or the individual phone level.
Wi-Fi Hotspot Profile	Select a Wi-Fi Hotspot Profile from the drop-down list box. You may also click **View Details** to display details about the Wi-Fi Hotspot Profile that you select.
Device Mobility Related Information	
Device Mobility Calling Search Space	Choose the appropriate calling search space to be used as the device calling search space when the device is roaming and in same device mobility group.
AAR Calling Search Space	Choose the appropriate calling search space for the device 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.
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.
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 pool. **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 for the device pool and you check the Use Device Pool Calling Party Transformation CSS check box in the device configuration window, 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.

Field Name	Description
Called Party Transformation CSS	This setting allows you to localize the called party number on the device. Make sure that the Called Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device pool. **Note** If you configure the Called Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Called Party Transformation pattern in a non-null partition that is not used for routing.
Geolocation Configuration	
Geolocation	From the drop-down list box, choose a geolocation. You can choose the Unspecified geolocation, which designates that the devices in this device pool do not associate with a geolocation. You can also choose a geolocation that has been configured with the **System** > **Geolocation Configuration** menu option. For an explanation of geolocations, including configuration details, see topics related to geolocations and location conveyance in the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocations, see topics related to geolocations and location conveyance in the *Cisco Unified Communications Manager Features and Services Guide*.
Geolocation Filter	From the drop-down list box, choose a geolocation filter. If you leave the <None> setting, no geolocation filter gets applied for the devices in this device pool. You can also choose a geolocation filter that has been configured with the **System** > **Geolocation Filter** menu option. For an explanation of geolocation filters, including configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocation filters, see the *Cisco Unified Communications Manager Features and Services Guide*.
Incoming Calling Party Settings	
Clear Prefix Settings	To delete all prefixes for all calling party number types, click Clear Prefix Settings.
Default Prefix Settings	To enter the default value for all prefix fields at the same time, click Default Prefix Settings.

Field Name	Description
National Number	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. If the word, Default, displays in the Prefix field, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip digit functionality. • Strip Digits—Enter the number of digits, up to the number 24, that you want Cisco Unified Communications Manager to strip from the calling party number of National type before it applies the prefixes. • 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. 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. **Tip** For more information on configuring these settings, see topics related to configuring incoming calling party settings for a device pool, gateway, or trunk in the *Cisco Unified Communications Manager Features and Services Guide*.

Field Name	Description
International Number	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. 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. • Strip Digits—Enter the number of digits, up to the number 24, that you want Cisco Unified Communications Manager to strip from the calling party number of International type before it applies the prefixes. • 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. 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. **Tip** For more information on configuring these settings, see topics related to configuring incoming calling party settings for a device pool, gateway, or trunk in the *Cisco Unified Communications Manager Features and Services Guide*.

Field Name	Description
Unknown Number	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 (#). 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. • Strip Digits—Enter the number of digits, up to the number 24, that you want Cisco Unified Communications Manager to strip from the calling party number of Unknown type before it applies the prefixes. • 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. 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. **Tip** For more information on configuring these settings, see topics related to configuring incoming calling party settings for a device pool, gateway, or trunk in the *Cisco Unified Communications Manager Features and Services Guide*.

Field Name	Description
Subscriber Number	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 (#). 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. • Strip Digits—Enter the number of digits, up to the number 24, that you want Cisco Unified Communications Manager to strip from the calling party number of Subscriber type before it applies the prefixes. • Calling Search Space—This setting allows you to globalize the calling party number of 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. 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. **Tip** For more information on configuring these settings, see topics related to configuring incoming calling party settings for a device pool, gateway, or trunk in the *Cisco Unified Communications Manager Features and Services Guide*.
Incoming Called Party Settings The Incoming Called Party Settings support H.323 trunks and gateways. The H.323 protocol does not support the international escape character +. To ensure the correct prefixes, including the +, get applied to inbound calls over H.323 gateways/trunks, configure the incoming called party settings; that is, configuring the incoming called party settings ensures that when an inbound call comes from a H.323 gateway or H.323 trunk, Cisco Unified Communications Manager transforms the called party number back to the value that was originally sent over the trunk/gateway.	
Clear Prefix Settings	To delete all prefixes for all called party number types, click Clear Prefix Settings.
Default Prefix Settings	To enter the default value for all prefix fields at the same time, click Default Prefix Settings.

Field Name	Description
National Number	Configure the following settings to transform incoming called party numbers that use National for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called party numbers that use National for the Called Party Numbering Type. You can enter up to 16 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 called party prefix, which supports both the prefix and strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, 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 called party number of National type before it applies the prefixes. • Calling Search Space—This setting allows you to transform the called party number of National called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

Field Name	Description
International Number	Configure the following settings to transform incoming called party numbers that use International for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called party numbers that use International for the Called Party Numbering Type. You can enter up to 16 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 called party prefix, which supports both the prefix and strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, 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 called party number of International type before it applies the prefixes. • Calling Search Space—This setting allows you to transform the called party number of International called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

Field Name	Description
Unknown Number	Configure the following settings to transform incoming called party numbers that use Unknown for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called numbers that use Unknown for the Called Party Numbering Type. You can enter up to 16 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 called party prefix, which supports both the prefix and strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, 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 called party number of Unknown type before it applies the prefixes. • Calling Search Space—This setting allows you to transform the called party number of Unknown called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

Field Name	Description
Subscriber Number	Configure the following settings to transform incoming called party numbers that use Subscriber for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called numbers that use Subscriber for the Called Party Numbering Type. You can enter up to 16 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 called party prefix, which supports both the prefix and strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, 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 called party number of Subscriber type before it applies the prefixes. • Calling Search Space—This setting allows you to transform the called party number of Subscriber called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.
Phone Settings	
Calling Party Transformation CSS	From the drop-down list box, choose the Calling Search Space that contains the Calling Party Transformation Pattern that you want to apply to devices in this device pool. When Cisco Unified CM receives a call from a device in this device pool on an inbound line, Cisco Unified CM immediately applies the calling party transformation patterns in this CSS to the digits in the calling party number before it routes the call. This setting allows you to apply digit transformations to the calling party number before Cisco Unified CM routes the call. For example, a transformation pattern can change a phone extension to appear as an E.164 number.
Connected Party Settings	

Field Name	Description
Connected Party Transformation CSS	This setting is applicable for inbound calls only. This setting allows you to transform the connected party number on the device to display the connected number in another format, such as a DID or E164 number. Cisco Unified Communications Manager includes the transformed number in the headers of various SIP messages, including 200 OK and mid-call update/reinvite messages for SIP calls and in the Connected Number Information Element of CONNECT and NOTIFY messages for H.323 and MGCP calls. Make sure that the Connected Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device pool. **Note** If you configure the Connected Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation pattern used for Connected Party Transformation in a non-null partition that is not used for routing.
Redirecting Party Settings	
Redirecting Party Transformation CSS	This setting allows you to transform the redirecting party number on the device to E164 format. Cisco Unified Communications Manager includes the transformed number in the diversion header of invite messages for SIP trunks and in the Redirecting Number Information Element of setup message (for H.323 and MGCP) sent out of Cisco Unified Communications Manager. Make sure that the Redirecting Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device pool. **Note** If you configure the Redirecting Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Redirecting Party Transformation CSS in a non-null partition that is not used for routing.

Related Topics

Location Setup , on page 127

Synchronize Device Pool Settings with Devices

To synchronize devices to a device pool that has undergone configuration changes, perform the following procedure, which applies 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 **System** > **Device Pool**.
The Find and List Device Pools window displays.

Step 2 Choose the search criteria to use.

Step 3 Click Find.
The window displays a list of Device Pools that match the search criteria.

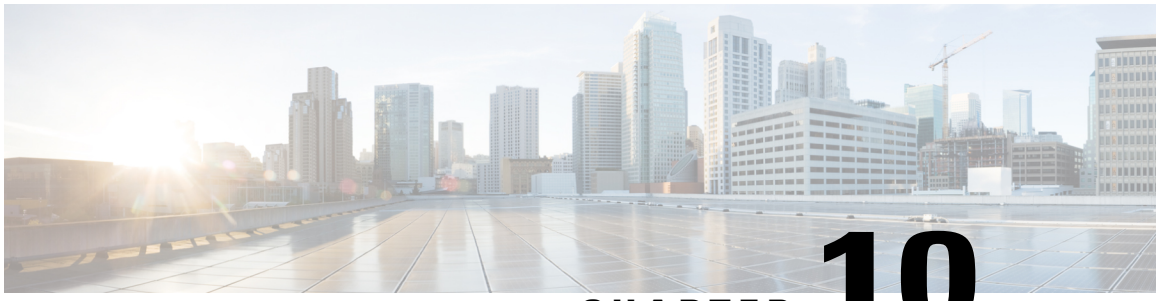
Step 4 Click the Device Pool to which you want to synchronize applicable devices. The Device Pool Configuration window displays.

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.



CHAPTER 10

DHCP Server Setup

This chapter contains information about DHCP server configuration.

For additional information, see topics related to Dynamic Host Configuration Protocol in the *Cisco Unified Communications Manager System Guide*.

About DHCP Server Setup

In Cisco Unified Communications Manager Administration, use the **System** > **DHCP** > **DHCP Server** menu path to configure a DHCP server.

Dynamic Host Configuration Protocol (DHCP) server enables Cisco Unified IP Phones, connected to either the customer's data or voice Ethernet network, to dynamically obtain their IP addresses and configuration information. DHCP uses Domain Name System (DNS) to resolve host names both within and outside the cluster.

DHCP Server Deletion

If the DHCP server is not in use, Cisco Unified Communications Manager allows you to delete the server. If the server is in use, an error message displays.

DHCP Server Settings

The following table describes the DHCP server settings.

Table 11: DHCP Server Settings

Server Information Field	Description
Host Server	Select a host server from the drop-down list of available host servers.
Primary DNS IPv4 Address	This field specifies primary DNS IPv4 address.
Secondary DNS IPv4 Address	This field specifies secondary DNS IPv4 address.
Primary TFTP Server IPv4 Address (Option 150)	You can enable the IP phones to access the TFTP server using DHCP custom option 150. This is the method that Cisco recommends. This field specifies the IPv4 address for primary Trivial File Transfer Protocol (TFTP) server.
Secondary TFTP Server IPv4 Address (Option 150)	This field specifies the IPv4 address for secondary TFTP server.
Bootstrap Server IPv4 Address	This field specifies the address of the server that is used in the next step of the bootstrap process. You can use as the IPv4 address of the TFTP server or as the default value to DHCP server address if the server supplies the next bootstrap service.
Domain Name	The Domain Name specifies the domain name that you should use when resolving hostname via the Domain Name System.
TFTP Server Name (Option 66)	You can enable the IP phones to access the TFTP server by using DHCP option 66. Use this field to identify a TFTP server. You can configure only one DNS name or a dotted decimal IP address in this parameter.
ARP Cache Timeout	This field specifies the timeout in seconds for ARP cache entries. Specify the time as a 32-bit unsigned integer. The default for the Cisco Network Registrar (CNR) DHCP server specifies 60 seconds.
IP Address Lease Time	The DHCP server uses the information in this field to specify the lease time that it is willing to offer. Specify the time in units of seconds and as a 32-bit unsigned integer. The default for the CNR DHCP server specifies seven days (604,800 seconds).
Renewal(T1) Time (sec)	This field specifies the time interval from address assignment until the client transitions to the RENEWING state. Typically, set this field to half the value of the IP address lease time. For example, if the IP address lease time is typically set to 60,000 seconds, the renewal time gets set to 30,000 seconds.

Server Information Field	Description
Rebinding (T2) Time (sec)	This field specifies the time interval from address assignment until the client transitions to the REBINDING state. Specify the value in units of seconds and as a 32-bit unsigned integer. Typically, set this field to approximately 75 percent of the value of the IP address lease time. For example, if the IP address lease time is set to 60,000 seconds, the rebinding time typically gets set to about 45,000 seconds. In Windows, 85 percent of the value of the IP address lease time represents the standard.

Related Topics

DHCP Server Setup , on page 99

Activate DHCP Monitor Service

You can activate and deactivate DHCP monitor process by using the Serviceability window of Cisco Unified Communications Manager. Use the following procedure to activate the service.

Procedure

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

Step 2 Choose the Cisco Unified Communications Manager server from the Servers drop-down list box and click Go.

Step 3 Choose Cisco DHCP Monitor Service from the CM Services list and click Save.
Note If the service is already activated, the Activation Status will display as Activated.

Step 4 The service gets activated, and the Activation Status column displays the status as Activated.
Note The DHCP monitor service starts automatically after it is activated.

Related Topics

DHCP Server Setup , on page 99

Start DHCP Monitor Service

The DHCP Monitor Service starts automatically after it is activated by using Cisco Unified Serviceability. This section describes the procedures to stop or restart the DHCP service.

Procedure

Step 1 In Cisco Unified Serviceability, choose **Tools** > **Control Center - Feature Services**.

The Control Center–Feature Services window displays.

Step 2 Choose the Cisco Unified Communications Manager server from the Servers drop-down list box and click Go.
Cisco DHCP Monitor Service displays in the list under Service Name column, in Unified CM Services.

Note The Activation Status displays as Activated if you followed the procedure to active the DHCP monitor service.

Step 3 Check the radio button corresponding to Cisco DHCP Monitor Service.

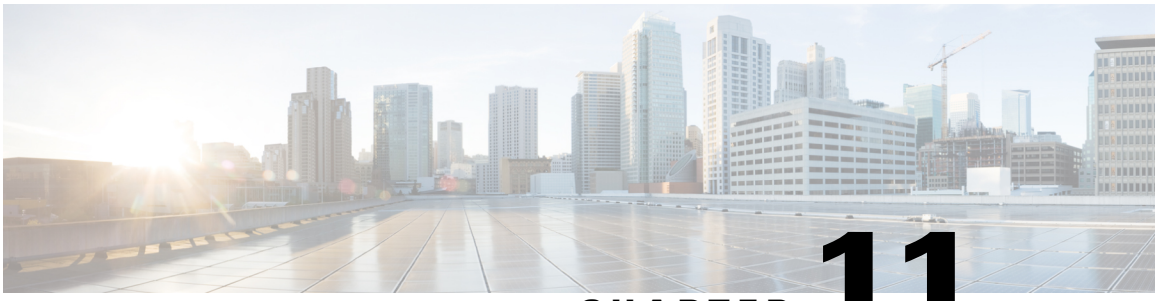
Step 4 If you want to restart the Cisco DHCP Monitor Service, click Restart.
The service restarts, and the message, Service Successfully Restarted, displays.

Step 5 If you want to stop the Cisco DHCP Monitor Service, click Stop.
The service stops, and the message, Service Successfully Stopped, displays.

Step 6 If you want to start a stopped Cisco DHCP Monitor Service, click Start.
The service starts, and the message, Cisco DHCP Monitor Service Restarted Successfully, displays.

Related Topics

DHCP Server Setup , on page 99
Activate DHCP Monitor Service , on page 101



CHAPTER 11

DHCP Subnet Setup

This chapter describes the procedures for adding subnets to DHCP servers. Use the following procedures to find and add subnets to DHCP servers:

For additional information, see topics related to Dynamic Host Configuration Protocol in the *Cisco Unified Communications Manager System Guide*.

About DHCP Subnet Setup

In Cisco Unified Communications Manager Administration, use the **System** > **DHCP Subnet** menu path to configure DHCP subnets.

DHCP Subnet Setup Tips

Changes to the server configuration do not take effect until you restart Cisco Unified Communications Manager. For information about restarting the Cisco CallManager service, see the *Cisco Unified Serviceability Administration Guide*.

DHCP Subnet Deletion

If the subnet is not in use, Cisco Unified Communications Manager allows you to delete it. If the subnet is in use, a message displays.

DHCP Subnet Settings

In the DHCP Subnet Configuration window, you can add subnets to the DHCP server. The following table describes the DHCP subnet settings.

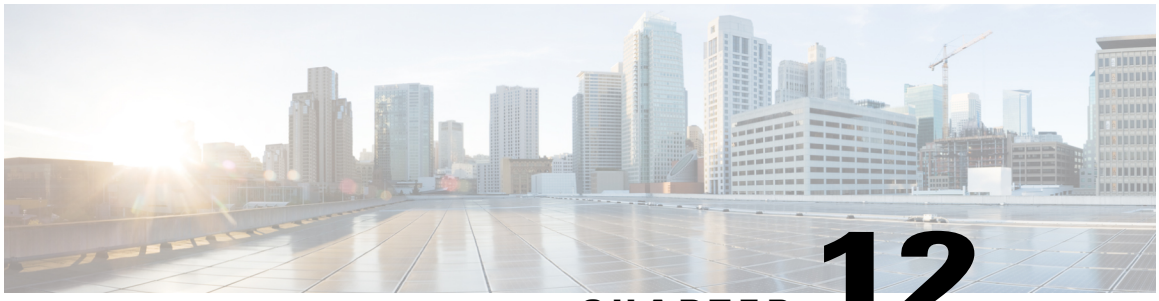
Table 12: DHCP Subnet Settings

DHCP Subnet Information	Description
DHCP Server	Choose the DHCP server name from the drop-down list box.
Subnet IPv4 Address	Enter the Subnet IPv4 address.
Primary Start IPv4 Address	Enter the start IPv4 address of the first range of IP addresses to be assigned.
Primary End IPv4 Address	Enter the end IPv4 address of the first range of IP addresses to be assigned.
Secondary Start IPv4 Address	Enter the start IPv4 address of the second range of IP addresses to be assigned.
Secondary End IPv4 Address	Enter the end IPv4 address of the second range of IP addresses to be assigned.
Primary Router IPv4 Address	Enter the IPv4 address of the primary router on your subnet.
Secondary Router IPv4 Address	Enter the IPv4 address of the secondary router on your subnet.
IPv4 Subnet Mask	Enter the subnet mask.
Domain Name	This field specifies the name that you should use when resolving hostname via the Domain Name System.
Primary DNS IPv4 Address	This field specifies primary DNS IPv4 server name.
Secondary DNS IPv4 Address	This field specifies secondary DNS IPv4 server name.
TFTP Server Name (Option 66)	Use this field to identify a TFTP server. You can configure only one DNS name or a dotted decimal IP address in this parameter.
Primary TFTP Server IPv4 Address (Option 150)	This field specifies the IPv4 addresses for primary Trivial File Transfer Protocol (TFTP) server.
Secondary TFTP Server IPv4 Address (Option 150)	This field specifies the IPv4 addresses for secondary TFTP server.
Bootstrap Server IPv4 Address	This field specifies the address of the server that is used in the next step of the bootstrap process. You can use this as the IPv4 address of the TFTP server or as the default value to DHCP server address if the server is to supply the next bootstrap service.
ARP Cache Timeout (sec)	This field specifies the timeout in seconds for ARP cache entries. Specify the time as a 32-bit unsigned integer.
IP Address Lease Time (sec)	The DHCP server uses the information in this field to specify the lease time that it is willing to offer. Specify the time in units of seconds and as a 32-bit unsigned integer.

DHCP Subnet Information	Description
Renewal (T1) Time (sec)	This field specifies the time interval from address assignment until the client transitions to the RENEWING state.
Rebinding (T2) Time (sec)	This field specifies the time interval from address assignment until the client transitions to the REBINDING state. Specify the value in units of seconds and as a 32-bit unsigned integer.

Related Topics

DHCP Subnet Setup , on page 103



CHAPTER 12

LDAP System Setup

This chapter provides information to configure LDAP system parameters using Cisco Unified Communications Manager. The LDAP directory configuration takes place in the following windows:

- LDAP System Configuration
- LDAP Directory
- LDAP Authentication
- LDAP Filter Configuration

For additional information, see topics related to the directory, application users, and end users in the *Cisco Unified Communications Manager System Guide*.

- About LDAP System Setup , page 107
- LDAP System Settings , page 108

About LDAP System Setup

In Cisco Unified Communications Manager Administration, use the **System** > **LDAP** > **LDAP System** menu path to configure LDAP system settings.

Use the LDAP System Configuration window to enable LDAP synchronization and to set up the LDAP server type and the LDAP attribute name for the user ID.

Note After an upgrade to Unified Communications Manager Release 10.0(1), when new users are synced from LDAP, the home cluster is not enabled. You must modify your existing LDAP synchronization agreement and add a Feature Group Template which has the home cluster enabled.

Before You Begin

The setting of the Enable Synchronizing from LDAP Server check box in this window affects the ability to modify end users in Cisco Unified Communications Manager Administration. LDAP synchronization applies only to end users; LDAP synchronization does not affect application users. See topics related to understanding

the directory in the *Cisco Unified Communications Manager System Guide* for more information about LDAP synchronization.

For end user data, you cannot use the End User Configuration window to update the attributes that are synchronized from the corporate directory. You can update these attributes only in the corporate directory itself, after which you should perform a resynchronization.

You can make changes to LDAP Directory information and LDAP Authentication settings only if synchronization from the customer LDAP directory is enabled in the Cisco Unified Communications Manager Administration LDAP System Configuration window.

Note

- If end users exist in the Cisco Unified Communications Manager database before synchronization with a corporate directory occurs, the system will leave those end users that did not have a matching user ID in the corporate directory as Active Local Users. For example, if users bob and sanjay were in the Cisco Unified Communications Manager database, but only bob was in the LDAP directory, then sanjay will be marked inactive and the End User Configuration window will display the User Status as Active Local User.
- After an LDAP Directory configuration for the DirSync service gets created or the LDAP user authentication is enabled, the settings in the LDAP System Configuration window become read only.
- After you configure LDAP synchronization in Cisco Unified Communications Manager Administration, users without last names in the corporate directory do not synchronize with the Cisco Unified Communications Manager database. No error displays in Cisco Unified Communications Manager Administration, but the log file indicates which users did not synchronize.

LDAP System Settings

The following table describes the LDAP system settings.

Table 13: LDAP System Settings

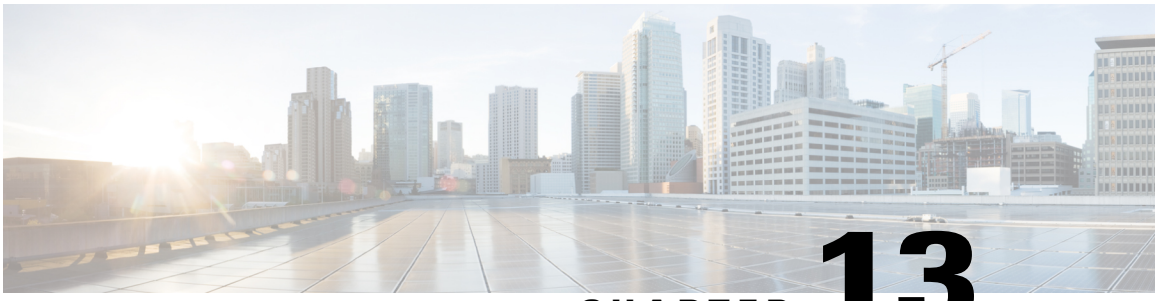
Field	Description
LDAP System Information	

Field	Description
Enable Synchronizing from LDAP Server	To enable synchronization of data from the customer LDAP server, check this check box. If synchronization with the LDAP server is enabled, the following circumstances occur: • You cannot modify end user data, except for the fields (attributes) that are not synchronized from the corporate directory. Example: user PIN. (The administrator can always modify application user data.) • You can modify the LDAP Directory information. • You can modify LDAP Authentication information. If synchronization with the LDAP server is not enabled (is disabled), the following circumstances occur: • You cannot modify LDAP Directory information. • You cannot modify LDAP Authentication information.
LDAP Server Type	If synchronization with the LDAP server is currently enabled, you can choose one of the selections in this drop-down list box. Choose the value that corresponds to the customer LDAP server type: • Microsoft Active Directory • Microsoft Active Directory Application Mode • Netscape or Sun ONE LDAP Server • OpenLDAP

Field	Description
LDAP Attribute for User ID	If synchronization with the LDAP server is enabled, you can choose an LDAP attribute value for the user ID. Choose one of the following values from the drop-down list box: • For Microsoft Active Directory ◦ sAMAccountName ◦ mail ◦ employeeNumber ◦ telephoneNumber ◦ userPrincipalName • Microsoft Active Directory Application Mode ◦ uid ◦ mail ◦ employeeNumber ◦ telephoneNumber ◦ userPrincipalName • For Sun ONE LDAP Server, iPlanet, and OpenLDAP ◦ uid ◦ mail ◦ employeeNumber ◦ telephoneNumber

Related Topics

LDAP System Setup , on page 107



CHAPTER 13

LDAP Directory Setup

This chapter provides information to configure the LDAP directory. The LDAP direcotry configuration takes place in these related windows:

- LDAP System Configuration
- LDAP Directory
- LDAP Authentication
- LDAP Filter Configuration

For additional information, see topics related to the directory, application users, and end users in the *Cisco Unified Communications Manager System Guide*.

- About LDAP Directory Setup , page 111
- LDAP Directory Settings, page 112

About LDAP Directory Setup

In Cisco Unified Communications Manager, use the **System** > **LDAP** > **LDAP Directory** menu path to configure LDAP directories.

In the LDAP Directory window, you specify information about the LDAP directory; for example, the name of the LDAP directory, where the LDAP users exist, how often to synchronize the data, and so on.

When LDAP synchronization happens, users get added to the Cisco Unified Communications Manager and are assigned with extensions. With the introduction of Self-Provisioning, changes to a users primary telephone number in LDAP are synced to the user. However, the extension that was assigned based upon mask and the old primary number is not updated with the new number. And, deleting the user does not delete the extension, thus retaining the extension on the phone that it was assigned to.

Note Assuming LDAP data is accurate, during LDAP synchronization, and using the mask, extensions are created based on the desired requirements. If LDAP data is not accurate, it can create undesired extensions and can affect dial plan and routing that can lead to outside dial tones to fail, or be delayed, or some other numbers to not be reachable. Ensure that LDAP data is always accurate to avoid changes in dial plans and routing behavior.

Before You Begin

Before you can synchronize the LDAP directory, you must activate the Cisco DirSync service. For information about how to activate services, see the *Cisco Unified Serviceability Administration Guide*.

Changes to LDAP Directory information and LDAP Authentication settings are possible only if synchronization from the customer LDAP directory is enabled in the Cisco Unified Communications Manager Administration LDAP System Configuration window.

LDAP Directory Settings

The following table describes the LDAP directory settings.

Table 14: LDAP Directory Settings

Field	Description
LDAP Directory Information	
LDAP Configuration Name	Enter a unique name (up to 40 characters) for the LDAP directory.
LDAP Manager Distinguished Name	Enter the user ID (up to 128 characters) of the LDAP Manager, who is an administrative user that has access rights to the LDAP directory in question.
LDAP Password	Enter a password (up to 128 characters) for the LDAP Manager.
Confirm Password	Reenter the password that you provided in the LDAP Password field.
LDAP User Search Base	Enter the location (up to 256 characters) where all LDAP users exist. This location acts as a container or a directory. This information varies depending on customer setup.

Field	Description
LDAP Custom Filter	Select an LDAP custom filter from the drop-down list. The LDAP filter filters the results of LDAP searches. LDAP users that match the filter get imported into the Cisco Unified Communications Manager database, but LDAP users that do not match the filter do not get imported. The default value is <None>. This value applies a default LDAP filter that is specific to the LDAP server type. These are the default LDAP filters: • Microsoft Active Directory (AD):(&(objectclass=user)(!(objectclass=Computer)) (!(UserAccountControl:1.2.840.113556.1.4.803:=2))) • iPlanet or Sun One LDAP Server:(objectclass=inetOrgPerson) • OpenLDAP:(objectclass=inetOrgPerson) • Microsoft Active Directory Application Mode (ADAM):(&(objectclass=user) (!(objectclass=Computer))(!(msDS-UserAccountDisabled=TRUE))) For more information about LDAP filters, see the LDAP Custom Filter Setup , on page 125.
LDAP Directory Synchronization Schedule	
Perform Sync Just Once	If you want to perform synchronization of the data in this LDAP directory with the data in the Cisco Unified Communications Manager database only once, check this check box.
Perform a Re-sync Every	If you want to perform synchronization of the data in this LDAP directory with the data in the Cisco Unified Communications Manager database at a regular interval, use these fields. In the left field, enter a number. In the drop-down list box, choose a value: • hours • days • weeks • months Cisco Unified Communications Manager can synchronize directory information every 6 hours, which is the minimum value allowed for this field. **Note** This field remains active only if you do not check the Perform Sync Just Once check box.
Next Re-sync Time (YYYY-MM-DD hh:mm)	Specify a time to perform the next synchronization of Cisco Unified Communications Manager directory data with this LDAP directory. Use a 24-hour clock to specify the time of day. For example, 1:00 pm equals 13:00.

Field		Description
Standard User Fields To Be Synchronized		
Cisco Unified Communications Manager User Fields	LDAP User Fields	
User ID	sAMAccountNameoruid	For these fields, the Cisco Unified Communications Manager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right. **Note** Cisco recommends that you do not use a slash (/) in the User ID field. Cisco User Data Services will not function properly for the user when the User ID contains a slash.
Middle Name	(drop-down list box)	For these fields, the Cisco Unified Communications Manager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right. For the LDAP User field, choose one of the following values: • middleName • initials
Manager ID	manager	For these fields, the Cisco Unified Communications Manager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right.
Work Number	(drop-down list box)	For these fields, the Cisco Unified Communications Manager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right. For the LDAP User field, choose one of the following values: • telephoneNumber • ipPhone
Title	title	For these fields, the Cisco Unified Communications Manager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right.
Mobile Number	mobile	For these fields, the Cisco Unified Communications Manager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right.

Field		Description
Directory URI	(drop-down list box)	For these fields, the Cisco Unified Communications Manager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right. For the LDAP User field, choose one of the following values: • msRTCSIP-primaryuseraddress • mail • None **Note** The msRTCSIP-primaryuseraddress option is only available if you choose Microsoft Active Directory as the LDAP Server Type in the LDAP System Configuration window. **Note** By default, the user portion of a directory URI is case-sensitive. Under this setting, whatever case the directory URI has in LDAP will be imported into Cisco Unified Communications Manager. For compatibility with third party call control systems, Cisco recommends that you change this setting by setting the value of the URI Lookup Policy enterprise parameter to case-insensitive.
First Name	givenName	For these fields, the Cisco Unified Communications Manager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right.
Last Name	sn	For these fields, the Cisco Unified Communications Manager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right.
Department	departmentordepart mentnumber	For these fields, the Cisco Unified Communications Manager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right.
Mail ID	(drop-down list box)	For these fields, the Cisco Unified Communications Manager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right. For the LDAP User field, choose one of the following values: • mail • sAMAccountName • uid
Home Number	homePhone	For these fields, the Cisco Unified Communications Manager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right.
Pager Number	pager	For these fields, the Cisco Unified Communications Manager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right.

Field	Description
Custom User Fields To Be Synchronized	
Custom User Field Name	Cisco Unified Communications Manager allows you to synchronize LDAP directory attributes that are not included among the defaults for the Standard User Fields to be Synchronized. Using Custom User Fields, you can synchronize LDAP attributes to a customized field that gets saved in the Cisco Unified Communications Manager database. In the Custom User Field text box, enter a name for the customized field that you want to create. The custom user field can contain up to 64 alphanumeric characters, including spaces. Cisco Unified Communications Manager saves the new customized field in the database. You can create up to five custom user fields. Click the **(+)** button to add additional rows on which you can create new fields.
LDAP Attribute	In the LDAP attribute field, enter a valid LDAP attribute that exists in your LDAP directory. The maximum field length is 128 characters.
Group Information	
Access Control Groups	Use this option to manage the Access Control Group to configure different levels of access for new users that were synchronized from the LDAP directory. Click the **Add to Access Control Group** button to open the Find and List Access Control Groups window. From the list, select one or more Access Control Groups for a user. Click the **Add Selected** button. The Find and List Access Control Groups window closes, and the Update Users Configuration window now shows the selected groups in the list box. To delete an existing Access Control Group, select the relevant Access Control Group from the list box. Click the **Remove from Access Control** button to complete the process. To add a new Access Control Group to the Find and List Access Control Groups window, use the following menu path: **User Management** > **User Settings** > **Access Control Group**

Field	Description
Feature Group Template	From the drop-down list box, select the Feature Group template to be associated with the new users that are synchronized from the LDAP directory. To create a Feature Group template that includes features such as mobility and IM and Presence, use the following menu path:**User Management** > **User/Phone Add** > **Feature Group Template** If you do not select a feature group template, a warning message displays as mentioned below: **Warning** If no template is selected, the new line features below will not be active. If you select a custom feature group template with no user profile, a warning message displays as mentioned below: **Warning** The selected Feature Group Template does not have a Universal Line Template configured. The new line features below will not be active.
Apply mask to synced telephone numbers to create a new line for inserted users	Check the check box to apply mask to the synced telephone number of the user. Enter a mask value in the **Mask** text box. The **Mask** can contain one to twenty four characters including numbers (0-9), X, and x. It must include at least one x or X. For example, if you set the mask as 11XX for the user with a telephone number 8889945, after the mask is applied, 1145 becomes the primary extension of the user.
Assign new line from the pool list if one was not created based on a synced LDAP telephone number	Check the check box to assign a new line from the DN pool list.
Next Candidate DN	Displays the next probable DN that will be assigned to the user. The DN from the next DN pool is displayed only after all the DNs from the first DN pool are assigned. **Note** The **Next Candidate DN** displays only when you check the **Assign new line from the pool list if one was not created based on a synced LDAP telephone number** check box.

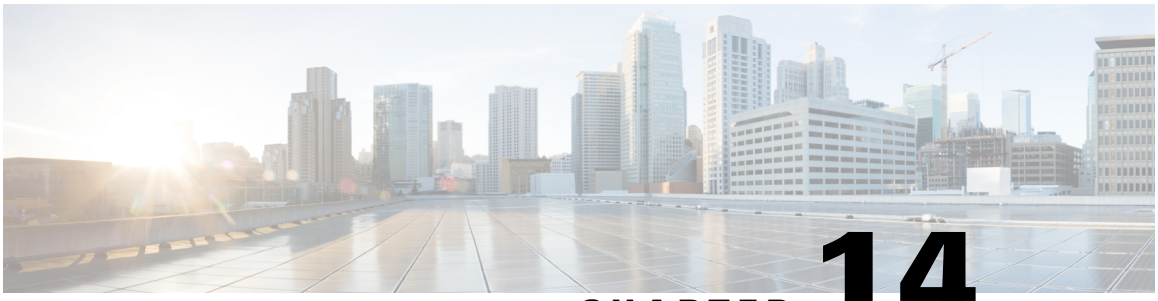
Field	Description
Add DN Pool	By default, only one DN pool is available. Click this option to add more DNs to the DN pool. The **DN Pool Start** and **DN Pool End** values must conform to the following requirements: • Must be a number and can contain one to twenty characters • **DN Pool End** must be greater than **DN Pool Start** • **DN Pool Start** and **DN Pool End** must not be null • DN range must be less than 10,000,000 **Note** The following error message displays if the DN range is not less than 10,000,000: `The DN range must be less than 10,000,000. Also, the Start DN and End DN can only vary in the rightmost seven digits. If the DNs are greater than seven digits long, the additional leftmost digits must be identical.` Enter the **DN Pool Start** and **DN Pool End** values in the text box. You can reorder the DN pool to prioritize the DNs that you want to assign. If the length of the start and end DN pools are different, an error message displays: `The DNs length must be identical.` You can create only three DN pools.
LDAP Server Information	
Host Name or IP Address for Server	Enter the host name or IP address of the server where the data for this LDAP directory resides.

Field	Description
LDAP Port	Enter the port number on which the corporate directory receives the LDAP requests. You can only access this field if LDAP authentication for end users is enabled. The default LDAP port for Microsoft Active Directory and for Netscape Directory specifies 389. The default LDAP port for Secured Sockets Layer (SSL) specifies 636. How your corporate directory is configured determines which port number to enter in this field. For example, before you configure the LDAP Port field, determine whether your LDAP server acts as a Global Catalog server and whether your configuration requires LDAP over SSL. Consider entering one of the following port numbers: LDAP Port when LDAP server is not a Global Catalog server: • 389—When SSL is not required. (This port number specifies the default that displays in the LDAP Port field.) • 636—When SSL is required. (If you enter this port number, make sure that you check the Use SSL check box.) LDAP Port when LDAP server Is a Global Catalog server: • 3268—When SSL is not required. • 3269—When SSL is required. (If you enter this port number, make sure that you check the Use SSL check box.) **Tip** Your configuration may require that you enter a different port number than the options that are listed in the preceding bullets. Before you configure the LDAP Port field, contact the administrator of your directory server to determine the correct port number to enter.
Use SSL	Check this check box to use Secured Sockets Layer (SSL) encryption for security purposes. **Note** If LDAP over SSL is required, the corporate directory SSL certificate must be loaded into Cisco Unified Communications Manager. The *Cisco Unified Communications Operating System Administration Guide* documents the certificate upload procedure in the Security chapter.
Add Another Redundant LDAP Server	Click this button to add another row for entry of information about an additional server.
Perform Full Sync	Click this button to perform a full directory sync. While the directory is synchronizing, the button name changes to Cancel Full Sync. You can click the Cancel Full Sync button to cancel the sync.

In addition to the user fields that appear in Cisco Unified Communications Manager Administration, the Microsoft Active Directory user fields that are described in the following table also get synchronized.

Table 15: Additional Synchronized Microsoft Active Directory User Fields

Cisco Unified Communications Manager User Fields	LDAP User Fields
UniqueIdentifier	ObjectGUID
OCSPrimaryUserAddress	msRTCSIP-primaryuseraddress



CHAPTER 14

LDAP Authentication Setup

This chapter provides information to configure LDAP directory, authentication, and custom filters using Cisco Unified Communications Manager. The LDAP directory configuration takes place in the following windows:

- LDAP System Configuration
- LDAP Directory
- LDAP Authentication
- LDAP Filter Configuration

You can make changes to LDAP directory information and LDAP authentication settings only if synchronization with the customer LDAP directory is enabled in the Cisco Unified Communications Manager Administration LDAP System Configuration window.

For additional information, see topics related to the directory, application users, and end users in the *Cisco Unified Communications Manager System Guide*.

- About LDAP Authentication Setup , page 121
- Update LDAP Authentication, page 122
- LDAP Authentication Settings , page 122

About LDAP Authentication Setup

In Cisco Unified Communications Manager Administration, use the **System** > **LDAP** > **LDAP Authentication** menu path to configure LDAP authentication.

The authentication process verifies the identity of the user by validating the user ID and password/PIN before granting access to the system. Verification takes place against the Cisco Unified Communications Manager database or the LDAP corporate directory.

You can only configure LDAP authentication if you enable LDAP synchronization in the LDAP System Configuration window.

Note User accounts must be synchronized with Cisco Unified Communications Manager to use LDAP authentication. Administrators must enable LDAP synchronization and configure LDAP directory instance(s) to use the LDAP authentication mechanism.

When both synchronization and LDAP authentication are enabled, the system always authenticates application users and end user PINs against the Cisco Unified Communications Manager database. End user passwords get authenticated against the corporate directory; thus, end users need to use their corporate directory password.

When only synchronization is enabled (and LDAP authentication is not enabled), end users get authenticated against the Cisco Unified Communications Manager database. In this case, the administrator can configure a password in the End User Configuration window in Cisco Unified Communications Manager Administration.

Update LDAP Authentication

The setting of the Enable Synchronizing from LDAP Server check box in the LDAP System Configuration window affects your ability to modify LDAP authentication settings. If synchronization with the LDAP server is enabled, you cannot modify LDAP directory information and LDAP authentication settings. See topics related to understanding the directory in the Cisco Unified Communications Manager System Guide for more information about LDAP synchronization.

Conversely, if you want to enable administrators to modify LDAP directory information and LDAP authentication settings, you must disable synchronization with the LDAP server.

LDAP Authentication Settings

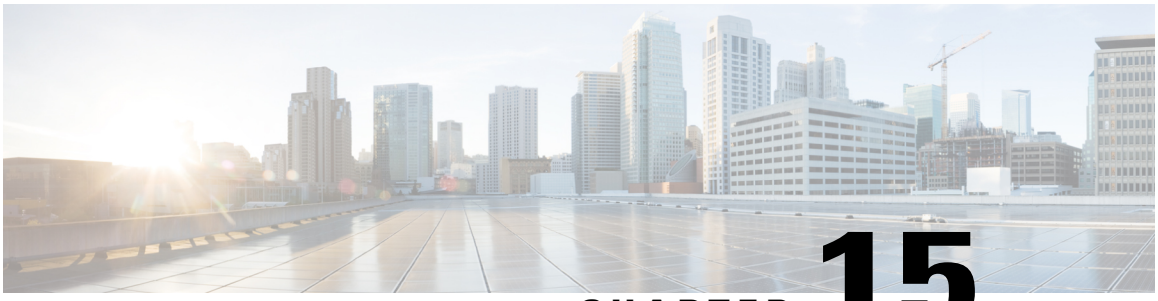
The following table describes the LDAP authentication settings.

Table 16: LDAP Authentication Settings

Field	Description
LDAP Authentication for End Users	
Use LDAP Authentication for End Users	Click this check box to require authentication of end users from the LDAP directory. If the check box is left unchecked, authentication gets performed against the database. **Note** You can only access this field if LDAP synchronization is enabled in the LDAP System Configuration window.
LDAP Manager Distinguished Name	Enter the user ID of the LDAP Manager who is an administrative user that has access rights to the LDAP directory in question. **Note** You can only access this field if LDAP authentication for end users is enabled.
LDAP Password	Enter a password for the LDAP Manager. **Note** You can only access this field if LDAP authentication for end users is enabled.

Field	Description
Confirm Password	Reenter the password that you provided in the LDAP Password field. **Note** You can only access this field if LDAP authentication for end users is enabled.
LDAP User Search Base	Enter the user search base. Cisco Unified Communications Manager searches for users under this base. **Note** You can only access this field if LDAP authentication for end users is enabled.
LDAP Server Information	
Host Name or IP Address for Server	Enter the host name or IP address where you installed the corporate directory. **Note** You can only access this field if LDAP authentication for end users is enabled.
LDAP Port	Enter the port number on which the corporate directory receives the LDAP requests. You can only access this field if LDAP authentication for end users is enabled. The default LDAP port for Microsoft Active Directory and for Netscape Directory specifies 389. The default LDAP port for Secured Sockets Layer (SSL) specifies 636. How your corporate directory is configured determines which port number to enter in this field. For example, before you configure the LDAP Port field, determine whether your LDAP server acts as a Global Catalog server and whether your configuration requires LDAP over SSL. Consider entering one of the following port numbers: LDAP port when LDAP server is not a Global Catalog server: • 389—When SSL is not required. (This port number specifies the default that displays in the LDAP Port field.) • 636—When SSL is required. (If you enter this port number, make sure that you check the Use SSL check box.) LDAP port when LDAP server is a Global Catalog server: • 3268—When SSL is not required. • 3269—When SSL is required. (If you enter this port number, make sure that you check the Use SSL check box.) **Tip** Your configuration may require that you enter a different port number than the options that are listed in the preceding bullets. Before you configure the LDAP Port field, contact the administrator of your directory server to determine the correct port number to enter.

Field	Description
Use SSL	Check this check box to use SSL encryption for security purposes. **Note** If LDAP over SSL is required, the corporate directory SSL certificate must be loaded into Cisco Unified Communications Manager. The *Cisco Unified Communications Operating System Administration Guide* describes the certificate upload procedure. If you check the Use SSL check box, enter the IP address or the hostname that exists in the corporate directory SSL certificate in the Host Name or IP Address for Server field in the LDAP Authentication Configuration window. If the certificate contains an IP address, enter the IP address. If the certificate contains the hostname, enter the hostname. If you do not enter the IP address or hostname exactly as it exists in the certificate, problems may occur for some applications; for example, applications that use CTIManager.
Add Another Redundant LDAP Server	Click this button to add another row for entry of information about an additional server. **Note** You can only access this button if LDAP authentication for end users is enabled.



CHAPTER 15

LDAP Custom Filter Setup

This chapter provides information to configure the LDAP directory. Configuration takes place in these related windows:

- LDAP System Configuration
- LDAP Directory
- LDAP Authentication
- LDAP Filter Configuration

For additional information, see topics related to the directory, application users, and end users in the *Cisco Unified Communications Manager System Guide*.

- About LDAP Custom Filter Setup , page 125
- LDAP Filter Deletion , page 126
- LDAP Filter Settings , page 126

About LDAP Custom Filter Setup

In Cisco Unified Communications Manager Administration, use the **System** > **LDAP** > **LDAP Custom Filter** menu path to configure LDAP filters.

In the LDAP Filter Configuration window, you specify information about the LDAP filter.

With the introduction of Self-Provisioning , you must setup correct filters for the LDAP synchronization to add only UC users and not contacts users. If you do not setup correct filters, during LDAP synchronization, both contacts and UC users get extensions assigned to them. This results in having more extensions than what you actually require.

Before You Begin

Before you can synchronize the LDAP directory, you must activate the Cisco DirSync service. For information about how to activate services, see the *Cisco Unified Serviceability Administration Guide*.

Changes to LDAP Directory information and LDAP Authentication settings are possible only if synchronization from the customer LDAP directory is enabled in the Cisco Unified Communications Manager Administration LDAP System Configuration window.

You can import and export LDAP custom filters by using the Bulk Administration Tool. For more information, see the *Cisco Unified Communications Manager Bulk Administration Guide*.

LDAP Filter Deletion

When you delete an LDAP filter, Cisco Unified Communications Manager removes that filter from the database.

You cannot delete an LDAP filter that is assigned to a directory agreement. To determine if an LDAP filter is assigned to a directory agreement, select Dependency Records from the Related Links drop-down list box in the LDAP Filter Configuration window. If any dependencies display for that LDAP filter, you cannot delete it.

LDAP Filter Settings

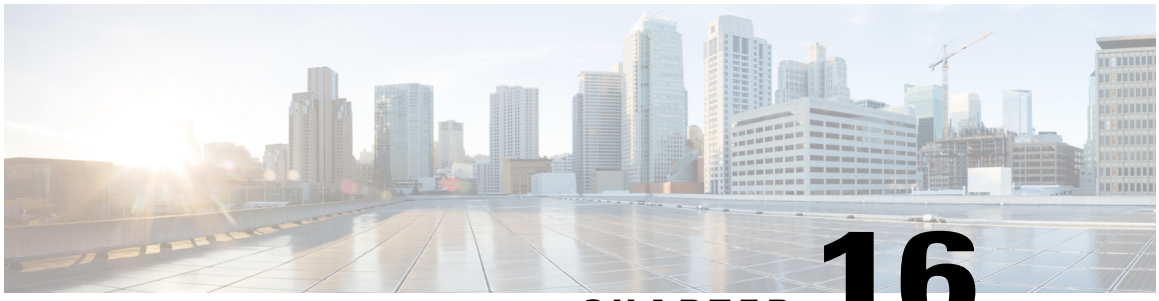
The following table describes the LDAP filter settings.

Table 17: LDAP Custom Filter Settings

Field	Description
LDAP Custom Filter Information	
Filter Name	Enter a name for the LDAP filter. The name can contain a maximum of 64 UTF-8 characters.
Filter	Enter a filter. The filter can contain a maximum of 1024 UTF-8 characters. Enclose the filter text within parentheses (). The LDAP filter filters the results of LDAP searches. LDAP users that match the filter get imported into the Cisco Unified Communications Manager database, while LDAP users that do not match the filter do not get imported. The filter text that you enter must comply with the regular LDAP search filter standards specified in RFC 4515. It is recommended that you verify the LDAP search filter against the LDAP directory/searchbase by using the ldapsearch command. You apply LDAP filters to LDAP directories. For more information, see the LDAP Directory Setup , on page 111. You can apply an LDAP filter to multiple LDAP directories, and to all LDAP directory types for which the filter is valid.

Related Topics

LDAP Custom Filter Setup , on page 125



CHAPTER 16

Location Setup

This chapter provides information about using Cisco Unified Communications Manager Administration to configure location settings and resynchronizing location bandwidth.

About Location Setup

In Cisco Unified Communications Manager Administration, use the **System** > **Location Info** menu path to configure locations.

Use locations to implement call admission control in a centralized call-processing system. Call admission control 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 the locations. For more information, see topics related to call admission control in the *Cisco Unified Communications Manager System Guide*.

Note If you do not use call admission control to limit the audio and video bandwidth on an IP WAN link, an unlimited number of calls can be active on that link at the same time. This situation can cause the audio quality of each audio call and the video quality of each video call to degrade as the link becomes oversubscribed.

Tip Do not confuse locations with geolocations. Locations, which you configure by using the **System** > **Location Info** 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.

In a centralized call-processing system, a single Cisco Unified Communications Manager cluster provides call processing for all locations on the IP telephony network. The Cisco Unified Communications Manager cluster usually resides at the main (or central) location, along with other devices such as phones and gateways. The remote locations contain additional devices, but no Cisco Unified Communications Manager. IP WAN links connect the remote locations to the main location.

Cisco Unified Communications Manager supports up to 2000 locations. The following limitations and restrictions apply:

- Configure as many locations as possible to Use System Default for the RSVP policy.
- This enhancement requires a virtual machine OVA with a capacity of 7500 users or larger.
- See the "Regions" subtopic under the "Administration Considerations" topic of the "IP Video Telephony" chapter of the **Cisco Unified Communications Solution Reference Network Design (SRND)** for the current release, which provides recommendations as to how the video bandwidth should be set for regions and locations, so the video portion of video calls will succeed, and the video calls will not get rejected nor set up as audio-only calls.

Enhanced Location Call Admission Control

The Enhanced Location Call Admission Control (CAC) feature improves the Location CAC mechanism to support more complex networks, including multi-tier, and multi-hop topologies. This feature supports Location CAC within a cluster and among multiple clusters, performing 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 Location CAC feature is provided by the Location Bandwidth Manager (LBM) service. The LBM service can be configured to run on every node or selected nodes of a Unified Communication Manager (Unified CM) server. For more information, see the chapter Enhanced Location Call Admission Control in the *Cisco Unified Communications Manager Features and Services Guide*.

Related Topics

About Cisco Unified Communications Manager Setup , on page 35
CTI Route Point Setup , on page 453
Gateway Setup , on page 465
Cisco Unified IP Phone Setup , on page 579

Location Deletion

You cannot delete a location to which devices are assigned. To find out which devices are using the location, click Dependency Records from Related Links in the Location Configuration window; then, click Go. If the dependency records are not enabled for the system, the dependency records summary window displays a message. If you try to delete a location that is in use, Cisco Unified Communications Manager displays a message. Before deleting a location that is currently in use, you must perform either or both of the following tasks:

- Update the devices to assign them to a different location.
- Delete the devices that are assigned to the location that you want to delete.

Note Deleting a location allocates infinite bandwidth for the links that are connected to that location and allows an unlimited number of calls on those links. Deleting a location can cause audio quality on the links to degrade.

Related Topics

Access Dependency Records , on page 982

Location Settings

The following table describes the location settings.

Table 18: Location Settings

Field	Description
Location Information	
Name	Enter the name of the new location that you are creating. Three system locations are predefined: • Hub_None—The Hub_None location specifies unlimited audio bandwidth and unlimited video bandwidth. A device that associates with the Hub_None location allows an unlimited number of active calls to or from the device. By default, devices not assigned to other locations are assigned to Hub_None. **Note** The location that is configured in a device pool takes precedence over the location configured in the device when the location in the device is set to Hub_None. If the device location is set to any other user-defined location, standard rules apply and the device parameter takes priority. • Phantom—Phantom location specifies unlimited audio bandwidth, unlimited video bandwidth, and unlimited immersive video bandwidth.. Specify this location to allow successful call admission control for calls across inter-cluster trunks that use the H.323 protocol or SIP trunks to certain destinations that support the earlier Location CAC feature. **Note** Both Hub_None and Phantom locations do allow configuration of the associated RSVP policy setting(s). • Shadow—Shadow is a system location created for inter-cluster Enhanced Location CAC. In order to pass location information across clusters, the SIP ICT must be assigned to the system location Shadow.
Links - Bandwidth Between This Location and Adjacent Locations	
Location	Select a location from the list.

Field	Description
Weight	Enter the relative priority of this link in forming the Effective Path between any pair of Locations. The Effective Path has the least cumulative Weight of all possible paths. Valid values are 0-100.
Audio Bandwidth	Enter the maximum amount of audio bandwidth (in kb/s) that is available for all audio calls on the link between this location and other locations. For audio calls, the audio bandwidth includes overhead. Choose between the following options: • Unlimited bandwidth—Click the Unlimited radio button. • Specified bandwidth—Specify a bandwidth by clicking the radio button next to the kb/s box and entering a specified bandwidth. Valid values are 1 to 2147483647. For purposes of location bandwidth calculations only, assume that each call stream consumes the following amount of bandwidth: • G.711 call uses 80 kb/s. • G.722 call uses 80 kb/s. • G.723 call uses 24 kb/s. • G.728 call uses 16 kb/s. • G.729 call uses 24 kb/s. • GSM call uses 29 kb/s. • Wideband call uses 272 kb/s. **Note** To improve audio quality, lower the bandwidth setting, so fewer active calls are allowed on this link.
Video Calls Information	
Video Bandwidth	Enter the maximum amount of video bandwidth (in kb/s) that is available for all video calls on the link between this location and other locations. For video calls, the video bandwidth does not include overhead. Choose among the following options: • None—The system does not allow video calls between this location and other locations. • Specified bandwidth—Specify a video bandwidth by clicking the radio button next to the kb/s box and entering a specified video bandwidth. The default value specifies 384 kb/s. • Unlimited bandwidth—Click the Unlimited radio button.
Immersive Video Information	

Field	Description
Immersive Video	Enter the maximum amount of immersive video bandwidth (in kb/s) that is available for all immersive video calls on the link within this location. For video calls, the immersive video bandwidth does not include overhead. Choose among the following options: • None—The system does not allow immersive video calls between this location and other locations. Immersive video calls can, however, take place within this location. • Specified bandwidth—Specify an immersive video bandwidth by clicking the radio button next to the kb/s box and entering a specified immersive video bandwidth. The default value specifies 384 kb/s. • Unlimited bandwidth—Click the Unlimited radio button.
Intra-location - Bandwidth for Devices within This Location	
Audio Calls Information	
Audio Bandwidth	Enter the maximum amount of audio bandwidth (in kb/s) that is available for all audio calls on the link within this location. For audio calls, the audio bandwidth includes overhead. Choose between the following options: • Unlimited bandwidth—Click the Unlimited radio button. • Specified bandwidth—Specify a bandwidth by clicking the radio button next to the kb/s box and entering a specified bandwidth. Valid values are 1 to 2147483647. For purposes of location bandwidth calculations only, assume that each call stream consumes the following amount of bandwidth: • G.711 call uses 80 kb/s. • G.722 call uses 80 kb/s. • G.723 call uses 24 kb/s. • G.728 call uses 16 kb/s. • G.729 call uses 24 kb/s. • GSM call uses 29 kb/s. • Wideband call uses 272 kb/s. To improve audio quality, lower the bandwidth setting, so fewer active calls are allowed within this location.
Video Calls Information	

Field	Description
Video Bandwidth	Enter the maximum amount of video bandwidth (in kb/s) that is available for all video calls on the link between this location and other locations. For video calls, the video bandwidth does not include overhead. Choose among the following options: • None—The system does not allow video calls between this location and other locations. • Specified bandwidth—Specify a video bandwidth by clicking the radio button next to the kb/s box and entering a specified video bandwidth. The default value specifies 384 kb/s. • Unlimited bandwidth—Click the Unlimited radio button.
Immersive Video Information	
Immersive Video	Enter the maximum amount of immersive video bandwidth (in kb/s) that is available for all immersive video calls on the link within this location. For video calls, the immersive video bandwidth does not include overhead. Choose among the following options: • None—The system does not allow immersive video calls between this location and other locations. Immersive video calls can, however, take place within this location. • Specified bandwidth—Specify an immersive video bandwidth by clicking the radio button next to the kb/s box and entering a specified immersive video bandwidth. The default value specifies 384 kb/s. • Unlimited bandwidth—Click the Unlimited radio button.
Locations RSVP Settings	
Location	This display-only field displays locations for which the inter-location RSVP setting has been changed from the system default RSVP policy.
RSVP Setting	This display-only field displays the RSVP policy setting between the selected location and the location that is listed in the Location column to the left.
Modify Setting(s) to Other Locations	
Location	To change the RSVP policy setting between the current location and a location that displays in this pane, choose a location in this pane.

Field	Description
RSVP Setting	To choose an RSVP policy setting between the current location and the location that is chosen in the Location pane at left, choose an RSVP setting from the drop-down list box. Choose from the following available settings: • Use System Default—The RSVP policy for the location pair matches the clusterwide RSVP policy. See topics related to clusterwide default RSVP policy in the *Cisco Unified Communications Manager System Guide* for details. • No Reservation—No RSVP reservations can get made between any two locations. • Optional (Video Desired)—A call can proceed as a best-effort audio-only call if failure to obtain reservations for both audio and video streams occurs. RSVP Agent continues to attempt RSVP reservation and informs Cisco Unified Communications Manager if reservation succeeds. • Mandatory—Cisco Unified Communications Manager does not ring the terminating device until RSVP reservation succeeds for the audio stream and, if the call is a video call, for the video stream as well. • Mandatory (Video Desired)—A video call can proceed as an audio-only call if a reservation for the video stream cannot be reserved.

Location Bandwidth Manager Group

In Cisco Unified Communications Manager Administration, use the **System > Location Info > Location Bandwidth Manager Group** menu path to configure which Location Bandwidth Manager (LBM) services each Cisco Callmanager service communicate with.

Each Cisco Callmanager service must communicate with an LBM service to determine the availability of bandwidth for each call, and to deduct bandwidth for the duration of each call that is admitted.

The LBM Group Page allows the Cisco Callmanger service to communicate with selected LBM services, instead of communicating with the local LBM service.

Table 19: Location Bandwidth Manager Group Configuration

Field	Description
Location Bandwidth Manager Group Setting	
Name	Enter the name of the new Location Bandwidth Manager Group that you are creating.
Description	If desired enter a description for the Location Bandwidth Manager Group.
Location Bandwidth Manager Group Members	
Active Member	Select the active member from the list.

Field	Description
Standby Member	If desired select a standby LBM to be used when the active LBM is not reachable.

Location Bandwidth Manager Intercluster Replication Group Settings

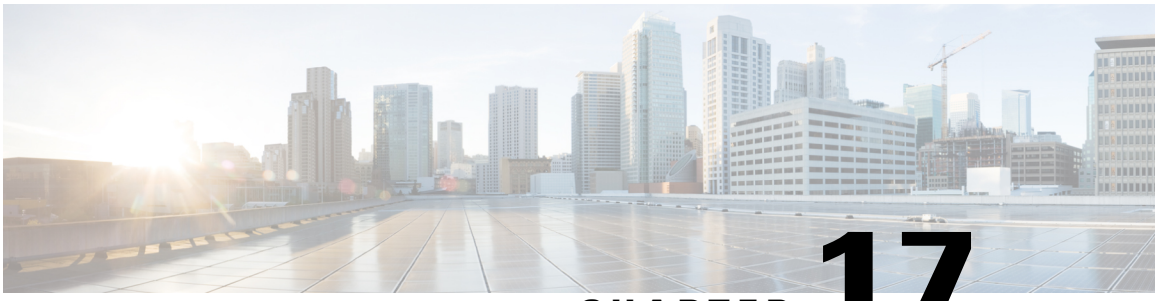
In Cisco Unified Communications Manager Administration, use the **System > Location Info > Location Bandwidth Manager (LBM) Intercluster Replication Group** menu path to configure LBM Intercluster Replication Group.

LBM Intercluster Replication Group configuration enables an LBM service to participate either directly or indirectly in intercluster replication of configured and dynamic Location Bandwidth data. LBMs assigned an LBM hub role participate directory in intercluster replication of Location Bandwidth data. LBM hubs discover each other through their common connections and form a fully-meshed replication network. LBMs assigned a spoke role participate indirectly in intercluster replication through the LBM hubs in their cluster.

Use the LBM Intercluster Replication Group Page to configure the LBM Intercluster Replication service to find a location in the remote clusters to establish external communication.

Table 20: LBM Intercluster Replication Group Configuration

Field	Description
Group Information	
Name	Enter the name of the new LBM Intercluster Replication Group that you are creating.
Description	If desired enter a description for the LBM Intercluster Replication Group.
Bootstrap Servers	
Server	Add servers to the list.
Role Assignment	
LBM Services Assigned to Hub Role	Services in this list become LBM hubs.
LBM Services not Assigned to Hub Role	Services in this list become LBM spokes.



CHAPTER 17

Survivable Remote Site Telephony Setup

This chapter provides information to add, update, copy, or delete a SRST reference.

For additional information, see topics related to survivable remote site telephony references in the *Cisco Unified Communications Manager System Guide*.

About SRST Reference Setup

In Cisco Unified Communications Manager Administration, use the **System** > **SRST** menu path to configure SRST references.

A survivable remote site telephony (SRST) reference comprises the gateway that can provide limited Cisco Unified Communications Manager functionality when all other Cisco Unified Communications Manager servers for a device are unreachable. Typically assigned to device pools, SRST references determine the gateways where calling devices search when they attempt to complete a call if Cisco Unified Communications Manager is unavailable. For more detailed information on SRST references, see topics related to SRST reference configuration settings in the *Cisco Unified Communications Manager System Guide*.

SRST Reference Deletion

You cannot delete SRST references that device pools or other items are using. To find out which device pools are using the SRST reference, click the Dependency Records link from the SRST Reference Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. If you try to delete an SRST reference that is in use, Cisco Unified Communications Manager displays an error message. Before deleting an SRST reference that is currently in use, you must perform either or both of the following tasks:

- Assign a different SRST reference to any device pools that are using the SRST reference that you want to delete.
- Delete the device pools that are using the SRST reference that you want to delete.

Caution Before initiating a deletion, check carefully to ensure that you are deleting the correct SRST reference. You cannot retrieve deleted SRST references. If an SRST reference is accidentally deleted, you must rebuild it.

Related Topics

About Device Pool Setup , on page 79
Access Dependency Records , on page 982

SRST Reference Settings

The following table describes the SRST reference settings.

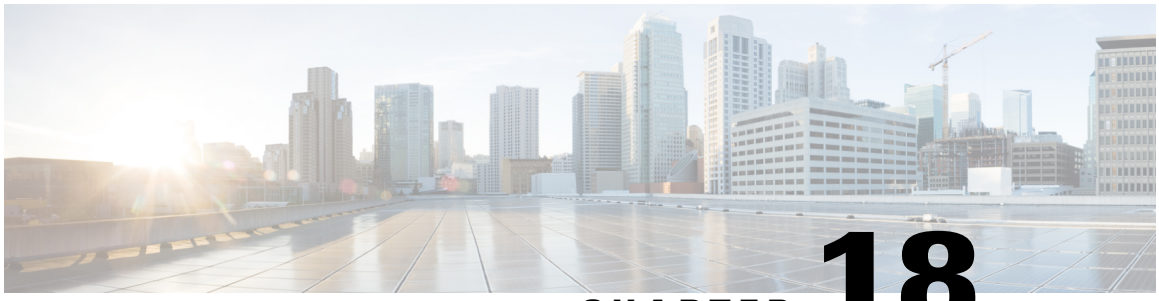
Table 21: SRST Reference Settings

Field	Description
Name	Enter a name in the SRST Reference Name field. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that each SRST reference name is unique. **Note** Use concise and descriptive names for your SRST references.
Port	Enter the port number for this SRST reference. Default value specifies 2000. **Note** Change this value only if it does not match the gateway port setting. This value and the gateway port setting must match.
IP Address	Enter the IP address of the gateway for devices in a device pool to use as an SRST reference.
SIP Network/IP Address	Enter the IP address of the server that the phones that are running SIP will use when in SRST mode. **Tip** You must configure the SIP Network/IP Address field and the SIP Port field for a SIP device to fall back to the SRST-enabled gateway
SIP Port	Enter the SIP port of the SRST gateway. Default value specifies 5060.
Is SRST Secure?	After you verify that the SRST-enabled gateway contains a self-signed certificate, check this check box. After you configure the SRST and reset the gateway and dependent phones, the Cisco CTL Provider service authenticates to the Certificate Provider service on the SRST-enabled gateway. The Cisco CTL client retrieves the certificate from the SRST-enabled gateway and stores the certificate in the Cisco Unified Communications Manager database. **Tip** To remove the SRST certificate from the database and phone, uncheck this check box, click Save, and reset the dependent phones.

Field	Description
SRST Certificate Provider Port	This port monitors requests for the Certificate Provider service on the SRST-enabled gateway. Cisco Unified Communications Manager uses this port to retrieve the certificate from the SRST-enabled gateway. The Cisco SRST Certificate Provider default port equals 2445. After you configure this port on the SRST-enabled gateway, enter the port number in this field. **Tip** You may need to configure a different port number if the port is currently used or if you use a firewall and you cannot use the port within the firewall.
Update Certificate	**Tip** This button displays only after you check the Is SRST Secure? check box and click Save. After you click this button, the Cisco CTL client replaces the existing SRST-enabled gateway certificate that is stored in the Cisco Unified Communications Manager database, if a certificate exists in the database. After you reset the dependent phones, the TFTP server sends the cnf.xml file (with the new SRST-enabled gateway certificate) to the phones.

Related Topics

Survivable Remote Site Telephony Setup , on page 135



CHAPTER 18

MLPP Domain setup

This chapter provides information to add, update, or delete MLPP domains.

For additional information, see topics related to multilevel precedence and preemption in the *Cisco Unified Communications Manager Features and Services Guide*.

About MLPP Domain Setup

In Cisco Unified Communications Manager Administration, use the **System** > **MLPP** > **Domain** > **MLPP Domain** menu path to configure MLPP domains.

An MLPP domain 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.

MLPP Domain Configuration Tips

You can add secure MLPP over SIP trunks by configuring a Resource Priority Namespace Network Domain and Resource Priority Namespace List.

Related Topics

About Resource Priority Namespace Network Domain Setup , on page 141
About Resource Priority Namespace List Setup , on page 143

MLPP Domain Deletion

You cannot delete an MLPP Domain that any device is using. To find out which devices are using the MLPP domain, from the MLPP Domain Configuration window, choose Dependency Records from the Related Links drop-down list box 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 Access

Dependency Records , on page 982. If you try to delete an MLPP Domain that is in use, Cisco Unified Communications Manager displays an error message. Before deleting an MLPP Domain that is currently in use, you must perform either or both of the following tasks:

- Assign a different MLPP domain to any devices that are using the MLPP domain that you want to delete.
- Delete the devices that are using the MLPP domain that you want to delete.

MLPP Domain Settings

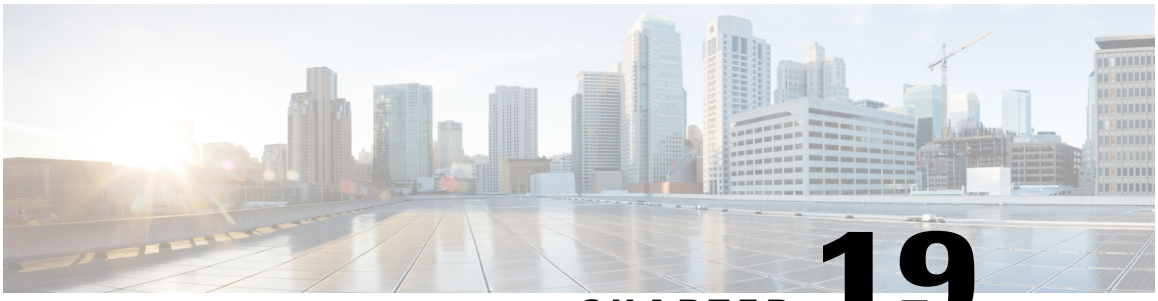
The following table describes the MLPP domain settings.

Table 22: MLPP Domain Settings

Field	Description
MLPP Domain Information	
Domain Name	Enter the name that you want to assign to the new MLPP domain. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that each MLPP domain name is unique. **Note** The name of the default MLPP domain specifies 000000. The Default domain cannot be changed nor deleted.
Domain ID	Enter a unique six-character hexadecimal MLPP domain ID. Valid values are numeric characters 0 through 9 and alphabetic characters A through F. Ensure that each MLPP domain ID is unique. Domain IDs must fall in the range between 000001 and FFFFFF. (000000 is reserved for the default MLPP domain ID.) **Note** Use leading zeroes for values lower than 100000.

Related Topics

MLPP Domain setup, on page 139



CHAPTER 19

Resource Priority Namespace Network Domain Setup

This chapter provides information to add, update, or delete Resource Priority Namespace Network Domains

For additional information, see topics related to multilevel precedence and preemption in the *Cisco Unified Communications Manager Features and Services Guide*.

About Resource Priority Namespace Network Domain Setup

In Cisco Unified Communications Manager Administration, use the **System** > **MLPP** > **Namespace** > **Resource Priority Namespace Network Domain** menu path to configure Resource Priority Namespace Network Domains.

Cisco Unified Communications Manager uses Resource Priority Namespace Network Domains to support Voice over Secured IP (VoSIP) networks by using Multilevel Precedence and Preemption (MLPP) for Session Initiation Protocol (SIP) trunks.

MLPP, with configured Resource Priority domains, prioritizes SIP–signaled resources and enables indications related to precedence and preempted calls. End users can establish secure calls when the calls traverse SIP trunks.

There are five registered namespaces for resource priority:

1. dsn—Defense Switched Network
2. drsn—Defense Red Switched Network
3. q735—Commercial equivalent of the DSN
4. ets—Emergency Telephone Service
5. wps—Wireless Priority Service

Note Cisco Unified Communications Manager accepts “Q735” and “q735” as the same value. It transmits “q735’ when signaling an MLPP call on the SIP trunk.

Resource Priority Namespace Network Domain Deletion

You cannot delete a Resource Priority Namespace Network Domain that any device is using. To find out which devices are using the Resource Priority Namespace Network Domain, from the Resource Priority Namespace Network Domain Configuration window, choose Dependency Records from the Related Links drop-down list box 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.

If you try to delete an Resource Priority Namespace Network Domain that is in use, Cisco Unified Communications Manager displays an error message. Before deleting a Resource Priority Namespace Network Domain that is currently in use, you must perform either or both of the following tasks:

- Assign a different Resource Priority Namespace Network Domain to any devices that are using the Resource Priority Namespace Network Domain that you want to delete.
- Delete the devices that are using the Resource Priority Namespace Network Domain that you want to delete.

Related Topics

Access Dependency Records , on page 982

Resource Priority Namespace Network Domain Settings

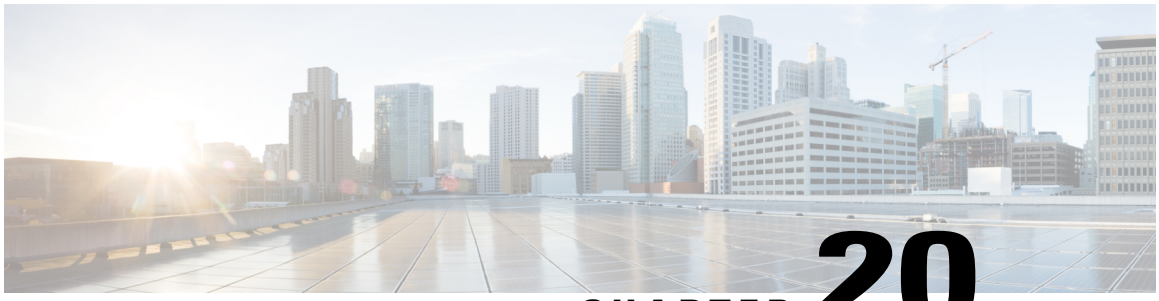
The following table describes the Resource Priority Namespace Network Domain settings.

Table 23: Resource Priority Namespace Network Domain Settings

Field	Description
Name	Enter the name for the Resource Priority Namespace Network Domain in the information section. The maximum number of domain names is 100.
Description	Enter a description for the domain name. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), or angle brackets (<>).
Make this the Default Resource Priority Namespace Network Domain	Check the box if you want the domain name to be the default.

Related Topics

Resource Priority Namespace Network Domain Setup , on page 141



CHAPTER 20

Resource Priority Namespace List Setup

This chapter provides information to add, update, or delete Resource Priority Namespace Lists.

About Resource Priority Namespace List Setup

In Cisco Unified Communications Manager Administration, use the **System** > **MLPP** > **Namespace** > **Resource Priority Namespace List** menu path to configure Resource Priority Namespace Lists.

Cisco Unified Communications Manager uses Resource Priority Namespace Lists to configure a default group of Resource Priority Namespace Network Domains to add to a SIP profile for validating incoming Resource Priority Namespace Network Domains.

Resource Priority Namespace List Deletion

You cannot delete a Resource Priority Namespace List that any device is using. To find out which devices are using the Resource Priority Namespace List, from the Resource Priority Namespace List Configuration window, choose Dependency Records from the Related Links drop-down list box and click Go. If the dependency records are not enabled for the system, the dependency records summary window displays a message. If you try to delete an Resource Priority Namespace List that is in use, Cisco Unified Communications Manager displays an error message. Before deleting an Resource Priority Namespace List that is currently in use, you must perform either or both of the following tasks:

- Assign a different Resource Priority Namespace List to any devices that are using the Resource Priority Namespace List that you want to delete.
- Delete the devices that are using the Resource Priority Namespace List that you want to delete.

Related Topics

Access Dependency Records , on page 982

Resource Priority Namespace List Settings

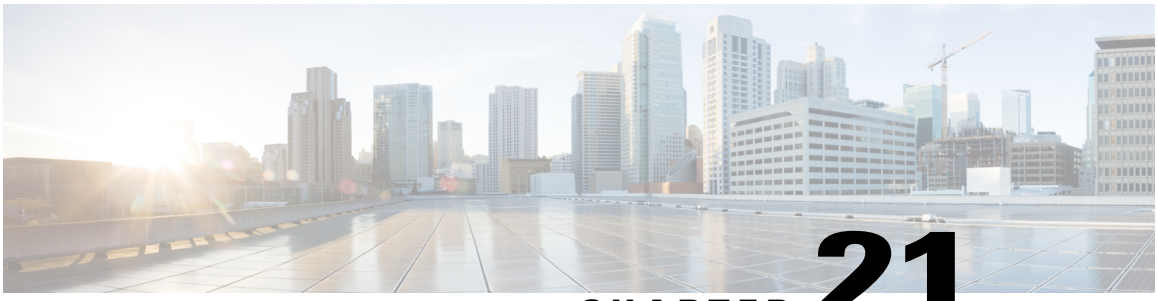
The following table describes the Resource Priority Namespace List settings.

Table 24: Resource Priority Namespace List Settings

Field	Description
Name	Enter the name for the Resource Priority Namespace List. The maximum number of characters is 50.
Description	Enter a description for the list. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
Available Resource Priority Namespaces	Use the Up and Down Arrows to select or deselect already configured Resource Priority Namespace Network Domains.
Selected Resource Priority Namespaces	Displays the selected Resource Priority Namespace Network Domains.

Related Topics

Resource Priority Namespace List Setup , on page 143



CHAPTER 21

E911 Messages

Users of devices designated for off-premises use are first presented with various messages, which assure that users are aware of the need to provide correct location information.

The E911 Messages page allows you to view and edit the messages that can be displayed on an off-premise device. The Find-List for these messages is different than the traditional Find-List. Instead of listing individual messages, the list is shown as message sets based on the language, for example English, American. Selecting a language takes you to the page where you can edit and save the messages.

E911 Messages Setup

Users of devices designated for off-premises use are first presented with various messages, which assure that users are aware of the need to provide correct location information.

The **E911 Messages** page allows you to view and edit the messages that can be displayed on an off-premise device. The Find-List for these messages is different than the traditional Find-List. Instead of listing individual messages, the list is shown as message sets based on the language, for example English, American. Selecting a language takes you to the page where you can edit and save the messages.

Set up E911 Messages

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

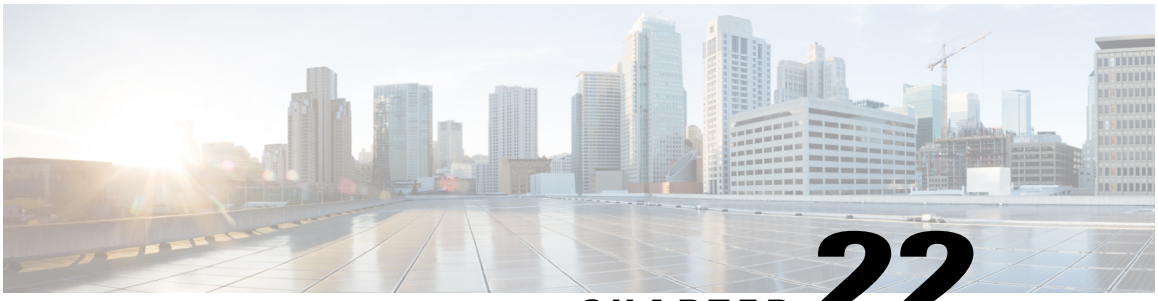
Procedure

Step 1 Choose **System** > **E911 Messages**.

Step 2 Select the required language link of the E911 messages.
The **E911 Messages Configuration** page displays the Agreement, Disclaimer, and Error messages.

Step 3 Optionally, you can edit the E911 messages to be displayed on off-premises devices.

Step 4 Click **Save**.



CHAPTER 22

Enterprise Parameter Setup

This chapter provides information to update existing enterprise parameters or synchronize enterprise-parameter configuration changes with affected devices.

About Enterprise Parameter Setup

Enterprise parameters provide default settings that apply to all devices and services in the same cluster. (A cluster comprises a set of Cisco Unified Communications Managers that share the same database.) When you install a new Cisco Unified Communications Manager, it uses the enterprise parameters to set the initial values of its device defaults. For more information on device defaults, see topics related to system-level configuration settings in the *Cisco Unified Communications Manager System Guide*.

Many of the enterprise parameters rarely require change. Do not change an enterprise parameter unless you fully understand the feature that you are changing or unless the Cisco Technical Assistance Center (TAC) specifies the change.

Caution Changes you make to enterprise parameters using Cisco Unified Communications Manager Administration also changes the enterprise parameter settings for IM and Presence Service clusters in your deployment.

Tip To view the descriptions of all enterprise parameters, click the ? button in the Enterprise Parameters Configuration window.

Clicking the Set to Default button updates all parameters to the suggested value, which is the default that displays on the right side of the parameter. If a parameter does not have a suggested value, Cisco Unified Communications Manager does not update the value when you click the Set to Default button; for example, the Phone URL Parameters in the Enterprise Parameters Configuration window do not display a suggested value, so clicking the Set to Default button does not change the value that you configured.

Related Topics

Device Defaults Setup , on page 701

Update Enterprise Parameters

Procedure

Step 1 Choose **System** > **Enterprise Parameters**.

Step 2 Update the appropriate parameter settings.
To view the description of a particular enterprise parameter, click the parameter name. To view the descriptions of all the enterprise parameters, click the ? button.

Step 3 To save the changes in the database, click Save.

Synchronize Enterprise Parameters with Devices

To synchronize devices with Enterprise Parameters that have undergone configuration changes, perform the following procedure, which applies any outstanding configuration settings in the least-intrusive manner possible. (For example, a reset/restart may not be required on some affected devices.)

Procedure

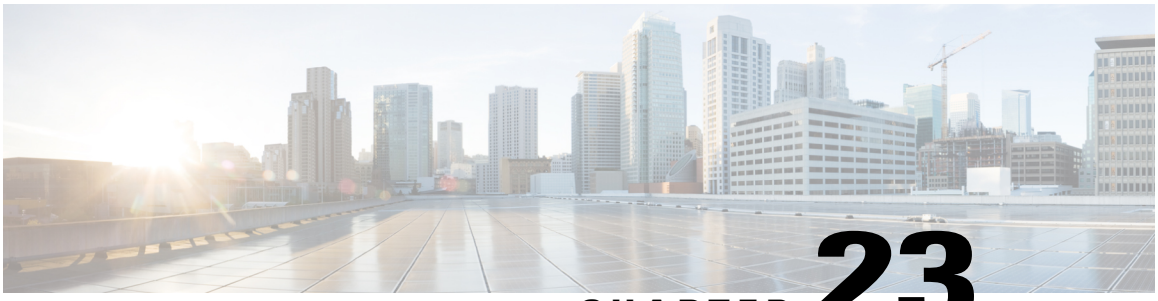
Step 1 Choose **System** > **Enterprise Parameters**.
The Enterprise Parameters Configuration window displays.

Step 2 Make any necessary configuration changes.

Step 3 Click Save.

Step 4 Click Apply Config.
The Apply Configuration Information dialog displays.

Step 5 Click OK.



CHAPTER 23

Enterprise Phone Setup

This chapter provides information to configure the Enterprise Phone parameters. In the Enterprise Phone Configuration window, you can configure parameters that apply to all phones that support these parameters.

- Set Up Enterprise Phone Parameters , page 149

Set Up Enterprise Phone Parameters

To configure parameters in the Enterprise Phone Configuration window, use the following procedure.

Procedure

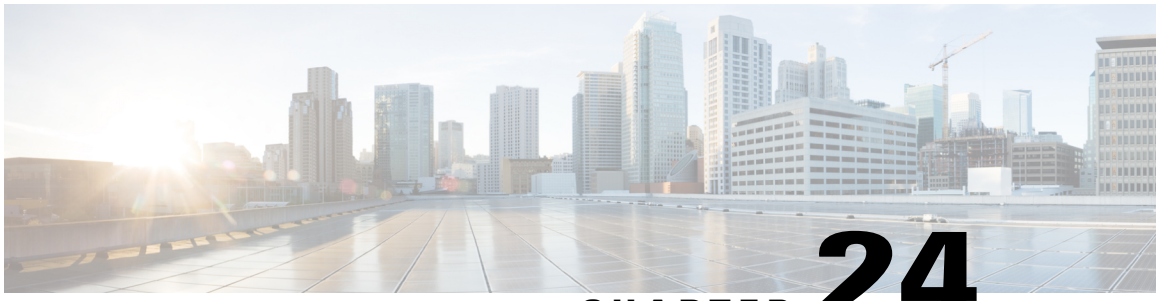
Step 1 Choose **System** > **Enterprise Phone Configuration**.

Step 2 Update the parameter settings as desired.
Select the "Override Common Settings" check box for each setting that you wish to update. If you do not check this box, the corresponding parameter setting does not take effect.

To view the descriptions of all the enterprise phone parameters, click the ? button.

Step 3 To save the changes in the database, click Save.

Note Parameters that you set in this window may also appear in the Common Phone Profile Configuration window and in the Phone Configuration window for various devices. If you set these same parameters in these other windows too, the following order determines the setting that takes precedence: 1) Phone Configuration window settings, 2) Common Phone Profile window settings, 3) Enterprise Phone Configuration window settings.



CHAPTER 24

Service Parameter Setup

This chapter provides information to configure and display different services on selected servers using Cisco Unified Communications Manager. You can view a list of service parameters and their descriptions by clicking the ? icon in the Service Parameter Configuration window.

Note For information about what happens to service parameter values during an upgrade, see *Upgrading Cisco Unified Communications Manager*.

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

About Server Service Parameter Setup

In Cisco Unified Communications Manager Administration, use the **System** > **Service Parameters** menu path to configure service parameters.

Service parameters for Cisco Unified Communications Manager allow you to configure different services on selected servers. You can view a list of parameters and their descriptions by clicking the ? icon in the Service Parameter Configuration window.

If you deactivate a service by using Cisco Unified Serviceability, Cisco Unified Communications Manager retains any updated service parameter values. If you start the service again, Cisco Unified Communications Manager sets the service parameters to the changed values.

Consider the following information before you configure the service parameters in the Service Parameters Configuration window:

- For information about what happens to service parameter values during an upgrade, see Upgrading Cisco Unified Communications Manager.

- To configure service parameters, you must select a single server and a single service on that server. After you make the selection you can configure parameters for the service on that single serve and on others that apply to the service on all servers within the cluster; these get marked as clusterwide.
  Unlike enterprise parameters that apply to all services, each service gets configured with a separate set of service parameters.
- Feature services, which display under Service Activation and Control Center–Feature Services in Cisco Unified Serviceability, can display as active or inactive in the Service Parameters Configuration window. If you activated the feature service in Cisco Unified Serviceability, the service displays as active in the Service Parameters Configuration window; for example, Cisco CallManager (active). If you have not activated the feature service, the service displays as inactive in the Service Parameters Configuration window.
- Network services, which display under Control Center–Network Services in Cisco Unified Serviceability, always display as active in the Service Parameters Configuration window; for example, Cisco DRF Master (active). With network services, you do not need to start the service in Cisco Unified Serviceability because it automatically runs on the server after the Cisco Unified Communications Manager installation/upgrade.
  In the Service Parameters Configuration window, be aware that network services display as active even for dummy nodes, which are servers that display in the Server Configuration window in Cisco Unified Communications Manager Administration but that do not have Cisco Unified Communications Manager installed on them.

  For more information about Cisco Unified Communications Manager services, see the Cisco Unified Serviceability Administration Guide.
- In the Server drop-down list box in the Service Parameter Configuration window, all servers, including dummy nodes, display as active; for example, <server name> (active). In this case, active means that you provisioned the server in Cisco Unified Communications Manager Administration.
- If you deactivate a service by using Cisco Unified Serviceability, Cisco Unified Communications Manager retains any updated service parameter values. If you start the service again, Cisco Unified Communications Manager sets the service parameters to the changed values.
- Clicking the Set to Default button updates all parameters to the suggested value, which is the default that displays on the right side of the parameter. If a parameter does not have a suggested value, Cisco Unified Communications Manager does not update the value when you click the Set to Default button; for example, the Mobile Voice Access service parameter for the Cisco CallManager service does not display a suggested value, so clicking the Set to Default button does not change the value that you enter for this parameter.

Caution Some changes to service parameters may cause system failure. Cisco recommends that you do not make any changes to service parameters unless you fully understand the feature that you are changing or unless the Cisco Technical Assistance Center (TAC) specifies the changes.

Note You can configure a SIP trunk to use a DNS SRV port on a Cisco Unified Presence server as a destination. If you use a SIP trunk with a DNS SRV destination to configure the CUP Publish Trunk service parameter and then modify the DNS record, you must restart all devices (phones) that previously published, so they point to the correct Cisco Unified Presence server destination.

Set Up Server Service Parameters

You can configure the service parameters for a particular service on a particular server.

Before You Begin

Ensure the following prerequisites are met before proceeding with the steps:

- Make sure that servers are configured.
- Make sure that the service is available on the servers. The Service Parameter Configuration window displays all the available services. For more information on services, see the *Cisco Unified Serviceability Administration Guide* for more information.

Procedure

Step 1 Choose **System** > **Service Parameters**.

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

Step 3 From the Service drop-down list box, choose the service that contains the parameter that you want to update.

Note The Service Parameter Configuration window displays all services (active or not active).

The Service Parameter Configuration window displays.

Step 4 Update the appropriate parameter value. To set all service parameters for this instance of the service to the default values, click the Set to Default button.

To view a list of parameters and their descriptions, click the ? icon. To view the list with a particular parameter at the top, click that parameter in the Service Parameter Configuration window.

Note Some services contain service parameters that should rarely be changed. Cisco Unified Communications Manager Administration does not automatically display these parameters when you access the Service Parameter Configuration window. To view all parameters, click Advanced. After all parameters display, you can redisplay the basic parameters by clicking Condensed. If the Advanced button is disabled, all parameters for that service display by default.

Step 5 Click Save.

The window refreshes, and Cisco Unified Communications Manager updates the service parameter with your changes.

Related Topics

Server Setup , on page 27
About Server Service Parameter Setup , on page 151

Display Service Parameters

You may need to compare all service parameters that belong to a particular service on all servers in a cluster. You may also need to display only out-of-sync parameters (that is, service parameters for which values differ from one server to another) or parameters that have been modified from the suggested value.

Use the following procedure to display the service parameters for a particular service on all servers in a cluster.

Procedure

Step 1 Choose **System** > **Service Parameters**.

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

Step 3 From the Service drop-down list box, choose the service for which you want to display the service parameters on all servers in a cluster.

Note The Service Parameter Configuration window displays all services (active or not active).

Step 4 In the Service Parameter Configuration window that displays, choose Parameters for All Servers in The Related Links Drop-down List Box; then, click Go.
The Parameters for All Servers window displays. For the current service, the list shows all parameters in alphabetical order. For each parameter, the suggested value displays next to the parameter name. Under each parameter name, a list of servers that contain this parameter displays. Next to each server name, the current value for this parameter on this server displays.

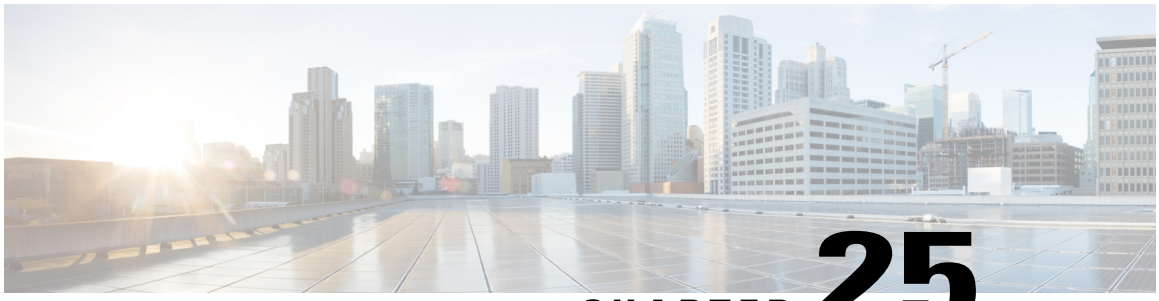
For a given parameter, click on the server name or on the current parameter value to link to the corresponding service parameter window to change the value. Click Previous and Next to navigate between Parameters for All Servers windows.

Step 5 If you need to display out-of-sync service parameters, choose Out of Sync Parameters for All Servers in the Related Links drop-down list box, then click Go.
The Out of Sync Parameters for All Servers window displays. For the current service, service parameters that have different values on different servers display in alphabetical order. For each parameter, the suggested value displays next to the parameter name. Under each parameter name, a list of servers that contain this parameter displays. Next to each server name, the current value for this parameter on this server displays.

For a given parameter, click the server name or the current parameter value to link to the corresponding service parameter window to change the value. Click Previous and Next to navigate between Out of Sync Parameters for All Servers windows.

Step 6 If you need to display service parameters that have been modified from the suggested value, choose Modified Parameters for All Servers in the Related Links drop-down list box; then, click Go.
The Modified Parameters for All Servers window displays. For the current service, service parameters that have values that differ from the suggested values display in alphabetical order. For each parameter, the suggested value displays next to the parameter name. Under each parameter name, a list of servers that have different values from the suggested values displays. Next to each server name, the current value for this parameter on this server displays.

For a given parameter, click the server name or the current parameter value to link to the corresponding service parameter window to change the value. Click Previous and Next to navigate between Modified Parameters for All Servers windows.



CHAPTER 25

Application Server Setup

This chapter provides information about working with and configuring application servers in Cisco Unified Communications Manager Administration.

For additional information, see topics related to Cisco Unity messaging integration in the *Cisco Unified Communications Manager System Guide*.

About Application Server Setup

In Cisco Unified Communications Manager Administration, use the **System** > **Application Server** menu path to configure application servers.

You can use the Application Server windows in Cisco Unified Communications Manager Administration to maintain associations between the Cisco Unified Communications Manager and off-cluster, external applications, such as Cisco Unity Connection, Cisco Unified CM IM and Presence, and Cisco Emergency Responder, and to synchronize Cisco Unified Communications Manager systems and applications, such as Cisco Web Dialer.

Tip Application server configuration does not support Cisco Unity Connection 2.x. To push a list of valid user templates for Cisco Unity Connection 2.x to Cisco Unified Communications Manager, create an AXL connection via Cisco Unity Connection 2.x, as described in the System Administration Guide for Cisco Unity Connection.

Application Server Configuration Tips

You can configure the application servers in Cisco Unified Communications Manager Administration after both the Cisco Unified Communications Manager servers and any other application servers are set up and fully operational and are running with a valid configuration.

Note For Cisco Unity and Cisco Unity Connection, make sure that AXL is running on the Cisco Unified Communications Manager server that was configured to communicate with the Cisco Unity and Cisco Unity Connection server.

Application Server Settings

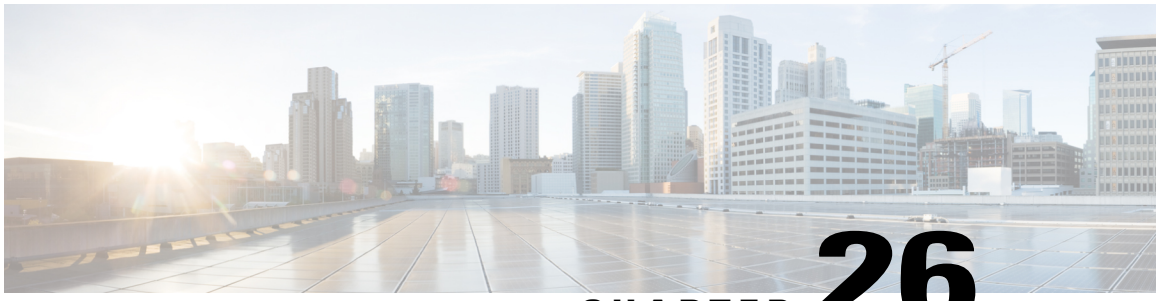
The following table describes all the available settings in the Application Server window. Because each server requires different settings, not all the settings in the table below apply to each server.

Table 25: Application Server Settings

Field	Description
Application Server Information	
Application Server Type	Choose the applicable application server for the type of application to which you want to connect (for example, to connect to a presence application server, choose Cisco Unified CM IM and Presence).
Name	Enter a name to identify the application server that you are configuring.
IP Address	Enter the IP address of the server that you are configuring. **Note** Ensure the IP address is numeric with a number pattern between 1-255 (10.255.172.57). **Tip** For Cisco Unity and Cisco Unity Connection, you must use the same Administrator user name and password that you defined in Cisco Unity and Cisco Unity Connection Administration. This user ID provides authentication between Cisco Unity or Cisco Unity Connection and Cisco Unified Communications Manager Administration.
URL	Enter a URL for the application server.
End User URL	Enter a URL for the end users that are associated with this application server.
Available Application Users	This pane displays the application users that are available for association with this application server. To associate an application user with this application server, select the application user (for example, CCMAdministrator, CCMSysUser, UnityConnection, and so on) and click the Down arrow below this pane.
Selected Application Users	This pane displays the application users that are associated with the application server. To remove an application user, select the application user and click the Up arrow above this pane. To add an application user, select an application user in the Available Application Users pane and click the Down arrow.

Related Topics

Application Server Setup , on page 155



CHAPTER 26

Autoregistration Setup

This chapter provides information to configure, enable, and disable autoregistration, as well as information to reuse autoregistration numbers.

About Autoregistration Setup

Use autoregistration if you want Cisco Unified Communications Manager to assign directory numbers automatically to new phones as they connect to the Cisco Unified Communications IP telephony network.

Note Cisco recommends that you use autoregistration to add fewer than 100 phones to your network. To add more than 100 phones to your network, use the Bulk Administration Tool (BAT).

After a phone has autoregistered, you can move it to a new location and assign it to a different device pool without affecting its directory number.

Autoregistration Settings

The following table describes the autoregistration settings.

Table 26: Autoregistration Settings

Field Name	Description
Universal Device Template	Select the required Universal Device Template from the drop-down list. If no Universal Device Template is created, you can select Default Universal Device Template.
Universal Line Template	Select the required Universal Line Template from the drop-down list. If no Universal Line Template is created, you can select Default Universal Line Template.
Starting Directory Number	Enter the first directory number to use for autoregistration of devices. Specifying a range of directory numbers in the Starting Directory Number and Ending Directory Number fields automatically enables autoregistration. Setting the starting and ending directory numbers to the same value disables autoregistration.
Ending Directory Number	Enter the last directory number to use for autoregistration of devices. The Ending Directory Number must be greater than the Starting Directory Number which automatically enables autoregistration. Setting the starting and ending directory numbers to the same value disables autoregistration.
Auto-registration Disabled on this Cisco Unified Communications Manager	Cisco Unified Communications Manager disables autoregistration by default to prevent unauthorized connections to the network. When autoregistration is disabled, you must configure the directory numbers manually whenever you add new devices to your network. • Uncheck the Auto-registration Disabled option to enable autoregistration for this Cisco Unified Communications Manager. • Check the Auto-registration Disabled option to disable autoregistration for this Cisco Unified Communications Manager. You can disable autoregistration by setting the Starting Directory Number and Ending Directory Number to the same value. If starting and ending directory numbers are specified when you disable autoregistration by checking this option, Cisco Unified Communications Manager sets the starting and ending directory numbers to the same value. The UDT and ULT information fields also reset when you disable autoregistration.

Enable Autoregistration

This section describes how to enable autoregistration for new devices.

Caution Cisco Unified Communications Manager disables autoregistration by default. Enabling autoregistration carries a security risk in that "rogue" phones can automatically register with Cisco Unified Communications Manager. You should enable autoregistration only for brief periods when you want to perform bulk phone adds.

Configuring mixed mode clusterwide security through the Cisco CTL Client automatically disables autoregistration. If you want to use autoregistration and you have configured security, you must change the clusterwide security mode to non-secure through the Cisco CTL Client.

Before You Begin

Check the following points before you begin to enable autoregistration:

- Ensure that the TFTP server is up and running. Ensure that the DHCP option for TFTP specifies the correct server.
- Check that the Device Defaults Configuration window specifies the correct phone image names for SIP and SCCP. Ensure that these files are available on the TFTP server.
- Ensure that directory numbers are available in the autoregistration range.
- Ensure enough license points are available to register new phones.

Procedure

Step 1 Choose **System** > **Enterprise Parameters**.
The Enterprise Parameters Configuration window displays.

Step 2 In the Auto Registration Phone Protocol drop-down list box, choose either SCCP or SIP.

Step 3 Choose **System** > **Cisco Unified CM**.
The Find and List Cisco Unified Communications Managers window displays. Click Find.

Step 4 From the list of Cisco Unified Communications Managers, choose the Cisco Unified Communications Manager, in the cluster, that you want to enable for autoregistration.

Note Always enable or disable autoregistration only on this Cisco Unified Communications Manager. If you shift the autoregistration function to another Cisco Unified Communications Manager in the cluster, you must reconfigure the appropriate Cisco Unified Communications Managers, the Default Cisco Unified Communications Manager Group, and, possibly, the default device pools.

Step 5 Enter the appropriate Autoregistration Information, as described in Table 26: Autoregistration Settings , on page 160.

Step 6 To save the changes in the database, click Save.

Step 7 Choose **System** > **Cisco Unified CM Group**.
The Find and List Cisco Unified Communications Manager Groups window displays.

Step 8 Click Find.

Step 9 From the list of Cisco Unified Communications Manager groups, choose the group that is enabled for autoregistration. (In most systems, the name of this group specifies Default. You can, however, choose a different Cisco Unified Communications Manager group.)
This group serves as the default Cisco Unified Communications Manager group for devices that autoregister. Ensure that the Selected Cisco Unified Communications Managers list for this group contains the Cisco

Unified Communications Manager that you configured for autoregistration in Enable Autoregistration , on page 160. The Cisco Unified Communications Managers get selected in the order in which they are listed in the Cisco Unified Communications Manager group.

Step 10 If you made any changes to the group configuration, click Save to save the changes in the database.

Step 11 Configure a calling search space specifically for autoregistration. For example, you can use the autoregistration calling search space to limit autoregistered phones to internal calls only.

Step 12 Configure the Default device pool for autoregistration by assigning the Default Cisco Unified Communications Manager Group and autoregistration calling search space to the Default device pool. If you are configuring a separate default device pool for each device type, use the Device Defaults Configuration window to assign the default device pools to the device.

Step 13 Enable autoregistration only during brief periods when you want to install and autoregister new devices (preferably when overall system usage is at a minimum). During other periods, turn autoregistration off to prevent unauthorized devices from registering with Cisco Unified Communications Manager.

Step 14 Install the devices that you want to autoregister.

Step 15 Reconfigure the autoregistered devices and assign them to their permanent device pools.

Step 16 In the Enterprise Parameters Configuration window, set the Auto Registration Phone Protocol setting to SIP or SCCP, whichever is needed.

Step 17 If you autoregister more phones with a different protocol, repeat Step 1, on page 161 through Step 16, on page 162.

Related Topics

Autoregistration Setup , on page 159

Disable Autoregistration

This section describes how to disable autoregistration.

Procedure

Step 1 Choose **System** > **Cisco Unified CM**.

Step 2 From the Cisco Unified Communications Manager list, choose the Cisco Unified Communications Manager where you want to disable autoregistration.

Step 3 To disable autoregistration for this Cisco Unified Communications Manager, click the Auto-registration Disabled on this Cisco Unified Communications Manager check box. (When this box is checked, autoregistration specifies disabled.)

Note You can also disable autoregistration by setting the Starting Directory Number and Ending Directory Number to the same value.

Step 4 To save the changes in the database, click Save.

Step 5 Repeat Step 2, on page 162 through Step 4, on page 162 for each Cisco Unified Communications Manager where you want to disable autoregistration.

Related Topics

Autoregistration Setup , on page 159

Reuse Autoregistration Numbers

When you connect a new device to the network, Cisco Unified Communications Manager assigns the next available (unused) autoregistration directory number to that device. If you manually change the directory number of an autoregistered device, or if you delete that device from the database, Cisco Unified Communications Manager can reuse the autoregistration directory number of that device.

When a device attempts to autoregister, Cisco Unified Communications Manager searches the range of autoregistration numbers that you specified and tries to find the next available directory number to assign to the device. It begins the search with the next directory number in sequence after the last one that was assigned. If it reaches the ending directory number in the range, Cisco Unified Communications Manager continues to search from the starting directory number in the range.

You can use the following procedure to reset the range of autoregistration directory numbers and force Cisco Unified Communications Manager to search from the starting number in the range.

Procedure

Step 1 Choose **System** > **Cisco Unified Communications Manager**.

Step 2 Choose the Cisco Unified Communications Manager where you want to reset autoregistration.

Step 3 Write down the current settings for Starting Directory Number and Ending Directory Number.

Step 4 Click Auto-registration Disabled on this Cisco Unified Communications Manager.

Caution New phones cannot autoregister while autoregistration is disabled.

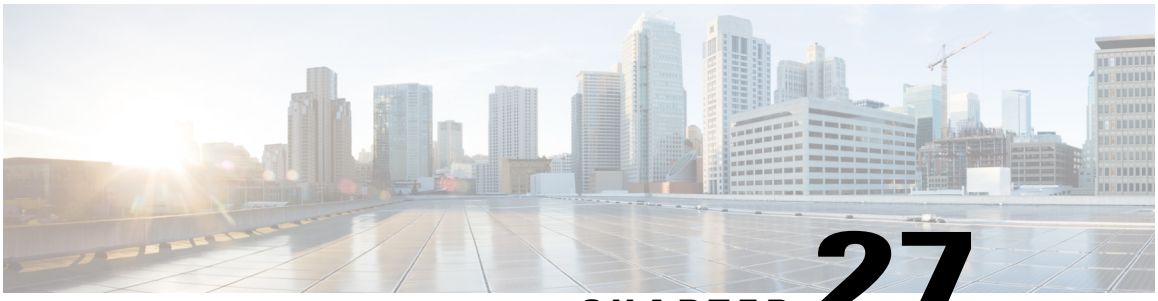
Step 5 Click Save.

Step 6 Set the Starting Directory Number and Ending Directory Number to their previous values (or to new values, if desired).

Step 7 Click Save.

Related Topics

Autoregistration Setup , on page 159



CHAPTER 27

Other System Menu Options

This chapter provides brief descriptions of selected System menu options. A pointer to documents that contain a more detailed description for each of these System menu options is provided.

BLF Presence Group Setup

In Cisco Unified Communications Manager Administration, use the **System** > **BLF Presence Group** menu path to configure BLF presence groups.

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 presence entity, from the device of the watcher.

Cisco Unified Communications Manager controls which destinations a watcher can monitor with BLF presence groups. A BLF presence group contains watchers and the destinations that can be monitored by the watchers in the group. To allow watchers in one group to monitor directory numbers in other groups, you specify permission settings to allow or block (disallow) the BLF presence request. Presence authorization works with the BLF presence groups that are configured to ensure that a watcher has permission to monitor the status of a destination.

After you configure the BLF presence groups, you apply a BLF presence group to the following items in Cisco Unified Communications Manager Administration:

- Directory number—Presence entity for which you want status
- SIP trunk—Watcher
- Phone that is running SIP—Watcher
- Phone that is running SCCP—Watcher
- Application user—Watcher
- End user—Watcher

For information about configuring BLF presence groups, see the *Cisco Unified Communications Manager Features and Services Guide*.

Device Mobility Group Setup

In Cisco Unified Communications Manager Administration, use the **System** > **Device Mobility** > **Device Mobility Group** menu path to configure device mobility groups.

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.

See topics related to device mobility group configuration in the *Cisco Unified Communications Manager Features and Services Guide* for more information on the Device Mobility feature.

Device Mobility Info Setup

In Cisco Unified Communications Manager Administration, use the **System** > **Device Mobility** > **Device Mobility Info** menu path to configure device mobility info.

The Device Mobility Info 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 device mobility subnets that are specified in the Device Mobility Info window and associated with one of the device pools.

The matching subnet becomes the device home subnet for the purpose of device mobility.

See the *Cisco Unified Communications Manager Features and Services Guide* for more information on the Device Mobility feature.

Physical Location Setup

In Cisco Unified Communications Manager Administration, use the **System** > **Physical Location** menu path to configure physical locations.

Physical locations support the Device Mobility feature. Physical locations provide a means of distinguishing the parameters that relate to a specific geographical location from other parameters. For example, a media resources 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, you want to have the media resources server at the roaming location serve the device. By defining the physical location according to availability of media services, 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 may define physical locations based upon a city, enterprise campus, or building.

See topics related to physical location configuration in the *Cisco Unified Communications Manager Features and Services Guide* for more information on the device mobility feature.

Certificate Setup

In Cisco Unified Communications Manager Administration, use the **System** > **Security** > **Certificate** menu path to configure certificates.

Phone Security Profile Setup

In Cisco Unified Communications Manager Administration, use the **System** > **Security** > **Phone Security Profile** menu path to configure phone security profiles.

The Phone Security Profile window includes security-related settings such as device security mode, CAPF settings, digest authentication settings (only for phones that are running SIP), and encrypted configuration file settings. You must apply a security profile to all phones that are configured in Cisco Unified Communications Manager Administration.

For information on configuring and applying a phone security profile, see the *Cisco Unified Communications Manager Security Guide*.

SIP Trunk Security Profile Setup

In Cisco Unified Communications Manager Administration, use the **System** > **Security** > **SIP Trunk Security Profile** menu path to configure SIP trunk security profiles.

The SIP Trunk Security Profile window includes security-related settings such as transport type, device security mode, digest authentication settings, and authorization settings for incoming SIP messages. You must apply a security profile to all SIP trunks that are configured in Cisco Unified Communications Manager Administration.

For information on configuring and applying a SIP trunk security profile, see the *Cisco Unified Communications Manager Security Guide*.

CUMA Server Security Profile Setup

In Cisco Unified Communications Manager Administration, use the **System** > **Security** > **CUMA Server Security Profile** menu path to configure CUMA server security profiles.

The CUMA Server Security Profile window includes security-related settings such as device security mode, incoming transport type, and X.509 subject name. This security profile automatically gets applied to all Cisco

Unified Mobile Communicator clients that you configure in the device configuration window of Cisco Unified Communications Manager Administration.

For information on configuring a Cisco Unity Mobility Advantage (CUMA) server security profile, see the *Cisco Unified Communications Manager Security Guide*. For information on setting up a security profile for a CUMA server, see your Cisco Unified Mobility Advantage documentation. Make sure that the CUMA Security Profile you configure on Cisco Unified Communications Manager matches the security profile on the CUMA servers.

License Usage Report Setup

In Cisco Unified Communications Manager Administration, use the **System** > **Licensing** > **License Usage Report** menu path to configure the license usage report.

Geolocation Setup

In Cisco Unified Communications Manager Administration, use the **System** > **Geolocation Configuration** menu path to configure geographic locations for use with geographic location filters and logical partition policies to provision logical partitioning and other features.

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.

For an explanation of geolocations, location conveyance, and configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*.

For more information on how the logical partitioning feature uses geolocations, see the *Cisco Unified Communications Manager Features and Services Guide*.

Geolocation Filter Setup

In Cisco Unified Communications Manager Administration, use the **System** > **Geolocation Filter** menu path geographic location filters for use with geographic locations and logical partition policies to provision logical partitioning.

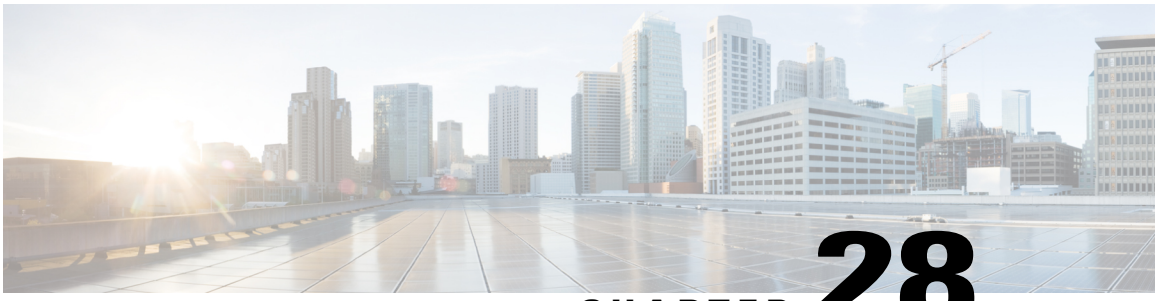
For an explanation of geolocations filters, including configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*.

For more information on how the logical partitioning feature uses geolocation filters, see the *Cisco Unified Communications Manager Features and Services Guide*.

PART III

Call Routing Setup

- Translation Pattern Setup , page 277
- Directory Number Setup , page 289
- Meet-Me Number and Pattern Setup , page 325
- Dial Plan Installer , page 327
- Route Plan Report , page 333
- Calling Party Transformation Pattern Setup , page 339
- Called Party Transformation Pattern Setup , page 343
- Other Call Routing Menu Options , page 347



CHAPTER 28

Automated Alternate Routing Group Setup

This chapter provides information to find, add, update, or delete AAR groups.

For additional information, see topics related to Automated Alternate Routing in the *Cisco Unified Communications Manager System Guide*.

About AAR Group Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **AAR Group** menu path to configure AAR groups.

Automated alternate routing (AAR) provides a mechanism to reroute calls through the PSTN or other network by using an alternate number when Cisco Unified Communications Manager blocks a call due to insufficient location bandwidth. With automated alternate routing, the caller does not need to hang up and redial the called party. The AAR group represents the dialing area where the line/directory number (DN), the Cisco voice mail port, and the gateway are located.

For each AAR group, you enter the prefix digits that are used for automated alternate routing within the AAR group, as well as the prefix digits used for automated alternate routing between a given AAR group and other AAR groups. Devices, such as gateways, phones (by means of directory numbers), and trunks, associate with AAR groups. If automated alternate routing of calls takes place, you may also associate devices with an AAR calling search space.

Note For AAR to function, you must configure AAR groups and also ensure that the Automated Alternate Routing Enable clusterwide service parameter is set to True. (The default value for this service parameter specifies False.)

See topics related to understanding route plans in the *Cisco Unified Communications Manager System Guide* for more information about automated alternate routing groups.

AAR Group Deletion

You cannot delete an AAR group that one or more devices references. To find out which devices are using the AAR group, choose the Dependency Records link from the Related Links drop-down list box that is on the AAR Group Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. You must remove the AAR group from all devices to which it belongs before deleting the AAR group.

Related Topics

Access Dependency Records , on page 982

AAR Group Settings

The following table describes the AAR group settings.

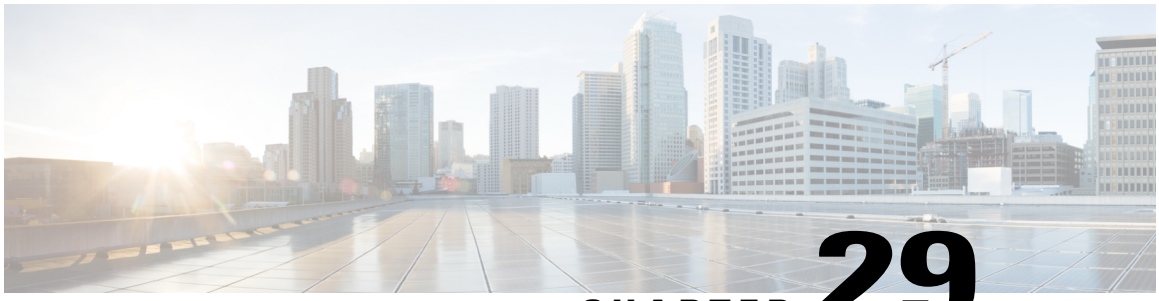
Table 27: AAR Group Settings

Field	Description
Automated Alternate Routing Group Information	
Name	Enter the name that you want to assign to the new AAR group. The name can contain up to 20 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). **Timesaver** Use concise and descriptive names for your AAR groups. The CompanynameLocationGroup format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify an AAR group. For example, CiscoDallasAA1 identifies a Cisco Access Analog AAR group for the Cisco office in Dallas.
Prefix Digits Within	
Prefix Digits	Enter the prefix digits to use for automated alternate routing within this AAR group. Valid entries include numeric characters (0-9), alpha characters (A-D), asterisk (*), pound (#), plus (+), and hyphen (-).
Prefix Digits Between This Group and Other AAR Groups	
Dial Prefix (From this group)	Enter the prefix digits to use for automated alternate routing when routing a call from this group to a device that belongs to another AAR group. Valid entries include numeric characters (0-9), alpha characters (A-D), asterisk (*), and pound (#). **Note** Prefix digits that are entered in this field for the originating AAR group also get added in the Prefix Digits (To this group) field of the AAR destination group.

Field	Description
Dial Prefix (To this group)	Enter the prefix digits to use for automated alternate routing when you are routing a call to this group from a device that belongs to another AAR group. Valid entries include numeric characters (0-9), alpha characters (A-D), asterisk (*), and pound (#). **Note** Prefix digits entered in this field for the destination AAR group also get added in the Prefix Digits (From this group) field of the AAR originating group.

Related Topics

Automated Alternate Routing Group Setup , on page 171



CHAPTER 29

Application Dial Rule Setup

This chapter provides information to configure dial rules.

For additional information about dial rules, see *Cisco Unified Communications Manager System Guide*.

About Application Dial Rule Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Dial Rules** > **Application Dial Rules** menu path to configure application dial rules.

The administrator uses dial rules configuration to add and sort the priority of dialing rules. Dial rules for applications such as Cisco Unified Communications Manager Assistant automatically strip numbers from or add numbers to telephone numbers that a user dials. For example, the dial rules automatically add the digit 9 in front of a 7-digit telephone number to provide access to an outside line.

For example, in Cisco Unified Communications Manager Assistant, the assistant can perform a directory search from the assistant console. The assistant can drag and drop the directory entry to the My Calls panel on the assistant console, which invokes a call to the number that is listed in the entry. The dial rules apply to the number that is listed in the entry before the call gets made.

Application Dial Rules Configuration Tips

When you perform the procedure to add a new dial rule or update an existing dial rule, see the *Cisco Unified Communications Manager System Guide* for dial rule design and error checking.

Note If more than one dial rule exists, you can change the priority of the dial rules.

Related Topics

Reprioritize Dial Rule , on page 177

Application Dial Rule Settings

The following table describes the available settings in the Application Dial Rule Configuration window.

Table 28: Application Dial Rule Settings

Field	Description
Name	Enter a name in the Name field. The name must be at least one character in length and can include up to 50 alphanumeric characters, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>). Ensure each application dial rule name is unique.
Description	Enter a description of the application dial rule in the Description field. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>)
Number Begins With	Enter the initial digits of the directory numbers to which you want to apply this application dial rule. Valid characters include numeric digits (0-9), plus sign (+), asterisk (*), and number sign (#). Be aware that you cannot enter more than 50 characters in this field. For information on special characters that can be used in this field, refer to the Wildcards and special characters in route patterns and hunt pilots section of the Understanding Route Plans chapter of the *Cisco Unified Communications Manager System Guide*.
Number of Digits	Enter the length of the dialed numbers to which you want to apply this application dial rule. This field • Supports numeric characters (0-9) only. • Must contain a value that is equal to or greater than 0 and less than 100.
Total Digits to be Removed	Enter the number of digits that you want Cisco Unified Communications Manager to remove from the beginning of dialed numbers that apply to this dial rule. This field • Supports numeric characters (0-9) only. • Must contain a value that is equal to or greater than 0 and less than 100. • Cannot contain a value that is more than the value in the Number of Digits field.

Field	Description
Prefix With Pattern	Enter the pattern to prepend to dialed numbers that apply to this application dial rule. Valid values include numeric digits (0-9), plus (+), asterisk (*), and pound (#). Be aware that you cannot enter more than 50 characters in this field.
Application Dial Rule Priority	Choose the dial rule priority as top, bottom, or middle.

Related Topics

Application Dial Rule Setup , on page 175

Reprioritize Dial Rule

Perform the following procedure to reprioritize a dial rule.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Call Routing** > **Dial Rules** > **Application Dial Rules**.

Note You can also change the priority by starting from the Application Dial Rules Configuration window.

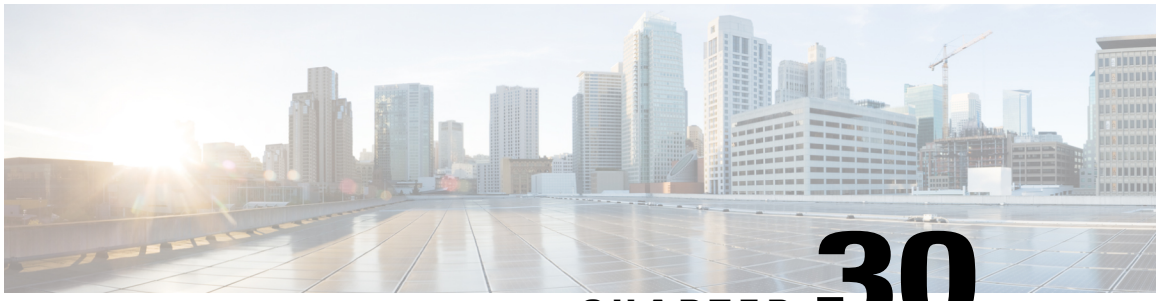
Step 2 In the Find and List Application Dial Rules window, choose a dial rule and click the dial rule name. The Application Dial Rule Configuration window displays.

Step 3 Use the up and down arrows to move the dial rule up or down the list.

Step 4 When you complete prioritizing the order, click Save.

Related Topics

Application Dial Rule Setup , on page 175



CHAPTER 30

Directory Lookup Dial Rule Setup

This chapter provides information about directory lookup dial rules configuration.

For additional information, see topics related to dial rules in the *Cisco Unified Communications Manager System Guide*.

About Directory Lookup Dial Rule Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Dial Rules** > **Directory Lookup Dial Rules** menu path to configure directory lookup dial rules.

Directory lookup rules transform caller identification numbers into numbers that can be looked up in the directory. Each rule specifies which numbers to transform based on the beginning digits and length of the number. For example, you can create a directory lookup rule that automatically removes the area code and 2 prefix digits from a 10-digit telephone, which would transform 4085551212 into 51212. If Cisco Unified Communications Manager Attendant Console can match the number with a user in the speed-dial entries of the attendant or in the directory, the attendant console displays the name in the Call Detail window.

Directory Lookup Dial Rule Settings

The following table describes the available settings in the Phone Configuration window.

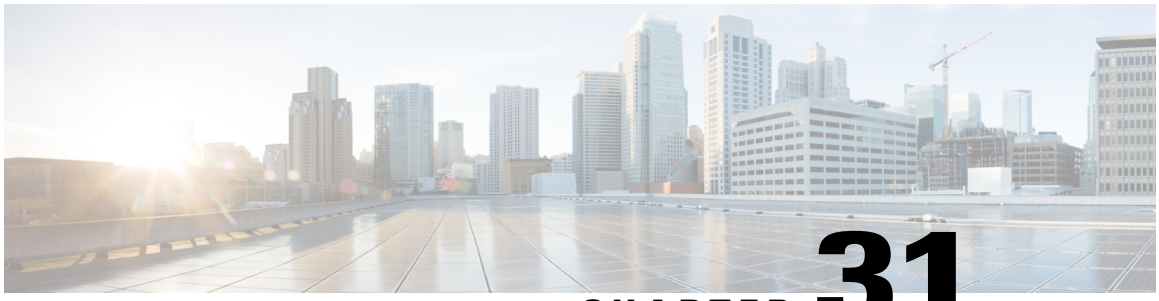
Table 29: Directory Lookup Dial Rule Settings

Field	Description
Name	Enter a name for the directory lookup dial rule. The name can contain up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_).

Field	Description
Description	Enter a description of the directory lookup dial rule in the Description field or leave blank. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), or angle brackets (<>).
Number Begins With	Enter the initial digits of the directory numbers to which you want to apply this directory lookup dial rule. For example, if you enter 972, this dial rule applies to directory numbers that include 9725551212. Valid values include numeric digits (0 through 9), plus (+), asterisk (*), and pound (#).
Number of Digits	Enter the length of the directory numbers to which you want to apply this directory lookup dial rule. For example, if you enter 7, this dial rule applies to directory numbers including 8675309.
Total Digits to be Removed	Enter the number of digits that you want Cisco Unified Communications Manager to remove from directory numbers that apply to this dial rule. For example, if you enter 3, Cisco Unified Communications Manager removes 408 from directory numbers that include 4085556666. Valid values for this field range from 1 to 100. The total digits to be removed cannot be more than the number of digits of the directory numbers that apply to this directory lookup dial rule.
Prefix With Pattern	Enter the pattern to prepend to directory numbers that apply to this directory lookup dial rule. Valid values include digits (0 through 9), plus (+), asterisk (*), and pound (#). **Note** If a prefix pattern is defined, the digits to be removed can equal 0. If the prefix pattern is not defined, the digits to be removed must be greater than 0.

Related Topics

Directory Lookup Dial Rule Setup , on page 179



CHAPTER 31

SIP Dial Rule Setup

This chapter provides information about SIP dial rules configuration.

For additional information, see topics related to dial rules in the *Cisco Unified Communications Manager System Guide*.

About SIP Dial Rule Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Dial Rules** > **SIP Dial Rules** menu path to configure SIP dial rules.

The administrator uses SIP dial rules configuration to configure dial plans for phones that are running SIP and associate them with the following phones that are running SIP:

- Cisco Unified IP Phone 7911, 7941, 7961, 7970, 7971, 9951 and 9971. These phones use the 7940_7960_OTHER dial rules patterns. Key Press Markup Language (KPML) allows the digits to be sent to Cisco Unified Communications Manager digit by digit; SIP Dial Rules allow a pattern of digits to be collected locally on the phone prior to sending to Cisco Unified Communications Manager. If SIP dial rules are not configured, KPML gets used. To increase the performance of Cisco Unified Communications Manager (increasing the number of calls that get processed), Cisco recommends that administrators configure SIP dial rules.
- Cisco Unified IP Phone 7940 and 7960. These phones use the 7940_7960_OTHER dial rules patterns and do not support KPML. If the administrator does not configure a SIP dial plan for these phones, the user must press the Dial softkey or wait a specified time before digits are sent to Cisco Unified Communications Manager for processing. This extra step for the user delays the actual call from being processed.
- Cisco Unified IP Phone 7905 and 7912. These phones use the 7905_7912 dial rules patterns and do not support KPML. If the administrator does not configure a SIP dial plan for these phones, the user must

press the Dial softkey or wait a specified time before digits are sent to Cisco Unified Communications Manager for processing. This extra step for the user delays the actual call from being processed.

If the administrator does not configure a dial plan for a phone that is running SIP, the user must press the Dial softkey unless the phone supports KPML. If the administrator configures SIP dial plans, those dial plans must get associated with a phone that is running SIP, so the dial plans get sent to the device.

Tip When you add or update a SIP dial rule in Cisco Unified Communications Manager Administration, be aware that the Cisco TFTP service rebuilds all phone configuration files, which may cause CPU to spike on the server where the Cisco TFTP service runs, especially if you have a large system with many phones. To ensure that CPU does not spike, add or update the SIP dial rule during a maintenance window or temporarily stop the Cisco TFTP service in Cisco Unified Serviceability before you make the configuration change. If you stop the Cisco TFTP service, remember to restart the service in Cisco Unified Serviceability after you add or update the SIP dial rule.

SIP Dial Rules Configuration Tips

When you add or update a SIP dial rule in Cisco Unified Communications Manager Administration, be aware that the Cisco TFTP service rebuilds all phone configuration files, which may cause CPU to spike on the server where the Cisco TFTP service runs, especially if you have a large system with many phones. To ensure that CPU does not spike, add or update the SIP dial rule during a maintenance window or temporarily stop the Cisco TFTP service in Cisco Unified Serviceability before you make the configuration change. If you stop the Cisco TFTP service, remember to restart the service in Cisco Unified Serviceability after you add or update the SIP dial rule. See topics related to configuring a SIP dial rule for steps that supplement the standard procedure for configuring or updating a record in Cisco Unified Communications Manager Administration.

Related Topics

Set Up SIP Dial Rule , on page 184

SIP Dial Rules Settings

The following table describes the available settings in the SIP Dial Rules Configuration window.

Table 30: SIP Dial Rule Settings

Field	Description
Dial Pattern	Choose the dial pattern that is applicable to the type of phone that is running SIP that you have; for example, dial pattern 7905_7912 applies for Cisco Unified IP Phones 7905 and 7912, and dial pattern 7940_7960_OTHER applies for Cisco Unified IP Phones 7911, 7940, 7941, 7960, 7961, 7970, and 7971. **Note** Cisco Unified IP Phones 7905, 7912, 7940, and 7960 do not support KPML.
SIP Dial Rule Information	

Field	Description
Name	Enter a name for the SIP dial rule; for example, Long Distance. Enter up to 50 alphanumeric characters including spaces and special characters.
Description	Enter a brief description of the dial rule.
Pattern Information	
Pattern Description	Enter a name for the pattern description; for example, Emergency.
Delete Pattern	Check this check box to delete the dial pattern; then, click the Delete Selected button.
Dial Parameter	From this drop-down list box, choose the type of parameter for this pattern from the following choices: • Pattern—Use this parameter for 7905_7912 and 7940_7960_OTHER dial rules. See the Pattern Formats , on page 185 for specific pattern formats. • Button—This parameter specifies the line button to which the dial pattern applies. If the user is initiating a call on line button 1, only the dial pattern that is specified for Button 1 applies. If this optional parameter is not configured, the dial pattern applies to all lines. It only applies to the Cisco Unified IP Phones 7940, 7941, 7960, 7961, 7970, and 7971. The administrator must enter a button number as the value. The button number corresponds to the order of the buttons on the side of the screen that is on the phone, from top to bottom, with 1 being on top. The Cisco Unified IP Phones 7940 and 7941 have two line buttons, the 7960 and 7961 have six line buttons, and the 7970 and 7971 have eight line buttons. • Timeout—This parameter specifies the time, in seconds, before the system times out and dials the number as entered by the user. To have the number dial immediately, specify 0. Use this parameter only for 7940_7960_OTHER dial rules. • User—This parameter represents the tag that automatically gets added to the dialed number. Valid values include IP and Phone for this tag that is not case sensitive. Use this parameter only for 7940_7960_OTHER dial rules.
Value	For the dial parameters that this table describes, enter the value for that field here. For example, enter 1 for Button 1 of PLAR, or 8,..... for a 7940_7960_OTHER pattern.
Delete Parameter	Check this check box to delete the dial pattern; then, click the Delete Selected button.
Edit Parameter	Click this button to update an existing parameter.

Field	Description
Add New Parameter	Click this button to add a new parameter to the pattern.
Delete Selected	Click this button to delete a parameter or a pattern.
Pattern Addition	
Pattern Description	Enter a name for a new pattern; for example, Longdistance; then, click the Add Pattern or Add PLAR button.
Add Pattern	Click this button to add the new pattern to the Pattern Information pane.
Add PLAR	Click this button to add the new PLAR pattern to the Pattern Information pane.

Related Topics

SIP Dial Rule Setup , on page 181

Set Up SIP Dial Rule

Use the standard procedure for configuring or updating a new record when you are configuring or updating a SIP dial rule. The following steps also apply when you configure or update a SIP dial rule.

Procedure

Step 1 From the Dial Pattern drop-down list box, choose either 7905_7912 or 7940_7960_OTHER as the SIP dial rule type.

Step 2 Click the Next button.
The SIP Dial Rule Configuration redisplays with updated information.

Step 3 Enter a name and description of the Dial Rule that you are creating by using the information as described in Table 30: SIP Dial Rule Settings, on page 182. Click Save.
The SIP Dial Rule Configuration redisplays with updated information.

Step 4 Enter a name for the pattern description by using the information as described in Table 30: SIP Dial Rule Settings, on page 182.

Step 5 Depending on the type of dial pattern that you want to create, click Add Pattern or Add PLAR (Private Line Automatic Ringdown [PLAR]).

Note The Add PLAR button only displays for 7940_7960_OTHER dial rules.

The SIP Dial Rule Configuration redisplays with updated information and an area to configure the dial pattern parameters.

Related Topics

SIP Dial Rule Setup , on page 181
Pattern Formats , on page 185
SIP Dial Rules Examples, on page 186

Pattern Formats

Formats are provided for the 7905_7912 and 7940_7960_OTHER patterns.

Value for 7905_7912 Pattern

- Period (.) matches any digit.
- Hyphen (-) means more digits can be entered. If this character is needed, it must appear at the end of an individual rule. For example, 1408t5- is legal, but 1408t5-3... is illegal.
- Pound sign (#) acts as the terminating key, and termination can be applied only after matching hits >#. So >* means that the terminating character specifies the asterisk (*); that is, the terminating key must follow the greater-than sign (>).
- Characters “tn” set the timeout to n seconds.

Note n equals 0-9, and a-z, which ranges from 0 to 26.

- Characters “rn” repeat the last pattern n times.

Note The characters “>#” and “tn” specify modifiers, not patterns. n equals 0-9 and a-z, which ranges from 0 to 26. Use the repeat modifier to specify more rules in less space.

- Modifier “S” causes rule-matching to cease (that is, if a rule matches and the modifier “S” is seen, all other rules after that matching rule do not get used for matching).

Value for 7940_7960_OTHER Pattern

- Period (.) matches any character.
- Pound sign (#) acts as the terminating key, and termination can be applied only after matching hits >#. So >* means that the terminating character specifies the asterisk (*); that is, the terminating key must follow the greater-than sign (>).

Note You must configure the pound sign in the pattern field for it to be valid for 7940_7960_OTHER.

- Asterisk (*) matches one or more characters. The * gets processed as a wildcard character. You can override this by preceding the * with a backward slash (\) escape sequence, which results in the sequence *. The phone automatically strips the \, so it does not appear in the outgoing dial string. When * is received as a dial digit, it gets matched by the wildcard characters * and period (.).
- Comma (,) causes the phone to generate a secondary dial tone.

  Example: 7.... will match any 4-digit DN that starts with 7. 8,..... will match 8, play secondary dial tone (default value), then match any 5-digit DN.

SIP Dial Rules Examples

The following table provides some example SIP dial rules for the 7905_7912 dial rules.

Table 31: SIP Dial Rule Examples for 7905_7912 Dial Rules

Pattern String	Effect
.t7>#.....t4-	You must enter at least one digit. After that, the send occurs after 7 seconds. The terminating # character can also be applied after the first digit is entered. After 7 digits are entered, the timeout changes to 4 seconds. The _ character means that more digits can be entered, as long as timeout or # does not terminate the string.
911 and 9911	Send immediately. Configure a SIP dial rule for each of these strings, with the timeout dial parameter set to 0, to ensure that no delay occurs in sending the call. The user does not have to press the Dial softkey to initiate the call, even if the phone does not support Key Press Markup Language (KPML).
1t7>#.....t1-	You must enter at least one digit. After that, the send occurs after 7 seconds. The terminating character # can also be applied after the first digit is entered. After 10 digits are entered, the timeout changes to 1 second. The _ character means that more digits can be entered, as long as timeout or # does not terminate the string.
0t4>#.t7-"	After a 0, if no other digit is entered, the send occurs after 4 seconds. If another digit is entered, send occurs after 7 seconds. Again, # acts as the terminating digit.

The following table provides some example SIP dial rules for the 7940_7960_OTHER dial rules.

Table 32: SIP Dial Rule Examples for 7940_7960_OTHER Dial Rules

Pattern String	Effect
123#45#6	The 123#45#6 string gets matched if the user dials 123#45#6. Pressing the pound sign (#) does not cause the phone to dial immediately because # is explicitly specified. For Cisco SIP IP Phones 7940 and 7960, dialing 1# or 123#4# causes the phone to dial immediately.

Pattern String	Effect
911 and 9911	Send immediately. Configure a SIP dial rule for each of these strings, with the timeout dial parameter set to 0, to ensure that no delay occurs in sending the call. The user does not have to press the Dial softkey to initiate the call, even if the phone does not support Key Press Markup Language (KPML).
12*345	This example uses the backward slash (\) and asterisk (*) to indicate that the asterisk (*) is a dialed digit. If you omit the backslash (\), the asterisk(*) gets treated as a wildcard pattern match. If you use the backslash (\) with a character other than the asterisk (*), the \ gets ignored, and the \\ character gets matched. If you need to explicitly specify the \ character in a dial plan, use \\. The \ does not get sent out as part of the dialed digit string because the phone removes it before it sends the dial string.

Reset SIP Dial Rule

Perform the following procedure to reset or restart the phone that is running SIP when the SIP dial rule gets updated, so the phone gets updated with the new SIP dial rule.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Call Routing** > **Dial Rules** > **SIP Dial Rules**.

Step 2 Locate the SIP dial rule that you want to reset.

Step 3 Click the SIP dial rule that you want to reset.
The SIP Dial Rule Configuration window displays.

Step 4 Click Reset.
The Device Reset dialog displays.

Step 5 Click one of the following choices:

a) Restart—Restarts the chosen devices without shutting them down (reregisters the phones with Cisco Unified Communications Manager).
b) Reset—Shuts down, then restarts, the device.
c) Close—Closes the Device Reset dialog without performing any action.

Related Topics

SIP Dial Rule Setup , on page 181
About SIP Dial Rule Setup , on page 181

Synchronize SIP Dial Rule Settings with SIP Phones

To synchronize a SIP phone with a SIP Dial Rule that has undergone configuration changes, perform the following procedure, which applies any outstanding configuration settings in the least intrusive manner possible. (For example, a reset/restart may not be required on some affected SIP phones.)

Procedure

Step 1 Choose **Device** > **Dial Rules** > **SIP Dial Rule**.
The Find and List SIP Dial Rules window displays.

Step 2 Choose the search criteria to use.

Step 3 Click Find.
The window displays a list of SIP Dial Rules that match the search criteria.

Step 4 Click the SIP Dial Rule to which you want to synchronize applicable SIP phones. The SIP Dial Rule Configuration window displays.

Step 5 Make any additional configuration changes.

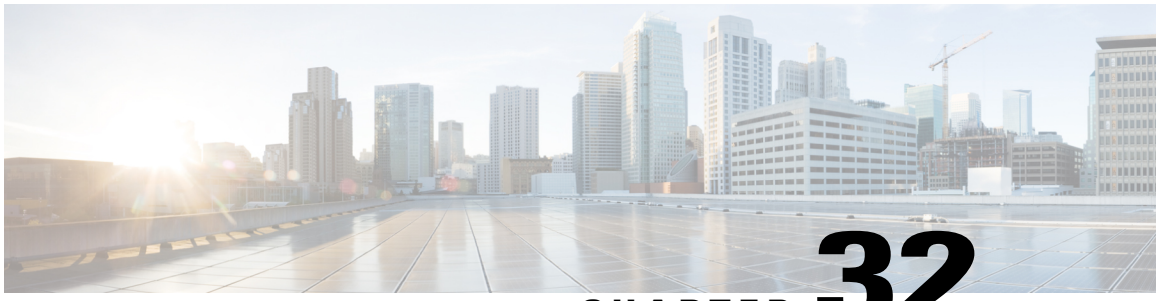
Step 6 Click Save.

Step 7 Click Apply Config.
The Apply Configuration Information dialog displays.

Step 8 Click OK.

Related Topics

SIP Dial Rule Setup , on page 181



CHAPTER 32

Route Filter Setup

This chapter provides information to add, update, copy, or delete a route filter.

For additional information about route plans, see the *Cisco Unified Communications Manager System Guide*.

About Route Filter Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Route Filter** menu path to configure route filters.

Route filters, along with route patterns/hunt pilots, use dialed-digit strings to determine how a call is handled. Route filters only apply when you configure a pattern that contains the at (@) wildcard. When the route pattern/hunt pilot contains the @ wildcard, Cisco Unified Communications Manager routes calls according to the numbering plan that is specified in the Numbering Plan drop-down list box. The route filter window that Cisco Unified Communications Manager displays varies according to the numbering plan that you select.

Route filters allow you to determine which route patterns/hunt pilots your users can dial; for example, whether your users can manually choose a long-distance carrier (by dialing 101 plus a carrier access code).

See topics related to understanding route plans in the *Cisco Unified Communications Manager System Guide* for more information.

Tip Always add and define the route filter first and then add the route filter to the route pattern/hunt pilot.

Route Filter Configuration Tips

Synchronize a route filter with affected devices after you configure or update a route filter.

After you configure or update a route filter, see topics related to adding, editing, and removing route filter clauses.

Related Topics

Add and Edit Route Filter Clauses , on page 191
Remove Route Filter Clauses , on page 192
Synchronize Route Filter Settings with Devices , on page 192

Route Filter Deletion

You cannot delete a route filter that route patterns/hunt pilots, translation patterns, or other items use. To find out which route patterns/hunt pilots, translation patterns, or other items are using the route filter, in the Route Filter Configuration window, choose Dependency Records from the Related Links drop-down list box and click Go. If the dependency records are not enabled for the system, the Dependency Records Summary window displays a message. If you try to delete a route filter that is in use, Cisco Unified Communications Manager displays an error message. Before deleting a route filter that is currently in use, you must perform either or both of the following tasks:

- Assign a different route filter to any route patterns/hunt pilots, translation patterns, or other items that are using the route filter that you want to delete.
- Delete the route patterns/hunt pilots, translation patterns, or other items that are using the route filter that you want to delete.

Related Topics

About Route Pattern Setup , on page 211
About Translation Pattern Setup , on page 277
Translation Pattern Deletions, on page 278
Access Dependency Records , on page 982

Route Filter Settings

The following table describes the route filter settings.

Table 33: Route Filter Settings

Field	Description
Numbering Plan	From the drop-down list, choose a dial plan; for example, North American Numbering Plan. Click Next.
Route Filter Information	

Field	Description
Route Filter Name	Enter a name in the Route Filter Name field. The name can contain up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure each route filter name is unique to the route plan. **Note** Use concise and descriptive names for your route filters. The CompanynameLocationCalltype format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a route filter. For example, CiscoDallasMetro identifies a route filter for tollfree, inter-local access and transport area (LATA) calls from the Cisco office in Dallas.
Clause Information	
Route Filter Tags	Choose the route filter tags and operators and enter data, where appropriate, to create a clause for this route filter. See Table 34: Route Filter Tags , on page 194 for explanations of the route filter tags, such as AREA-CODE.
Route Filter Operators	Choose the route filter tags and operators and enter data, where appropriate, to create a clause for this route filter. See Table 35: Route Filter Operators , on page 195 for explanations of the route filter operators, such as NOT-SELECTED.

Related Topics

Route Filter Setup , on page 189

Add and Edit Route Filter Clauses

Adding route filter clauses allows you to expand upon an existing route filter by incorporating additional operators and entries for existing tags by using a logical OR. You can add route filter clauses either when initially adding a new route filter or when updating an existing route filter.

Editing route filter clauses allows you to modify an existing route filter clause.

This procedure describes adding and editing route filter clauses that comprise an existing route filter.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Call Routing** > **Route Filter**.

Step 2 Locate the route filter to which you want to add or edit route filter clauses.

Step 3 If you want to add a new route filter clause, click Add Clause to display a new Route Filter Clause Configuration data entry window. All the operator fields for this new clause display NOT-SELECTED.

Step 4 Choose the route filter tags and operators and enter data, where appropriate, to create an additional clause for this route filter.

Note See topics related to route filter tag descriptions for help with entering data for route filter tags and operators for the North American Numbering Plan.

Step 5 To add the clause, click Save.
The new clause displays below the existing clauses in the window. (Scroll down, if necessary, to view the new information.)

Step 6 If you want to edit an existing route filter clause, click the Edit Clause button directly above the route filter clause that you want to edit. The Route Filter Clause Configuration window opens to display the current definition of the route filter clause that you chose.

Step 7 Modify the route filter tags and operators and enter data, where appropriate, to edit the route filter clause that you chose to edit.

Step 8 To save your changes to this route filter clause, click Save.

Related Topics

Route Filter Setup , on page 189
Route Filter Tag Descriptions , on page 193

Remove Route Filter Clauses

You can remove route filter clauses either when setting up a new route filter or when updating an existing route filter. This procedure describes removing a route filter clause from an existing route filter.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Call Routing** > **Route Filter**.

Step 2 Locate the route filter from which you want to remove route filter clauses.

Step 3 Scroll down to the top of the clause that you want to remove and click Remove Clause.
A dialog box appears that warns you that you cannot undo the removal of this route filter clause.

Caution Each Remove Clause button applies to the clause immediately below the button. Check carefully to ensure that you are removing the correct clause before initiating this action. If you accidentally remove a clause, you cannot retrieve it, and you must rebuild it.

Step 4 To remove the clause, click OK or to cancel the action, click Cancel. If you click OK, Cisco Unified Communications Manager removes the clause from the route filter.

Related Topics

Route Filter Setup , on page 189

Synchronize Route Filter Settings with Devices

To synchronize devices with a route filter that has undergone configuration changes, perform the following procedure, which applies 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** > **Route Filter**.
The Find and List Route Filters window displays.

Step 2 Choose the search criteria to use.

Step 3 Click Find.
The window displays a list of route filters that match the search criteria.

Step 4 Click the route filter to which you want to synchronize applicable devices. The Route Filter 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 Any necessary resetting of devices that are associated with the route filter causes calls on affected gateways to drop.

Step 8 Click OK.

Related Topics

Route Filter Setup , on page 189

Route Filter Tag Descriptions

The tag serves as the core component of a route filter. A tag applies a name to a subset of the dialed-digit string. For example, the NANP number 972-555-1234 comprises LOCAL-AREA-CODE (972), OFFICE-CODE (555), and SUBSCRIBER (1234) route filter tags.

Route filter tags require operators and can require additional values to decide which calls are filtered.

The values for route filter tag fields can contain the wildcard characters X, *, #, [,], -, ^, and the numbers 0 through 9. (See topics related to special characters and settings for route filters in the *Cisco Unified Communications Manager System Guide* for definitions of wildcard characters.) The descriptions in The following table use the notations [2-9] and XXXX to represent actual digits. In this notation, [2-9] represents any single digit in the range 2 through 9, and X represents any single digit in the range 0 through 9. Therefore, the description The three-digit area code in the form [2-9]XX" means that you can enter the actual digits 200 through 999, or all wildcards, or any mixture of actual digits and wildcards that results in a pattern with that range.

Route filter tags vary depending on the numbering plan that you choose from the Numbering Plan drop-down list box on the Route Filter Configuration window. The following table describes the route filter tags for the North American Numbering Plan.

Table 34: Route Filter Tags

Tag	Description
AREA-CODE	This three-digit area code in the form [2-9]XX identifies the area code for long-distance calls.
COUNTRY CODE	These one-, two-, or three-digit codes specify the destination country for international calls.
END-OF-DIALING	This single character identifies the end of the dialed-digit string. The # character serves as the end-of-dialing signal for international numbers that are dialed within the NANP.
INTERNATIONAL-ACCESS	This two-digit access code specifies international dialing. Calls that originate in the U.S. use 01 for this code.
INTERNATIONAL-DIRECT-DIAL	This one-digit code identifies a direct-dialed international call. Calls that originate in the U.S. use 1 for this code.
INTERNATIONAL-OPERATOR	This one-digit code identifies an operator-assisted international call. This code specifies 0 for calls that originate in the U.S.
LOCAL-AREA-CODE	This three-digit local area code in the form [2-9]XX identifies the local area code for 10-digit local calls.
LOCAL-DIRECT-DIAL	This one-digit code identifies a direct-dialed local call. NANP calls use 1 for this code.
LOCAL-OPERATOR	This one-digit code identifies an operator-assisted local call. NANP calls use 0 for this code.
LONG-DISTANCE-DIRECT-DIAL	This one-digit code identifies a direct-dialed, long-distance call. NANP calls use 1 for this code.
LONG-DISTANCE-OPERATOR	These one- or two-digit codes identify an operator-assisted, long-distance call within the NANP. Operator-assisted calls use 0 for this code, and operator access uses 00.
NATIONAL-NUMBER	This tag specifies the nation-specific part of the digit string for an international call.
OFFICE-CODE	This tag designates the first three digits of a seven-digit directory number in the form [2-9]XX.
SATELLITE-SERVICE	This one-digit code provides access to satellite connections for international calls.
SERVICE	This three-digit code designates services such as 911 for emergency, 611 for repair, and 411 for information.

Tag	Description
SUBSCRIBER	This tag specifies the last four digits of a seven-digit directory number in the form XXXX.
TRANSIT-NETWORK	This four-digit value identifies a long-distance carrier. Do not include the leading 101 carrier access code prefix in the TRANSIT-NETWORK value. See TRANSIT-NETWORK-ESCAPE for more information.
TRANSIT-NETWORK-ESCAPE	This three-digit value precedes the long-distance carrier identifier. The value for this field specifies 101. Do not include the four-digit carrier identification code in the TRANSIT-NETWORK-ESCAPE value. See TRANSIT-NETWORK for more information.

Route filter tag operators determine whether a call is filtered based on the existence, and sometimes the contents, of the dialed-digit string that is associated with that tag. The operators EXISTS and DOES-NOT-EXIST simply check for the existence of that part of the dialed-digit string. The operator == matches the actual dialed digits with the specified value or pattern. The following table describes the operators that can be used with route filter tags.

Table 35: Route Filter Operators

Operator	Description
NOT-SELECTED	Specifies do not filter calls based on the dialed-digit string that is associated with this tag. **Note** The presence or absence of the tag with which the operator is associated does not prevent Cisco Unified Communications Manager from routing the call.
EXISTS	Specifies filter calls when the dialed-digit string that is associated with this tag is found. **Note** Cisco Unified Communications Manager routes or blocks the call only if the dialed-digit string contains a sequence of digits that are associated with the tag.
DOES-NOT-EXIST	Specifies filter calls when the dialed-digit string that is associated with this tag is not found. **Note** Cisco Unified Communications Manager routes or blocks the call only if the dialed-digit string does not contain a sequence of digits that are associated with the tag.
==	Specifies filter calls when the dialed-digit string that is associated with this tag matches the specified value. **Note** Cisco Unified Communications Manager routes or blocks the call only if the dialed-digit string contains a sequence of digits that are associated with the tag and within the numbering range that is specified in the attached field.

Caution Do not enter route filter tag values for tags that are using the operators EXISTS, DOES-NOT-EXIST, or NOT-SELECTED.

Route Filter Examples

Example 1: A route filter that uses AREA-CODE and the operator DOES-NOT-EXIST selects all dialed-digit strings that do not include an area code.

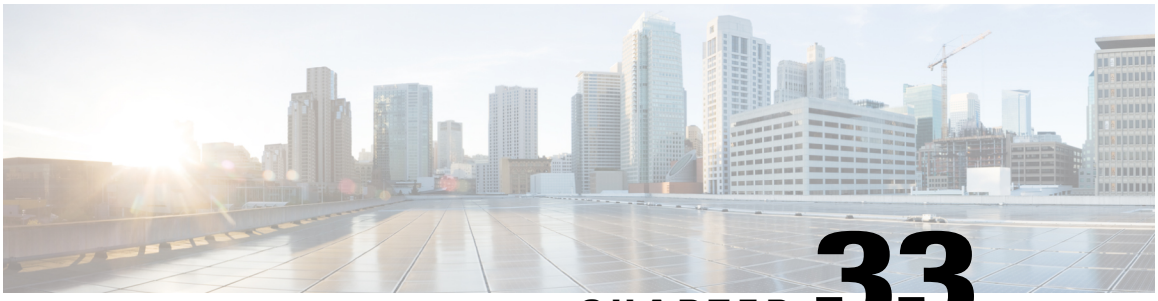
Example 2: A route filter that uses AREA-CODE, the operator ==, and the entry 515 selects all dialed-digit strings that include the 515 area code.

Example 3: A route filter that uses AREA-CODE, the operator ==, and the entry 5[2-9]X selects all dialed-digit strings that include area codes in the range of 520 through 599.

Example 4: A route filter that uses TRANSIT-NETWORK, the operator ==, and the entry 0288 selects all dialed-digit strings with the carrier access code 1010288.

Related Topics

Route Filter Setup , on page 189



CHAPTER 33

Route Group Setup

This chapter provides information to add or delete a route group or to add devices to or to remove devices from a route group.

For additional information about route plans, see the *Cisco Unified Communications Manager System Guide*. See the *Cisco Unified Communications Manager Features and Services Guide* for additional information about local route groups.

About Route Group Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Route/Hunt** Route Group menu path to configure route groups.

Route/Hunt
A route group allows you to designate the order in which gateways and trunks are selected. It allows you to prioritize a list of gateways and ports for outgoing trunk selection.

For example, if you use two long-distance carriers, you could add a route group, so long-distance calls to the less expensive carrier are given priority. Calls route to the more expensive carrier only if the first trunk is unavailable.

Note For information about configuring the Local Route Group feature, see the *Cisco Unified Communications Manager Features and Services Guide*.

Route Group Configuration Tips

After you configure a route group, see the following topics to add or remove devices from a route group:

- Add Devices to Route Group , on page 200
- Remove Devices From Route Group , on page 201

Route Group Deletion

You cannot delete a route group that a route/hunt list references. To find out which route lists are using the route group, in the Route Group Configuration window, choose Dependency Records from the Related Links drop-down list box and click Go. If the dependency records are not enabled for the system, the Dependency Records Summary window displays a message. If you try to delete a route group that is in use, Cisco Unified Communications Manager displays a message. Before deleting a route group that is currently in use, you must perform the following task:

- Remove the route group from all route lists to which it belongs before deleting the route group.

Tip To delete route groups and route patterns, first delete the route pattern; second, delete the route list; and finally, delete the route group.

Related Topics

Remove Route Groups From Route List , on page 209
Access Dependency Records , on page 982

Route Group Settings

The following table describes the route group settings.

Table 36: Route Group Settings

Field	Description
Route Group Information	
Route Group Name	Enter a name for this route group. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that each route group name is unique to the route plan. **Timesaver** Use concise and descriptive names for your route groups. The CompanynameLocationGroup format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a route group. For example, CiscoDallasAA1 identifies a Cisco Access Analog route group for the Cisco office in Dallas.

Field	Description
Distribution Algorithm	Choose a distribution algorithm from the options in the drop-down list box: • Top Down—If you choose this distribution algorithm, Cisco Unified Communications Manager distributes a call to idle or available members starting from the first idle or available member of a route group to the last idle or available member. • Circular—If you choose this distribution algorithm, Cisco Unified Communications Manager distributes a call to idle or available members starting from the (n+1)th member of a route group, where the nth member is the member to which Cisco Unified Communications Manager most recently extended a call. If the nth member is the last member of a route group, Cisco Unified Communications Manager distributes a call starting from the top of the route group. The default value specifies Circular.
Route Group Member Information	
Find Devices to Add to Route Group	
Device Name contains	Enter the character(s) that are found in the device name that you are seeking and click the Find button. Device names that match the character(s) that you entered display in the Available Devices box. **Note** To find all available devices, leave the text box blank and click the Find button.
Available Devices	Choose a device in the Available Devices list box and add it to the Selected Devices list box by clicking Add to Route Group. If the route group contains a gateway that uses the QSIG protocol, only gateways that use the QSIG protocol display in the list. If the route group contains a gateway that uses the non-QSIG protocol, gateways that use the controlled intercluster trunks, which are QSIG protocol, do not display in the list. If you included the route group in a route list that contains QSIG gateways, the H.323 gateways do not display in the list.
Port(s)	If this device supports individually configurable ports, choose the port. (Devices that allow you to choose individual ports include Cisco Access Analog and Cisco MGCP Analog gateways and T1 CAS.) Otherwise, choose the default value (All or None Available, depending upon the device that is chosen). For a device that has no ports available (None Available), the device may already be added to the Route Group or cannot be added to the route group.
Current Route Group Members	

Field	Description
Selected Devices	To change the priority of a device, choose a device name in the Selected Devices list box. Move the device up or down in the list by clicking the arrows on the right side of the list box. To reverse the priority order of the devices in the Selected Devices list box, click Reverse Order of Selected Devices. For more information about the order of devices in a route group, see topics related to route plan overview in the *Cisco Unified Communications Manager System Guide*.
Removed Devices	Choose a device in the Selected Devices list box and add it to the Removed Devices list box by clicking the down arrow button between the two list boxes. **Note** You must leave at least one device in a route group.
Route Group Members	
(list of devices)	This pane displays links to the devices that have been added to this route group. Click one of the device names to go to the configuration window for that particular device. **Note** When you are adding a new route group, this list does not display until you save the route group.

Related Topics

Route Group Setup , on page 197

Add Devices to Route Group

You can add devices to a new route group or to an existing route group. You can add gateways to multiple route groups. After you add a gateway to any route group, the gateway does not display in the Route Pattern configuration window. The following procedure describes adding a device to an existing route group.

Before You Begin

You must define one or more gateway and trunk devices before performing this procedure. A device can reside in only one route group.

Procedure

Step 1 Choose **Call Routing** > **Route/Hunt** > **Route Group**.

Step 2 Locate the route group to which you want to add a device.

Step 3 In the Available Devices list box, choose a device to add and click Add to Route Group to move it to the Selected Devices list box. Repeat this step for each device that you want to add to this route group.

Step 4 In the Selected Devices list box, choose the order in which the new device or devices are to be accessed in this route group. To change the order, click a device and use the Up and Down arrows to the right of the list box to change the order of devices.

Step 5 To add the new device(s) and to update the device order for this route group, click Save.

Related Topics

Route Group Setup , on page 197

Remove Devices From Route Group

You can remove devices from a new route group or from an existing route group. The following procedure describes removing a device from an existing route group.

Procedure

Step 1 Choose **Call Routing** > **Route/Hunt** > **Route Group**.

Step 2 Locate the route group from which you want to remove a device.

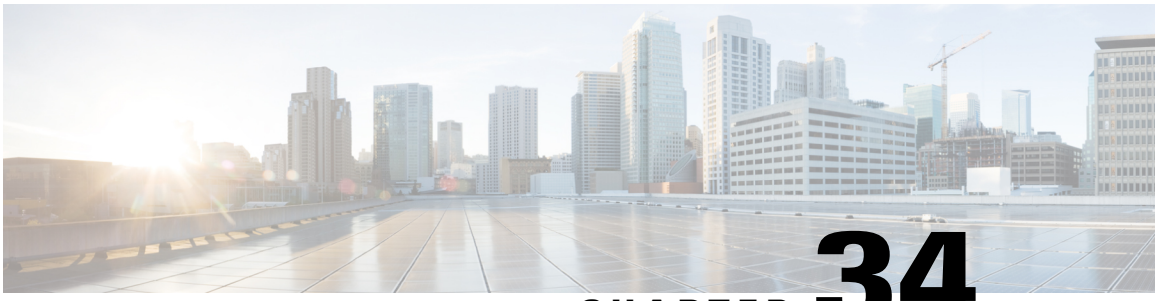
Step 3 In the Selected Devices list box, choose a device to be removed and click the Down arrow below the Selected Devices list box to move the device to the Removed Devices list box. Repeat this step for each device that you want to remove from this route group.

Note You must leave at least one device in a route group.

Step 4 To remove the devices, click Save.

Related Topics

Route Group Setup , on page 197



CHAPTER 34

Local Route Group Names Setup

This chapter provides information about local route group names configuration.

For additional information, see topics related to local route group feature in the *Cisco Unified Communications Manager Features and Services Guide*.

About Local Route Group Names Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Route/Hunt** > **Local Route Group Names** menu path to configure local route group names.

A local route group name is a unique name that you assign to a local route group in the Local Route Group Names window. The Local Route Group Names window allows you to add and configure multiple local route group names that you can customize and associate with route groups for a given device pool.

Note From Cisco Unified Communications Manager Release 10.0(1), a given device pool supports multiple local route groups.

Local Route Group Names Settings

The following table describes the available fields and buttons in the Local Route Group Names window.

Table 37: Local Route Group Names Settings

Field or Button	Description
Name	Enter a unique local route group name in this required field. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscores (_). **Note** The Standard Local Route Group entry in the Name field is a default entry. It is populated from pre-10.0(1) release input. This field is editable. It allows you to change the name to a name of your choice. **Note** The Device Pool Configuration window under **System** > **Device Pool** displays the local route group name entries as labels under Local Route Group Settings.
Description	(Optional) Enter a description that will help you to distinguish between local route group names. You can change the description if required. The description can comprise up to 100 alphanumeric characters except the following characters: ampersand (&), double quotation marks ("), angle brackets (<>), and percent (%).
Add Row	Click this button to add new local route group names. This button adds an empty row below the previous row entry. Enter the name and description of the local route group that you want to add to this row. To delete an existing local route group name, click the **Minus Sign (-)** button at the right corner of the relevant row. Click **Save** to confirm the process. **Note** By default, the **Minus Sign (-)** button in the first row is inactive. **Note** You can delete an existing local route group name only if it does not have any dependency on any device pool or route list. To delete an existing local route group, you must first find the associated device pools as well as the route lists from the dependency record, disassociate them, and then delete the local route group name.
Save	Click this button to save the local route group name entries.

CHAPTER 35

Route List Setup

This chapter provides information to add or delete route lists or to add, remove, or change the order of route groups in a route list.

For additional information about route plans, see the *Cisco Unified Communications Manager System Guide*.

For additional information about local route groups and how presence works with route lists, see the *Cisco Unified Communications ManagerFeatures and Services Guide*.

About Route List Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Route/Hunt** > **Route List** menu path to configure route lists.

A route list associates a set of route groups in a specified priority order. A route list then associates with one or more route patterns and determines the order in which those route groups are accessed. The order controls the progress of the search for available devices for outgoing calls.

A route list can contain only route groups. Each route list should have at least one route group. Each route group includes at least one device, such as a gateway, that is available. Based on device type, Cisco Unified Communications Manager can choose some, or all, ports as resources in each route group. Some devices, such as digital access, only allow you to choose all ports.

You can add a route group to any number of route lists.

Route List Configuration Tips

To begin configuration of a new route list, click the Add New button to display the Route List Configuration window where you configure the new route list.

After you configure a new route list, add at least one route group to the new route list.

After you configure a route list, continue configuration of the route list.

Related Topics

Add Route Groups to Route List , on page 207

Route List Deletion

The Cisco Unified Communications Manager associates a route list with a route pattern. You cannot delete a route list if it associates with a route pattern. To find out which route patterns are using the route list, click the Dependency Records link from the Route List Configuration window. If dependency records are not enabled for the system, the dependency records summary window displays a message.

Tip To delete route groups and route patterns, first delete the route pattern; second, delete the route list, and finally, delete the route group.

Related Topics

Access Dependency Records , on page 982

Route List Settings

The following table describes the route list settings.

Table 38: Route List Settings

Field	Description
Route List Information	
Route List Name	Enter a name for this rout e list. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that each route list name is unique to the route plan. **Warning** Use concise and descriptive names for your route lists. The CompanynameLocationCalltype format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a route list. For example, CiscoDallasMetro identifies a route list for toll-free, inter-local access transport area (LATA) calls from the Cisco office in Dallas.
Description	Enter a description for this route list.

Field	Description
Cisco Unified Communications Manager Group	From this drop-down list box, choose a Cisco Unified Communications Manager group. **Note** The route list registers with the first Cisco Unified Communications Manager in the group, which is its primary Cisco Unified CM. **Note** If you choose a Cisco Unified CM group that has only one configured Cisco Unified CM, you receive the following warning: WARNING! The selected Cisco Unified Communications Manager Group has only one Cisco Unified Communications Manager configured. For the control process to have redundancy protection, please select a Cisco Unified Communications Manager Group with more than one Cisco Unified Communications Manager.
Enable this Route List	By default, the system checks this check box for a new route list. If you want to disable this route list, uncheck this check box. A popup window explains that calls in progress do not get affected, but this route list will not accept additional calls.
Run On All Active Unified CM Nodes	To enable the active route list to run on every node, check this check box.
Save	When you click this button to save a route list, a popup message reminds you that you must add at least one route group to this route list for it to accept calls.
Add Route Group	To add a route group to this route list, click this button and perform the procedure to add a route group to a route list. **Note** For called party and calling party transformation information, you can click the name of a route group that belongs to this route list. The route group names display in the Route List Details list box at the bottom of the Route List Configuration window. This action displays the Route List Detail Configuration window for the route group that you choose.

Related Topics

Route List Setup , on page 205
Add Route Groups to Route List , on page 207

Add Route Groups to Route List

You can add route groups to a new route list or to an existing route list. Route groups can exist in one or more route lists. The following procedure describes adding a route group to an existing route list.

Note You cannot add route groups that contain MGCP gateways that use the QSIG protocol (a QSIG route group) and route groups that contain gateways that use the H.323 protocol (H.323 route group) to the same route list. For more information, see topics related to route groups and route lists in the *Cisco Unified Communications Manager System Guide*.

Before You Begin

Before performing this procedure, you must build one or more route groups and add a route list.

Procedure

Step 1 Choose **Call Routing** > **Route/Hunt** > **Route List**.

Step 2 Locate the route list to which you want to add route group.

Step 3 To add a route group, click Add Route Group.
The Route List Detail Configuration window displays.

Step 4 From the Route Group drop-down list box, choose a route group to add to the route list.

Note If the route list contains a QSIG route group, H.323 route groups do not display in the drop-down list box. If the route group contains a H.323 route group, QSIG route groups do not display in the drop-down list box.

Note When you configure the Local Route Group feature, add the route groups to the route list by selecting those local route group names that are appended with the Local Route Group tag that appears in the drop-down list box.

Note See topics related to local route groups in the *Cisco Unified Communications Manager Features and Services Guide* for details.

Step 5 If you need to manipulate the calling party number on calls that are routed through this route group, set up the calling party transformations in the appropriate fields.

Note For more information on calling party transformations, see the *Cisco Unified Communications Manager System Guide*.

Step 6 If you need to manipulate the dialed digits on calls that are routed through this route group, set up the called party transformations in the appropriate fields.

Note For more information on called party transformations, see the *Cisco Unified Communications Manager System Guide*.

Step 7 To add the route group, click Save.
The route group details information appears in the Route List Details link.

Step 8 To add more route groups to this list, click Add Route Group and repeat Step 3, on page 208 through Step 7, on page 208.

Step 9 When you finish adding route groups to the route list, click Save.

Note See topics related to synchronizing a route list with the affected route groups before deciding whether to proceed to Step 10, on page 208 below.

Step 10 Click Reset for changes to take effect. When the popup windows display, click Reset.

Related Topics

Route List Setup , on page 205

Synchronize Route List Settings with Route Groups , on page 210

Remove Route Groups From Route List

You can remove route groups from a new route list or from an existing route list. The following procedure describes removing a route group from an existing route list.

Procedure

Step 1 Choose **Call Routing** > **Route/Hunt** > **Route List** in the menu bar.

Step 2 Locate the route list from which you want to remove a route group.

Step 3 From the Selected Groups list, choose a route group name.

Note To select multiple route groups from the list, press the Shift key and click the desired route groups.

Step 4 Click the Down Arrow below the Selected Groups list box to move the selected route group to the Removed Groups list.

Step 5 To remove the route group, click Save.
When the window refreshes, click OK to remove the route group from the route list.

Step 6 Click Reset for the changes to take effect. Click Reset in response to the popup windows.

Related Topics

Route List Setup , on page 205

Change Route Group Order in Route List

Cisco Unified Communications Manager accesses route groups in the order in which they appear in the route list. The following procedure allows you to change the access order of route groups.

Procedure

Step 1 Choose **Call Routing** > **Route/Hunt** > **Route List**.

Step 2 Locate the route list in which you want to change the order of a route group.

Step 3 From the Selected Groups list, choose a route group.

Step 4 To move the route group up or down in the list, choose a route group; then, click the up or down arrows on the right side of the list box.

Step 5 Click Save.

Note For called party and calling party transformation information, click the route group icon or route group name in the Route List Details list at left. This action takes you to the Route List Detail Configuration window for the corresponding route group.

Step 6 Click Reset for the changes to take effect. Click Reset in response to the popup windows.

Related Topics

Route List Setup , on page 205

Synchronize Route List Settings with Route Groups

To synchronize route groups with a route list that has undergone configuration changes, perform the following procedure, which applies 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** > **Route/Hunt** > **Route List**.
The Find and List Route Lists window displays.

Step 2 Choose the search criteria to use and click Find.
The window displays a list of route lists that match the search criteria.

Step 3 Check the check boxes next to the route lists to which you want to synchronize applicable route groups. To choose all route lists in the window, check the check box in the matching records title bar.

Step 4 Click Apply Config to Selected.
The Apply Configuration Information dialog displays.

Step 5 Click OK.

Related Topics

Route List Setup , on page 205

CHAPTER 36

Route Pattern Setup

This chapter provides information to find, add, update, copy, or delete a route pattern.

For additional information, see topics related to wildcards and special characters in route patterns and hunt pilots in the *Cisco Unified Communications Manager System Guide*, as well as topics related to route plans and route filter configuration.

For additional information about local route groups, see the *Cisco Unified Communications Manager Features and Services Guide*.

About Route Pattern Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Route/Hunt** > **Route Pattern** menu path to configure route patterns.

A route pattern comprises a string of digits (an address) and a set of associated digit manipulations that route calls to a route list or a gateway. Route patterns provide flexibility in network design. They work in conjunction with route filters and route lists to direct calls to specific devices and to include, exclude, or modify specific digit patterns.

See topics related to understanding route plans in the *Cisco Unified Communications Manager System Guide* for more detailed route pattern information.

Note See topics related to local route groups in the *Cisco Unified Communications Manager Features and Services Guide* for a discussion of route patterns and their use and configuration when the Local Route Group feature is configured.

Route Pattern Configuration Tips

Before you begin, ensure that the following items are configured in Cisco Unified Communications Manager:

- Gateway

- Route list
- Partition (unless you are using <None>)
- Route filter (unless you are using <None>)

Timesaver Assigning 8XXX to a gateway routes all directory numbers 8000 to 8999 out the gateway. Similarly, 82XX routes directory numbers 8200 to 8299. See topics related to special characters and settings in the *Cisco Unified Communications Manager System Guide* for more information about wildcards.

Note If you change the gateway or route list, you must click Save prior to choosing the Edit link. Otherwise, you get linked to the previous gateway or route list.

Note The (Edit) link next to the Gateway or Route List field takes you to the Gateway Configuration or Route List Configuration window for reference, depending on whether the Gateway or Route List field contains a gateway or a route list. The Gateway Configuration window displays devices that are associated with the specified gateway. The Route List Configuration window displays the route groups that are associated with the specified route list.

Route Pattern Settings

The following table describes the available fields in the Route Pattern Configuration window.

Table 39: Route Pattern Settings

Field	Description
Pattern Definition	
Route Pattern	Enter the route pattern, including numbers and wildcards (do not use spaces); for example, for 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 +. **Note** Ensure that the directory route pattern, which uses the chosen partition, route filter, and numbering plan combination, is unique. Check the route pattern, translation pattern, directory number, call park number, call pickup number, message waiting on/off, or meet me number if you receive an error that indicates duplicate entries. You can also check the route plan report. See topics related to wildcards and special characters in route patterns and hunt pilots in the *Cisco Unified Communications Manager System Guide* for more information about wildcards.

Field	Description
Route Partition	If you want to use a partition to restrict access to the route pattern, choose the desired partition from the drop-down list box. If you do not want to restrict access to the route pattern, 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, then find and choose a 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 route pattern, route filter, and partition is unique within the Cisco Unified Communications Manager cluster.
Description	Enter a description of the route 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.
Route Filter	If your route pattern includes the @ wildcard, you may choose a route filter. The optional act of choosing a 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. You can configure the number of items that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more route filters 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 Route Filters window, then find and choose a route filter name. **Note** To set the maximum list box items, choose **System** > **Enterprise Parameters** and choose CCMAdmin Parameters.

Field	Description
MLPP Precedence	Choose an MLPP precedence setting for this route 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. **Note** See topics related to multilevel precedence and preemption in the *Cisco Unified Communications Manager Features and Services Guide* for more information. **Note** You cannot configure the Multilevel Precedence Preemption (MLPP) level on the Route Pattern page to flash, flash override, or executive override levels if you want to enable the DCC feature. You must set the MLPP level to these levels at the translation pattern instead.
Apply Call Blocking Percentage	Check this check box to enable the Destination Code Control (DCC) feature. By enabling DCC, all calls other than flash and higher precedence calls made to the destination are filtered and allowed or disallowed based on the Call Blocking Percentage quota set for the destination. Flash and higher precedence calls are allowed at all times. DCC is disabled by default. **Note** The Apply Call Blocking Percentage field gets enabled only if the MLPP level is immediate, priority, routine or 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 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 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.
Resource Priority Namespace Network Domain	Choose a Resource Priority Namespace Network Domain from the drop-down list box. To configure the Resource Priority Namespace Network Domains, choose **System** > **MLPP** > **Namespace** > **Resource Priority Namespace Network Domain**. See the *Cisco Unified Communications Manager Features and Services Guide* for more information.

Field	Description
External Call Control Profile	In Cisco Unified Communications Manager, you enable external call control by assigning an external call control profile to a route pattern. If the route pattern has an external call control profile assigned to it, when a call occurs that matches the route 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. For more information on external call control, see topics related to external call control in the *Cisco Unified Communications Manager Features and Services Guide*. From the drop-down list box, choose the external call profile that you want to assign to the route 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.
Gateway/Route List	Choose the gateway or route list for which you are adding a route pattern. **Note** If the gateway is included in a Route Group, this drop-down list box does not display the gateway. When a gateway is chosen in the drop-down list box, Cisco Unified Communications Manager uses all the ports in the gateway to route/block this route pattern. This action does not apply for MGCP gateways.

Field	Description
Route Option	The Route Option designation indicates whether you want this route 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 route 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
Call Classification	Call Classification indicates whether the call that is routed through this route pattern is considered either off (OffNet) or on (OnNet) the local network. The default value specifies OffNet. When adding a route pattern, if you uncheck the Provide Outside Dial Tone check box, you set Call Classification as OnNet.
Allow Device Override	This check box remains unchecked by default. When the check box is checked, the system uses the Call Classification setting that is configured on the associated gateway or trunk to consider the outgoing call as OffNet or OnNet.
Provide Outside Dial Tone	Check this check box to provide outside dial tone. To route the call in the network, leave the check box unchecked.
Allow Overlap Sending	With overlap sending enabled, when Cisco Unified Communications Manager passes a call to the PSTN, it relies on overlap sending in the PSTN to determine how many digits to collect and where to route the call. Check this check box for each route pattern that you consider to be assigned to a gateway or route list that routes the calls to a PSTN that supports overlap sending. 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, the system disables the Allow Overlap Sending check box.
Urgent Priority	If the dial plan contains overlapping route patterns, Cisco Unified Communications Manager does not route the call until the interdigit timer expires (even if dialing a sequence of digits to choose a current match is possible). Check this check box to interrupt interdigit timing when Cisco Unified Communications Manager must route a call immediately.

Field	Description
Require Forced Authorization Code	If you want to use forced authorization codes with this route pattern, check this check box. The FAC feature does not support overlap sending because the Cisco Unified Communications Manager cannot determine when to prompt the user for the code. If you check the Allow Overlap Sending check box, the system disables the Require Forced Authorization Code check box.
Authorization Level	Enter the authorization level for the route pattern. The number that you specify in this field determines the minimum authorization level that is needed to successfully route a call through this route pattern. **Tip** To activate the authorization code, you must check the Require Forced Authorization Code. If you do not check the check box, a message displays when you insert the route pattern that indicates that the authorization code cannot be activated. To activate the code, click Cancel, check the Require Forced Authorization Code check box, and click Insert. To activate the code at a later time, click OK.
Require Client Matter Code	If you want to use client matter codes with this route pattern, check this check box. The CMC feature does not support overlap sending because the Cisco Unified Communications Manager cannot determine when to prompt the user for the code. If you check the Allow Overlap Sending check box, the Require Client Matter Code check box become disabled.
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. You may also configure an External Phone Number Mask on all phone devices. **Note** The calling party transformation settings that are assigned to the route groups in a route list override any calling party transformation settings that are assigned to a route pattern that is associated with that route list.
Calling Party Transform Mask	Enter a transformation mask value. Valid entries for the National Numbering Plan include the digits 0 through 9; the wildcard characters X, 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. See topics related to calling party number transformation settings in the *Cisco Unified Communications Manager System Guide* for more information.
Prefix Digits (Outgoing Calls)	Enter prefix digits in the Prefix Digits (Outgoing Calls) field. Valid entries for the National Numbering Plan 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.

Field	Description
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 route 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.
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 route 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.
Calling Party Number Type	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 Unified Communications Manager—The Cisco Unified Communications Manager sets the directory number type. • Unknown—Use 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.

Field	Description
Calling Party Numbering Plan	Choose the format for the numbering plan in calling party directory numbers. Cisco Unified Communications Manager sets the calling DN numbering plan. 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 PBXs by using routing as a non national type number. Choose one of the following options: • Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the Numbering Plan in the directory number. • ISDN—Use when you are dialing outside the dialing plan for your country. • National Standard—Use when you are dialing within the dialing plan for your country. • Private—Use when you are dialing within a private network. • Unknown—Use when the dialing plan is unknown.
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 route 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. If a call that originates from an IP phone on Cisco Unified Communications Manager encounters a device, such as a trunk, gateway, or route pattern, that has the Connected Line ID Presentation set to Default, the presentation value is automatically set to Allowed. For more information about this field, see topics related to connected party presentation and restriction settings in the *Cisco Unified Communications Manager System Guide*.

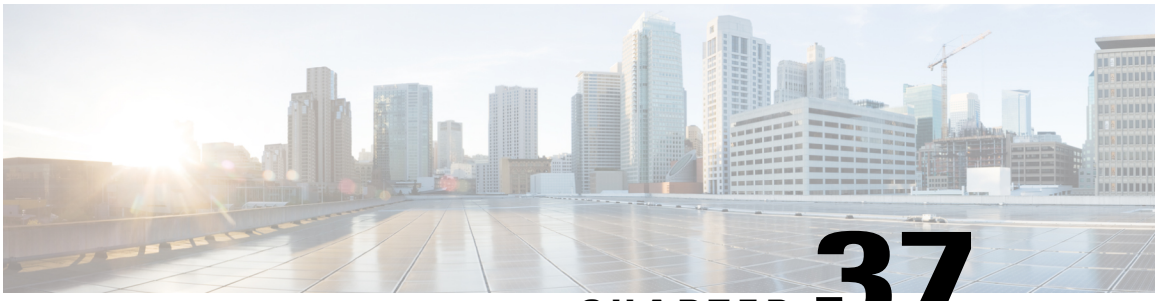
Field	Description
Connected Name Presentation	Cisco Unified Communications Manager uses connected name presentation (CONP/CONR) as a supplementary service to allow or restrict the called party name on a call-by-call basis. Choose whether you want Cisco Unified Communications Manager to allow or restrict the display of the connected party name on the calling party phone display for this route 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. For more information about this field, see topics related to connected party presentation and restriction settings in the *Cisco Unified Communications Manager System Guide*.
Called Party Transformations	
Discard Digits	From the Discard Digits drop-down list box, choose the discard digits instructions that you want to associate with this route pattern. The discard digits that display depend on the numbering plan that you choose from the Numbering Plan drop-down list box. See topics related to discard digits instructions in the *Cisco Unified Communications Manager System Guide* for more information on discard instructions for the North American Numbering Plan. **Note** The called party transformation settings that are assigned to the route groups in a route list override any called party transformation settings that are assigned to a route pattern that is associated with that route list.
Called Party Transform Mask	Enter a transformation mask value. Valid entries for the National Numbering Plan include the digits 0 through 9; the wildcard characters X, asterisk (*), and octothorpe (#); the international escape character +; and blank. If the field is blank, no transformation takes place. Cisco Unified Communications Manager sends the dialed digits exactly as dialed.
Prefix Digits (Outgoing Calls)	Enter prefix digits in the Prefix Digits (Outgoing Calls) field. Valid entries for the National Numbering Plan 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.

Field	Description
Called Party Number Type	Choose the format for the number type in called party directory numbers. Cisco Unified Communications Manager sets the called 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 called directory number to be encoded to a non-national type numbering plan. Choose one of the following options: • Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the directory number type. • Unknown—Use 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.
Called Party Numbering Plan	Choose the format for the numbering plan in called party directory numbers. Cisco Unified Communications Manager sets the called DN numbering plan. 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 PBXs by using routing as a non national type number. Choose one of the following options: • Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the Numbering Plan in the directory number. • ISDN—Use when you are dialing outside the dialing plan for your country. • National Standard—Use when you are dialing within the dialing plan for your country. • Private—Use when you are dialing within a private network. • Unknown—Use when the dialing plan is unknown.
ISDN Network-Specific Facilities Information Element	
Network Service Protocol	From the Network Service Protocol drop-down list box, choose the PRI protocol that matches the protocol of the terminating gateway.

Field	Description
Carrier Identification Code	Enter the appropriate carrier identification code (0, 3, or 4 digits) in the Carrier Identification Code field. Carrier identification codes allow customers to reach the services of interexchange carriers. The following list shows examples of commonly used carrier identification codes: • ATT—0288 • Sprint—0333 • WorldCom/MCI—0222 For a complete list of NANP carrier identification codes, visit the NANPA website.
Network Service	Choose the appropriate network service. The values vary depending on the network service protocol that you choose from the Network Service Protocol field.
Service Parameter Name	This field displays the service parameter name that is associated with the chosen network service. If no service parameter exists for the network service, the field displays <Not Exist>.
Service Parameter Value	Enter the appropriate service parameter value. Valid entries include the digits 0 through 9. If a service parameter does not exist for the network service, Cisco Unified Communications Manager Administration disables this field.

Related Topics

About Route Filter Setup , on page 189
Synchronize Route List Settings with Route Groups , on page 210
Route Pattern Setup , on page 211
Search for Partition , on page 270



CHAPTER 37

Line Group Setup

This chapter provides information to add or delete a line group or to add directory numbers to or to remove directory numbers from a line group.

For additional information, see topics related to understanding route plans in the *Cisco Unified Communications Manager System Guide*.

About Line Group Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Route/Hunt** > **Line Group** menu path to configure line groups.

A line group allows you to designate the order in which directory numbers are chosen. Cisco Unified Communications Manager distributes a call to idle or available members of a line group based on a call distribution algorithm and on the Ring No Answer Reversion (RNAR) Timeout setting.

Note Users cannot pick up calls to a DN that belongs to a line group by using the Directed Call Pickup feature.

Tip Although you can configure an empty line group with no members (directory numbers), Cisco Unified Communications Manager does not support this configuration for routing calls. If the line group contains no members, the hunt list stops hunting when the call gets routed to the empty line group. To avoid this situation, make sure that you configure at least one member in the line group.

Line Group Configuration Tips

You must define one or more directory numbers before configuring a line group.

After you configure or update a line group, you can add or remove members from that line group.

Related Topics

Add Members to Line Group , on page 229
Remove Members From Line Group , on page 229

Line Group Deletion

You cannot delete a line group that one or more route/hunt lists references. To find out which hunt lists are using the line group, in the Line Group Configuration window, choose Dependency Records from the Related Links drop-down list box and click Go. If the dependency records are not enabled for the system, the Dependency Records Summary window displays a message. If you try to delete a line group that is in use, Cisco Unified Communications Manager displays an error message. Before deleting a line group that is currently in use, you must perform the following task:

- Remove the line group from all hunt lists to which it belongs before deleting the line group.

Tip To delete line groups and hunt pilots; first, delete the hunt pilot; second, delete the hunt list; and finally, delete the line group.

Related Topics

Remove Route Groups From Route List , on page 209
Access Dependency Records , on page 982

Line Group Settings

The following table describes the line group settings.

Table 40: Line Group Settings

Field	Description
Line Group Information	

Field	Description
Line Group Name	Enter a name for this line group. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that each line group name is unique to the route plan. **Timesaver** Use concise and descriptive names for your line groups. The CompanynameLocationGroup format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a line group. For example, CiscoDallasAA1 identifies a Cisco Access Analog line group for the Cisco office in Dallas.
RNA Reversion Timeout	Enter a time, in seconds, after which Cisco Unified CM will distribute a call to the next available or idle member of this line group or to the next line group if the call is not answered and if the first hunt option, Try next member; then, try next group in Hunt List, is chosen. The RNA Reversion Timeout applies at the line-group level to all members.
Distribution Algorithm	Choose a distribution algorithm, which applies at the line-group level, from the options in the drop-down list box: • Top Down—If you choose this distribution algorithm, Cisco Unified CM distributes a call to idle or available members starting from the first idle or available member of a line group to the last idle or available member. • Circular—If you choose this distribution algorithm, Cisco Unified CM distributes a call to idle or available members starting from the (n+1)th member of a route group, where the nth member is the next sequential member in the list who is either idle or busy but not “down.” If the nth member is the last member of a route group, Cisco Unified CM distributes a call starting from the top of the route group. • Longest Idle Time—If you choose this distribution algorithm, Cisco Unified CM only distributes a call to idle members, starting from the longest idle member to the least idle member of a line group. • Broadcast—If you choose this distribution algorithm, Cisco Unified CM distributes a call to all idle or available members of a line group simultaneously. See the Note in the description of the Selected DN/Route Partition field for additional limitations in using the Broadcast distribution algorithm. The default value specifies Longest Idle Time.
Hunt Options	

Field	Description
No Answer	For a given distribution algorithm, choose a hunt option for Cisco Unified CM to use if a call is distributed to a member of a line group that does not answer. This option gets applied at the member level. Choose from the options in the drop-down list box: • Try next member; then, try next group in Hunt List—If you choose this hunt option, Cisco Unified CM distributes a call to idle or available members starting from the first idle or available member of a line group to the last idle or available member. If unsuccessful, Cisco Unified CM then tries the next line group in a hunt list. • Try next member, but do not go to next group—If you choose this hunt option, Cisco Unified CM distributes a call to idle or available members starting from the first idle or available member of a line group to the last idle or available member. Cisco Unified CM stops trying upon reaching the last member of the current line group. • Skip remaining members, and go directly to next group—If you choose this hunt option, Cisco Unified CM skips the remaining members of this line group when the RNA reversion timeout value elapses for the first member. Cisco Unified CM then proceeds directly to the next line group in a hunt list. • Stop hunting—If you choose this hunt option, Cisco Unified CM stops hunting after trying to distribute a call to the first member of this line group and the member does not answer the call.
Automatically Logout Hunt Member on No Answer	If this check box is checked, line members will be logged off the hunt list automatically. Line members can log back in using the "HLOG" softkey or PLK.

Field	Description
Busy	For a given distribution algorithm, choose a hunt option for Cisco Unified CM to use if a call is distributed to a member of a line group that is busy. Choose from the options in the drop-down list box: • Try next member; then, try next group in Hunt List—If you choose this hunt option, Cisco Unified CM distributes a call to idle or available members starting from the first idle or available member of a line group to the last idle or available member. If unsuccessful, Cisco Unified CM then tries the next line group in a hunt list. • Try next member, but do not go to next group—If you choose this hunt option, Cisco Unified CM distributes a call to idle or available members starting from the first idle or available member of a line group to the last idle or available member. Cisco Unified CM stops trying upon reaching the last member of the current line group. • Skip remaining members, and go directly to next group—If you choose this hunt option, Cisco Unified CM skips the remaining members of this line group upon encountering a busy member. Cisco Unified CM proceeds directly to the next line group in a hunt list. • Stop hunting—If you choose this hunt option, Cisco Unified CM stops hunting after trying to distribute a call to the first busy member of this line group.
Not Available	For a given distribution algorithm, choose a hunt option for Cisco Unified CM to use if a call is distributed to a member of a line group that is not available. The Not Available condition occurs when none of the phones that are associated with the DN in question is registered. Not Available also occurs when extension mobility is in use and the DN/user is not logged in. Choose from the options in the drop-down list box: • Try next member; then, try next group in Hunt List—If you choose this hunt option, Cisco Unified CM distributes a call to idle or available members starting from the first idle or available member of a line group to the last idle or available member. If unsuccessful, Cisco Unified Communications Manager then tries the next line group in a hunt list. • Try next member, but do not go to next group—If you choose this hunt option, Cisco Unified CM distributes a call to idle or available members starting from the first idle or available member of a line group to the last idle or available member. Cisco Unified CM stops trying upon reaching the last member of the current line group. • Skip remaining members, and go directly to next group—If you choose this hunt option, Cisco Unified CM skips the remaining members of this line group upon encountering the first unavailable member. Cisco Unified CM proceeds directly to the next line group in a hunt list. • Stop hunting—If you choose this hunt option, Cisco Unified CM stops hunting after trying to distribute a call to the first unavailable member of this line group.

Field	Description
Line Group Member Information	
Find Directory Numbers to Add to Line Group	
Partition	Choose a route partition for this line group from the drop-down list box. The default value specifies <None>. If you click Find, the Available DN/Route Partition list box displays all DNs that belong to the chosen partition.
Directory Number Contains	Enter the character(s) that are found in the directory number that you are seeking and click the Find button. Directory numbers that match the character(s) that you entered display in the Available DN/Route Partition box.
Available DN/Route Partition	Choose a directory number in the Available DN/Route Partition list box and add it to the Selected DN/Route Partition list box by clicking Add to Line Group.
Current Line Group Members	
Selected DN/Route Partition	To change the priority of a directory number, choose a directory number in the Selected DN/Route Partition list box. Move the directory number up or down in the list by clicking the arrows on the right side of the list box. To reverse the priority order of the directory numbers in the Selected DN/Route Partition list box, click Reverse Order of Selected DNs/Route Partitions. For more information about the order of directory numbers in a line group, see topics related to route plans in the *Cisco Unified Communications Manager System Guide*. **Note** Do not put DNs that are shared lines in a line group that uses the Broadcast distribution algorithm. Cisco Unified CM cannot display all DNs that are shared lines on devices where the DNs are configured as shared lines if the DNs are members of a line group that uses the Broadcast distribution algorithm.
Removed DN/Route Partition	Choose a directory number in the Selected DN/Route Partition list box and add it to the Removed DN/Route Partition list box by clicking the down arrow between the two list boxes.
Directory Numbers	
(list of DNs that currently belong to this line group)	Click a directory number in this list to go to the Directory Number Configuration window for the specified directory number. **Note** When you are adding a new line group, this list does not display until you save the line group.

Related Topics

Line Group Setup , on page 223

Add Members to Line Group

You can add members to a new line group or to an existing line group. The following procedure describes adding a member to an existing line group.

Before You Begin

You must define one or more directory numbers before performing this procedure.

Procedure

Step 1 Choose **Call Routing** > **Route/Hunt** > **Line Group**.

Step 2 Locate the line group to which you want to add a member.

Step 3 If you need to locate a directory number, choose a route partition from the Partition drop-down list box, enter a search string in the Directory Number Contains field, and click Find. To find all directory numbers that belong to a partition, leave the Directory Number Contains field blank and click Find.
A list of matching directory numbers displays in the Available DN/Route Partition list box.

Step 4 In the Available DN/Route Partition list box, choose a directory number to add and click Add to Line Group to move it to the Selected DN/Route Partition list box. Repeat this step for each member that you want to add to this line group.

Step 5 In the Selected DN/Route Partition list box, choose the order in which the new directory number(s) is to be accessed in this line group. To change the order, click a directory number and use the Up and Down arrows to the right of the list box to change the order of directory numbers.

Step 6 Click Save to add the new directory numbers and to update the directory number order for this line group.

Related Topics

Line Group Setup , on page 223

Remove Members From Line Group

You can remove members from a new line group or from an existing line group. The following procedure describes removing a directory number from an existing line group.

Procedure

Step 1 Choose **Call Routing** > **Route/Hunt** > **Line Group**.

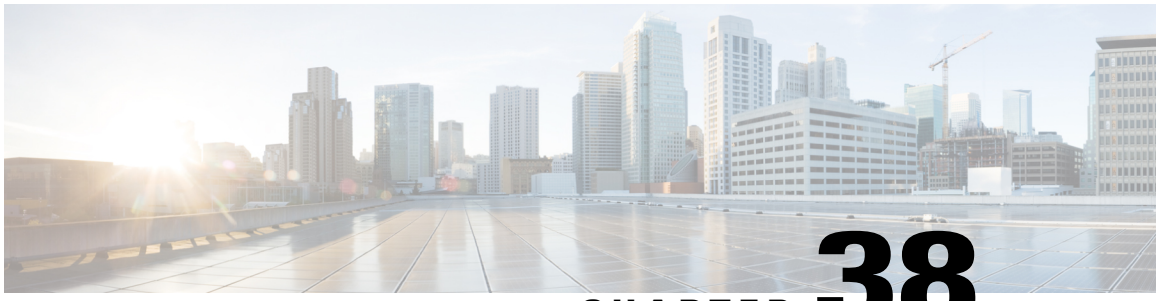
Step 2 Locate the line group from which you want to remove a directory number.

Step 3 In the Selected DN/Route Partition list box, choose a directory number to be deleted and click the down arrow below the list box to move the directory number to the Removed DN/Route Partition list box. Repeat this step for each member that you want to remove from this line group.

Step 4 To remove the members, click Save.

Related Topics

Line Group Setup , on page 223



CHAPTER 38

Hunt List Setup

The following chapter provides information to add or remove hunt lists or to add, remove, or change the order of line groups in a hunt list, or synchronize configuration changes with affected line groups.

For additional information, see topics related to understanding route plans in the *Cisco Unified Communications Manager System Guide*.

About Hunt List Configuration

A Hunt List lists a set of Line groups in a specific order. A hunt list then associates with one or more hunt pilots and determines the order in which those line groups are accessed. The order controls the progress of the search for available directory numbers for incoming calls.

A hunt list comprises a collection of directory numbers as defined by line groups. After Cisco Unified Communications Manager determines a call that is to be routed through a defined hunt list, Cisco Unified Communications Manager finds the first available device on the basis of the order of the line group(s) that a hunt list defines.

Note The Group Call Pickup feature and Directed Call Pickup feature do not work with hunt lists.

A hunt list can contain only line groups. Each hunt list should have at least one line group. Each line group includes at least one directory number. A single line group can appear in multiple hunt lists.

Find Hunt Lists

Because you might have several hunt lists in your network, Cisco Unified Communications Manager lets you use specific criteria to locate specific hunt lists. To locate hunt lists, use the following procedure.

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

Procedure

Step 1 Choose **Call Routing** > **Route/Hunt** > **Hunt List**.
The Find and List Hunt Lists 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; go to Find Hunt Lists , on page 232.
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 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

Hunt List Setup , on page 231

Add Hunt List

The following procedure describes how to add a hunt list.

Procedure

Step 1 Choose **Call Routing** > **Route/Hunt** > **Hunt List**.

Step 2 Click Add New.

Step 3 In the Name field, enter a name. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure each hunt list name is unique to the route plan.

Warning Use concise and descriptive names for your hunt lists. The CompanynameLocationCalltype format, which usually provides a sufficient level of detail and is short enough, enables you to quickly and easily identify a hunt list. For example, CiscoDallasMetro identifies a hunt list for toll-free, inter-local access transport area (LATA) calls from the Cisco office in Dallas.

Step 4 Enter a description in the Description field.

Step 5 Choose a Cisco Unified Communications Manager Group from the drop-down list box.

Note Hunt List registers to the first Cisco Unified Communications Manager in the Cisco Unified Communications Manager Group as primary Cisco Unified Communications Manager.

Note If you choose a Cisco Unified Communications Manager group that has only one Cisco Unified Communications Manager that is configured, you receive the following warning:

The selected Cisco Unified Communications Manager Group has only one Cisco Unified Communications Manager configured. For the control process to have redundancy protection, please select a Cisco Unified Communications Manager Group with more than one Cisco Unified Communications Manager.

Step 6 If this hunt list is to be used for voice mail, click the For Voice Mail Usage check box.
If you check the For Voice Mail Usage check box, the route list control process keeps a count of the setups that are being served to the hunt list, and will not allow more setups than the number of available devices. As a result, each device in the hunt list is treated as if it has a Busy Trigger and related Maximum Number of Calls of one.

For example, if the hunt list contains five devices, and if busy trigger is two for each member, with the For Voice Mail Usage checkbox unchecked, it can process up to ten setups. For the same number of hunt list devices with a busy trigger of two for each member, with the For Voice Mail Usage checkbox checked, it can process only five setups and the next immediate setup after five gets rejected.

Step 7 To add this hunt list, click Save.

Note A popup message reminds you that you must add at least one line group to this hunt list for it to accept calls.

The Hunt List window displays the newly added hunt list.

Step 8 The system checks the Enable this Hunt List check box by default for the new hunt list.
If you want to disable this hunt list, uncheck this check box. A popup window explains that calls in progress are not affected, but this hunt list will not accept additional calls.

Step 9 Add at least one line group to the new hunt list.
To add a line group to this list, click Add Line Group and perform Step 3, on page 234 through Step 6, on page 234 of the Add Line Groups to Hunt List , on page 234.

Related Topics

Hunt List Setup , on page 231

Add Line Groups to Hunt List

You can add line groups to a new hunt list or to an existing hunt list. Line groups can exist in one or more hunt lists. The following procedure describes adding a line group to an existing hunt list.

Before You Begin

You must build one or more line groups and add a hunt list before performing this procedure.

Procedure

Step 1 Choose **Call Routing** > **Route/Hunt** > **Hunt List**.

Step 2 Locate the hunt list to which you want to add a line group.

Step 3 To add a line group, click Add Line Group.
The Hunt List Detail Configuration window displays.

Step 4 From the Line Group drop-down list box, choose a line group to add to the hunt list.

Step 5 To add the line group, click Save.
The line group name displays in the Selected Groups pane.

Note The added line group also displays in the Hunt List Details pane at the bottom of the Hunt List Configuration window. You can make changes to a line group by clicking on the line group name. Doing so causes the Line Group Configuration window for that line group to display.

Step 6 To add more line groups to this list, click Add Line Group and repeat Step 3, on page 234 through Step 5, on page 234.

Step 7 When you finish adding line groups to the hunt list, click Save.

Note See topics related to synchronizing a hunt list with affected line groups before deciding whether to proceed to Step 8, on page 234 below.

Step 8 To reset the hunt list, click Reset. When the popup windows display, click Reset.

Related Topics

Hunt List Setup , on page 231
Find Hunt Lists , on page 232
Synchronize Hunt List Settings with Line Groups , on page 236

Remove Line Groups From Hunt List

You can remove line groups from a new hunt list or from an existing hunt list. The following procedure describes removing a line group from an existing hunt list.

Procedure

Step 1 Choose **Call Routing** > **Route/Hunt** > **Hunt List** in the menu bar.

Step 2 Locate the hunt list from which you want to remove a line group.

Step 3 From the Selected Groups list, choose a line group name.

Note To choose multiple line groups from the list, press the Shift key and click the desired line groups.

Step 4 Click the down arrow below the Selected Groups list box to move the chosen line group to the Removed Groups list.

Step 5 To remove the line group, click Save. If you click OK, when the window refreshes, the line group no longer displays in the Selected Groups pane of the hunt list.

Step 6 Click Reset for the changes to take effect. Click Reset and Close in response to the popup window.

Related Topics

Hunt List Setup , on page 231
Find Hunt Lists , on page 232

Change Line Groups Order in Hunt List

Cisco Unified Communications Manager accesses line groups in the order in which they display in the hunt list. The following procedure allows you to change the access order of line groups.

Procedure

Step 1 Choose **Call Routing** > **Route/Hunt** > **Hunt List**.

Step 2 Locate the hunt list in which you want to change the order of a line group.

Step 3 From the Selected Groups list, choose a line group.

Step 4 To move the line group up or down in the list, select a group; then, click the up or down arrows on the right side of the list box.

Step 5 Click Save.

Step 6 Click Reset for the changes to take effect. Click Reset and Close in response to the popup window.

Related Topics

Hunt List Setup , on page 231
Find Hunt Lists , on page 232

Synchronize Hunt List Settings with Line Groups

To synchronize line groups with a hunt list that has undergone configuration changes, perform the following procedure, which applies 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** > **Route/Hunt** > **Hunt List**.
The Find and List Hunt Lists window displays.

Step 2 Choose the search criteria to use.

Step 3 Click Find.
The window displays a list of hunt lists that match the search criteria.

Step 4 Check the check boxes next to the hunt lists to which you want to synchronize applicable line groups. To choose all hunt lists 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.

Related Topics

Hunt List Setup , on page 231

Delete Hunt List

Cisco Unified Communications Manager associates hunt lists with line groups and hunt pilots; however, deletion of line groups and hunt pilots does not occur when the hunt list is deleted. To find out which hunt pilots are using the hunt list, click the Dependency Records link from the Hunt List Configuration window. If dependency records are not enabled for the system, the dependency records summary window displays a message.

Tip To delete line groups and hunt pilots, first delete the hunt pilot; second, delete the hunt list; and finally, delete the line group.

The following procedure describes how to delete a hunt list.

Procedure

Step 1 Choose **Call Routing** > **Route/Hunt** > **Hunt List**.

Step 2 Locate the hunt list that you want to delete.

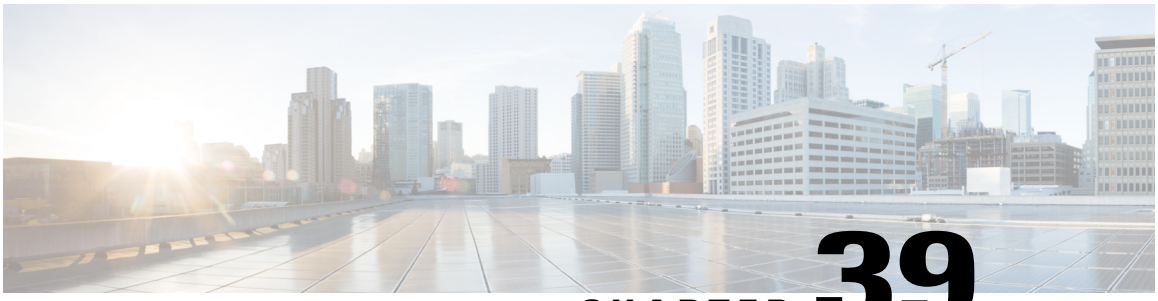
Step 3 Click Delete.
A dialog box displays to warn you that you cannot undo the deletion of a hunt list.

Step 4 To delete the hunt list, click OK or to cancel the action, click Cancel.

Caution You cannot delete a hunt list if it is associated with one or more hunt pilots.

Related Topics

Hunt List Setup , on page 231
Find Hunt Lists , on page 232
Access Dependency Records , on page 982



CHAPTER 39

Hunt Pilot Setup

This chapter provides information to add, configure, or delete a hunt pilot.

For additional information about understanding route plans, wildcards and special characters in route patterns and hunt pilots, see the *Cisco Unified Communications Manager System Guide*.

About Hunt Pilot Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Route/Hunt** > **Hunt Pilot** menu path to configure hunt pilots.

A hunt pilot comprises a string of digits (an address) and a set of associated digit manipulations that route calls to a hunt list. Hunt pilots provide flexibility in network design. They work in conjunction with route filters and hunt lists to direct calls to specific devices and to include, exclude, or modify specific digit patterns.

See topics related to understanding route plans in the *Cisco Unified Communications Manager System Guide* for more detailed hunt pilot information.

Call Queuing

The Call Queuing feature provides an enhanced capability for handling incoming calls to a hunt pilot number. For detailed information on the Call Queuing feature, see “Call Queuing”, in Cisco Unified Communications Manager Features and Services Guide.

Hunt Pilot Configuration Tips

Before you begin, ensure that the following items are configured in Cisco Unified Communications Manager:

- Hunt list
- Partition (unless you are using <None>)
- Route filter (unless you are using <None>)

Timesaver Assigning 8XXX to a hunt pilot causes hunting through all directory numbers 8000 to 8999. Similarly, 82XX hunts through directory numbers 8200 to 8299. See topics related to special characters and settings in the *Cisco Unified Communications Manager System Guide* for more information about wildcards.

Note After you choose a hunt list from the Hunt List drop-down list box, you can use the (Edit) link that displays next to the Hunt List field to take you to the Hunt List Configuration window for the hunt list that you choose. Use the Hunt List Configuration window to see the line group(s) that are included in that hunt list.

Hunt Pilot Settings

The following table describes the available fields in the Hunt Pilot Configuration window.

Table 41: Hunt Pilot Settings

Field	Description
Pattern Definition	
Hunt Pilot	Enter the hunt pilot, including numbers and wildcards (do not use spaces); for example, for 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 +. **Note** Ensure that the directory hunt pilot, which uses the chosen partition, route filter, and numbering plan combination, is unique. Check the hunt pilot, translation pattern, directory number, call park number, call pickup number, message waiting on/off, or meet me number if you receive an error that indicates duplicate entries. You can also check the route plan report. • See topics related to wildcards and special characters in route patterns and hunt pilots in the *Cisco Unified Communications Manager System Guide* for more information about wildcards.

Field	Description
Route Partition	If you want to use a partition to restrict access to the hunt pilot, choose the desired partition from the drop-down list box. If you do not want to restrict access to the hunt pilot, 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, then find and choose a partition name. **Note** To set the maximum list box items, choose **System** > **Enterprise Parameters** and choose Unified CMAdmin Parameters. **Note** Make sure that the combination of hunt pilot, route filter, and partition is unique within the Cisco Unified CM cluster.
Description	Enter a description of the hunt pilot. 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.
Route Filter	If your hunt pilot includes the @ wildcard, you may choose a route filter. The optional act of choosing a 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. You can configure the number of items that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more route filters 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 Route Filters window, then find and choose a route filter name. **Note** To set the maximum list box items, choose **System** > **Enterprise Parameters** and choose Unified CMAdmin Parameters.
MLPP Precedence	Choose an MLPP precedence setting for this hunt pilot 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. **Note** See topics related to multilevel precedence and preemption in the *Cisco Unified Communications Manager Features and Services Guide* for more information.

Field	Description
Hunt List	Choose the hunt list for which you are adding a hunt pilot from the drop-down list box. After you choose a hunt list, click the Edit link to the right to edit the hunt list.
Call Pickup Group	Choose the number that can be dialed to answer calls to this directory number (in the specified partition). **Note** The Call Pickup Group setting has been moved to this section from the Forward settings section.
Alerting Name	Enter an alerting name for the hunt pilot in UNICODE format. This name gets displayed on phones that the hunt pilot dials when it receives an incoming call, along with calling party information. The phone users can use this information to answer the call accordingly. This name also gets displayed on the calling phone. If you do not enter a name, the hunt pilot DN displays on the phones.
ASCII Alerting Name	Enter an alerting name for the hunt pilot in ASCII format. This name gets displayed on phones that the hunt pilot dials when it receives an incoming call, along with calling party information. The phone users can use this information to answer the call accordingly. This name also gets displayed on the calling phone. If you do not enter a name, the hunt pilot DN displays on the phones.
Route Option	The Route Option designation indicates whether you want this hunt pilot 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 hunt pilot 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	Provide Outside Dial Tone indicates that Cisco Unified CM routes the calls off the local network. Check this check box for each hunt pilot that routes the call off the local network and provides outside dial tone to the calling device. To route the call in the network, leave the check box unchecked.

Field	Description
Urgent Priority	If the dial plan contains overlapping hunt lists, Cisco Unified CM would 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 CM must route a call immediately.
Hunt Call Treatment Settings	
Forward Hunt No Answer	When the call that is distributed through the hunt list is not answered in a specific period of time, this field specifies the destination to which the call gets forwarded. Choose from the following options: • Do Not Forward Unanswered Calls • Use Forward Settings of Line Group Member (replaces "Use Personal Preferences" check box) • Forward Unanswered Calls to: ◦ Destination—This setting indicates the directory number to which calls are forwarded. ◦ Calling Search Space—This setting applies to all devices that are using this directory number. • Maximum Hunt Timer—Enter a value (in seconds) that specifies the maximum time for hunting without queuing. Valid values specify 1 to 3600. The default value specifies 1800 seconds (30 minutes). This timer cancels if either a hunt member answers the call or if the hunt list gets exhausted before the timer expires. If you do not specify a value for this timer, hunting continues until a hunt member answers or hunting exhausts. If neither event takes place, hunting continues for 30 minutes, after which the call gets taken for final treatment. **Note** If hunting exceeds the number of hops that the Forward Maximum Hop Count service parameter specifies, hunting expires before the 30-minute maximum hunt timer value, and the caller receives a reorder tone. In addition, Cisco Unified CM only uses the configuration for the Maximum Hunt Timer setting if you configure the Hunt Forward settings in the Hunt Pilot Configuration window.

Field	Description
Forward Hunt Busy	When the call that is distributed through the hunt list is busy in a specific period of time, this field specifies the destination to which the call gets forwarded. Choose from the following options: • Do Not Forward Busy Calls • Use Forward Settings of Line Group Member • Forward Busy Calls to: ◦ Destination—This setting indicates the directory number to which calls are forwarded. ◦ Calling Search Space—This setting applies to all devices that are using this directory number.
Queuing **Note** Forward Hunt No Answer or Forward Hunt Busy settings are designed to move calls through the route list. Queuing, on the other hand, is used to hold callers in a route list. Therefore, if queuing is enabled, both Forward Hunt No Answer and Forward Hunt Busy are automatically disabled. Conversely, if Forward Hunt No Answer or Forward Hunt Busy are enabled, queuing is automatically disabled.	
Queue Calls	Check the Queue Calls check box to enable queuing. When a hunt pilot has more calls distributed through the call distribution feature than its hunt members can handle at any given time, call queuing holds these calls in a queue until they can be answered. Once Queue Calls has been selected, choose from the following options:
Network Hold/MoH Source and Announcements	Choose a Music On Hold (MoH) source from the drop-down list box, which will be used to play announcements and provide queue hold treatments. The default value is NULL. If nothing is selected, the default Network Hold MoH/MoH Source and Announcements configured on service parameter is used. The MoH source can be configured as unicast or multicast. Caller side's MRGL takes precedence for multicast or unicast. The MoH source announcement locale is used to determine the language used for the announcement. Only one type of language announcement can be played per hunt pilot. When any of the MoH settings are changed, the existing callers in queue are not affected. All future queued callers will listen to MoH and announcements as per the updated settings.

Field	Description
Maximum Number of Callers Allowed in Queue	Enter an integer value for the number of callers allowed in the queue for this hunt pilot. The default value is 32. The field range is from 1 to 100. When the maximum number of callers in queue has been reached, and if subsequent calls need to be disconnected, select the “Disconnect the call” radio button. When the maximum number of callers in queue has been reached, and if subsequent calls need to be routed to a secondary destination, select the “Route the call to this destination” radio button. Provide a specific device DN, shared line DN, or another Hunt Pilot DN. You may also select the “Full Queue Calling Search Space” from the drop-down list (optional).
Maximum Wait Time in Queue	Enter an integer value to set the maximum wait time, in seconds, in a queue. The default value is 900 seconds. The field range is from 10 to 3600 seconds. When the maximum wait time in queue has been reached, and if the queued caller needs to be disconnected, select the “Disconnect the call” radio button. When the maximum wait time in queue has been reached, and if the queued caller needs to be routed to a secondary destination, select the “Route the call to this destination” radio button. Provide a specific device DN, shared line DN, or another Hunt Pilot DN. You may also select the “Maximum Wait Time Calling Search Space” from the drop-down list (optional).
When no hunt members are logged in or registered	When no line members are logged in or registered at the time of an incoming call, and if that call needs to be disconnected, select the “Disconnect the call” radio button. When no line members are logged in or registered at the time of an incoming call, and if that call needs to be routed to a secondary destination, select the “Route the call to this destination” radio button. Provide a specific device DN, shared line DN, or another Hunt Pilot DN. You may also select the “No hunt members logged in or registered Calling Search Space” from the drop-down list (optional).
Park Monitoring	

Field	Description
Park Monitoring Forward No Retrieve Destination	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) to forward the parked call when the service parameter Park Monitoring Forward No Retrieve Timer expires. If the parameter value of the Hunt Pilot Park Monitoring Forward No Retrieve Destination parameter 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. Specify the following values: • Destination—This setting specifies the directory number to which a parked call is forwarded when the service parameter Park Monitoring Forward No Retrieve Timer expires. Use any dialable phone number, including an outside destination. • Calling Search Space—A calling search space comprises an ordered list of route partitions that are typically assigned to devices. Calling search spaces determine the partitions that calling devices search when they are attempting to complete a call.
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. You may also configure an External Phone Number Mask on all phone devices. **Note** The calling party transformation settings that are assigned to the line groups in a hunt list override any calling party transformation settings that are assigned to a hunt pilot that is associated with that hunt list.
Calling Party Transform Mask	Enter a transformation mask value. Valid entries include the digits 0 through 9, the wildcard character X, 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. See topics related to calling party number transformations settings in the *Cisco Unified Communications Manager Features and Services Guide* for more information.
Prefix Digits (Outgoing Calls)	Enter prefix digits in the Prefix Digits (Outgoing Calls) field. 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.

Field	Description
Calling Line ID Presentation	Cisco Unified CM 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 CM to allow or restrict the display of the calling party phone number on the called party phone display for this hunt pilot. Choose Default if you do not want to change calling line ID presentation. Choose Allowed if you want Cisco Unified CM to allow the display of the calling number. Choose Restricted if you want Cisco Unified CM to block the display of the calling number. For more information about this field, see topics related to calling party number transformations settings in the *Cisco Unified Communications Manager Features and Services Guide* .
Display Line Group Member DN as Connected Party	Check this check box to display the directory number of the answering phone as the connected party when a call is routed through a hunt list. Uncheck this check box to display the hunt pilot number as the connected party when a call is routed through a hunt list.
Calling Name Presentation	Cisco Unified CM 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 CM to allow or restrict the display of the calling party name on the called party phone display for this hunt pilot. Choose Default if you do not want to change calling name presentation. Choose Allowed if you want Cisco Unified CM to display the calling name information. Choose Restricted if you want Cisco Unified CM to block the display of the calling name information. For more information about this field, see topics related to calling party number transformations settings in the *Cisco Unified Communications Manager Features and Services Guide* .

Field	Description
Calling Party Number Type	Choose the format for the number type in calling party directory numbers. Cisco Unified CM 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 CM 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 Unified Communications Manager—The Cisco Unified Communications Manager sets the directory number type. • Unknown—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.
Calling Party Numbering Plan	Choose the format for the numbering plan in calling party directory numbers. Cisco Unified CM sets the calling DN numbering plan. 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 CM does not recognize European national dialing patterns. You can also change this setting when you are connecting to PBXs by using routing as a non-national type number. Choose one of the following options: • Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the Numbering Plan in the directory number. • ISDN—Use when you are dialing outside the dialing plan for your country. • National Standard—Use when you are dialing within the dialing plan for your country. • Private—Use when you are dialing within a private network. • Unknown—Use when the dialing plan is unknown.
Connected Party Transformations	

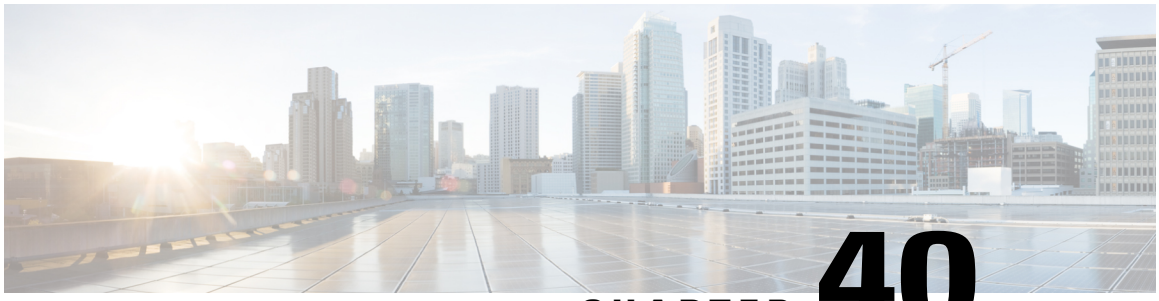
Field	Description
Connected Line ID Presentation	Cisco Unified Communications Manager uses connected line ID presentation (COLP/COLR) as a supplementary service to allow or restrict the called party phone number on a call-by-call basis. Choose whether you want Cisco Unified CM to allow or restrict the display of the connected party phone number on the calling party phone display for this hunt pilot. 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 CM to block the display of the connected party phone number. If a call that originates from an IP phone on Cisco Unified Communications Manager encounters a device, such as a trunk, gateway, or route pattern, that has the Connected Line ID Presentation set to Default, the presentation value is automatically set to Allowed. For more information about this field, see topics related to connected party presentation and restriction settings in the *Cisco Unified Communications Manager Features and Services Guide* .
Display Line Group Member DN as Connected Party	Check this check box to display the directory number of the answering phone as the connected party when a call is routed through a hunt list. Uncheck this check box to display the hunt pilot number as the connected party when a call is routed through a hunt list.
Connected Name Presentation	Cisco Unified CM 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 CM to allow or restrict the display of the connected party name on the calling party phone display for this hunt pilot. 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 CM to block the display of the connected party name. For more information about this field, see topics related to connected party presentation and restriction settings in the *Cisco Unified Communications Manager Features and Services Guide* .
Called Party Transformations	
Discard Digits	From the Discard Digits drop-down list box, choose the discard digits instructions that you want to associate with this hunt pilot. The discard digits that display depend on the numbering plan that you choose from the Numbering Plan drop-down list box. See topics related to discard digits instructions in the *Cisco Unified Communications Manager System Guide* for more information on discard instructions for the North American Numbering Plan. **Note** The called party transformation settings that are assigned to the line groups in a hunt list override any called party transformation settings that are assigned to a hunt pilot that is associated with that hunt list.

Field	Description
Called Party Transform Mask	Enter a transformation mask value. Valid entries include the digits 0 through 9; the wildcard characters X, asterisk (*), and octothorpe (#); the international escape character +; and blank. If the field is blank, no transformation takes place. Cisco Unified CM sends the dialed digits exactly as dialed.
Prefix Digits (Outgoing Calls)	Enter prefix digits in the Prefix Digits (Outgoing Calls) field. 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.
Called Party Number Type	Choose the format for the number type in called party directory numbers. Cisco Unified Communications Manager sets the called 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 CM does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the called directory number to be encoded to a non-national type numbering plan. Choose one of the following options: • Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the directory number type. • Unknown—Use 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.

Field	Description
Called Party Numbering Plan	Choose the format for the numbering plan in called party directory numbers. Cisco Unified CM sets the called DN numbering plan. 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 CM does not recognize European national dialing patterns. You can also change this setting when you are connecting to PBXs by using routing as a non-national type number. Choose one of the following options: • Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the Numbering Plan in the directory number. • ISDN—Use when you are dialing outside the dialing plan for your country. • National Standard—Use when you are dialing within the dialing plan for your country. • Private—Use when you are dialing within a private network. • Unknown—Use when the dialing plan is unknown.
AAR Group Settings	
AAR Group	Choose an Automated Alternate Routing (AAR) group from the drop-down list box.
External Number Mask	Enter an external number mask value for the hunt pilot. Cisco Unified CM uses this mask to format calling line identification for external (outbound) calls. When AAR initiates a reroute, the system applies this external number mask to the hunt pilot number to form a fully qualified DN of the called party, which allows AAR to reroute properly in out-of-bandwidth conditions.

Related Topics

About Route Filter Setup , on page 189
Hunt Pilot Setup , on page 239
Partition Setup , on page 267
Search for Partition , on page 270



CHAPTER 40

SIP Route Pattern Setup

This chapter provides information about SIP Route Pattern configuration.

About SIP Route Pattern Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **SIP Route Pattern** menu path to configure SIP route patterns.

Cisco Unified Communications Manager uses SIP route patterns to route or block both internal and external calls.

The domain name or IP address provides the basis for routing. The administrator can add domains, IP addresses, and IP network (subnet) addresses and associate them to SIP trunks (only). This method allows requests that are destined for these domains to be routed through particular SIP trunk interfaces.

Note Because no default SIP route patterns exist in Cisco Unified Communications Manager, the administrator must set them up.

Note Domain name examples: cisco.com, my-pc.cisco.com, *.com, rtp-ccm[1-5].cisco.com

Note Valid characters for domain names: [, -, ., 0-9, A-Z, a-z, *, and].

Note IPv4 address examples: 172.18.201.119 or 172.18.201.119/32 (explicit IP host address); 172.18.0.0/16 (IP subnet); 172.18.201.18/21 (IP subnet).

Note Valid characters for IP addresses: 0-9, ., and /

SIP Route Patterns Configuration Tips

Before you begin, ensure at least one SIP Profile and SIP trunk are configured before you can configure a SIP route pattern.

Related Topics

Set Up Trunk , on page 695

SIP Route Pattern Deletion

If the SIP route pattern is not in use, Cisco Unified Communications Manager deletes it. If it is in use, a message displays.

SIP Route Pattern Settings

The following table describes the SIP route pattern settings.

Table 42: SIP Route Pattern Settings

Field	Description
Pattern Definition	
Pattern Usage	(Required) From the drop-down list, choose either Domain Routing or IP Address Routing.
IPv4 Pattern	(Required) Enter the domain, sub-domain, IPv4 address, or IP subnetwork address. For Domain Routing pattern usage, enter a domain name IPv4 Pattern field that can resolve to an IPv4 address. The domain name can contain the following characters: [, -, ., 0-9, A-Z, a-z, *, and]. For IP Address Routing pattern usage, enter an IPv4 address the IPv4 Pattern field that follows the format X.X.X.X, where X represents a number between 0 and 255. For the IP subnetwork address, in Classless Inter-Domain Routing (CIDR) notation, X.X.X.X/Y; where Y is 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.

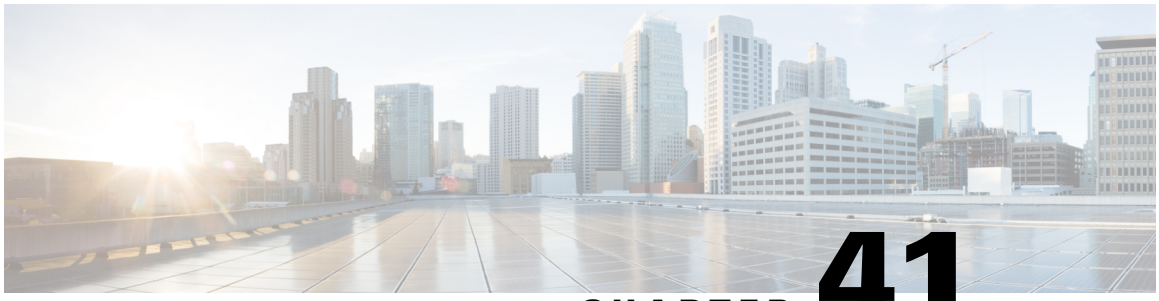
Field	Description
IPv6 Pattern	Cisco Unified Communications Manager uses SIP route patterns to route or block both internal and external calls. The IPv6 address in this field provides the basis for routing internal and external calls to SIP trunks that support IPv6. **Tip** If the SIP trunk supports IPv6 or both IPv4 and IPv6 (dual-stack mode), configure the IPv4 Pattern in addition to the IPv6 Pattern.
Description	For this optional entry, enter a description of the SIP Route Pattern. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), or angle brackets (<>).
Route Partition	If you want to use a partition to restrict access to the SIP route pattern, choose the desired partition from the drop-down list box. If you do not want to restrict access to the SIP route pattern, 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 than 250 partitions are specified by using the Max List Box Items enterprise parameter, the Find button displays next to the drop-down list box. Click the Find button to display the Select Partition window. Enter a partial partition name in the List items where Name contains field. Click the desired partition name in the list of 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. Make sure that the combination of SIP route pattern, route filter, and partition is unique within the Cisco Unified Communications Manager cluster.
SIP Trunk/Route List	(Required) From the drop-down list choose the SIP trunk or route list to which the SIP route pattern should be associated. Click Edit to open the trunk or route list in the Trunk or Route List Configuration window. **Note** URI dialing is available over SIP trunks only. If you are using URI dialing and you select a route list from this drop-down list box, the route list must contain route groups with SIP trunks only.
Block Pattern	If you do not want this pattern to be used for routing calls, click the Block Pattern check box.
Calling Party Transformations	
Use Calling Party's External Phone Mask	Check the check box if you want the full, external phone number to be used for calling line identification (CLID) on outgoing calls. You may also configure an External Phone Number Mask on all phone devices.

Field	Description
Calling Party Transformation Mask	Enter a transformation mask value. Valid entries include the digits 0 through 9 and the wildcard characters X, asterisk (*), and octothorpe (#). If this field is blank and the preceding field is not checked, no calling party transformation takes place. See topics related to calling party number transformations settings in the *Cisco Unified Communications Manager System Guide* for more information.
Prefix Digits (Outgoing Calls	Enter prefix digits in the Prefix Digits (Outgoing Calls) field. Valid entries include the digits 0 through 9 and the wildcard characters asterisk (*) and octothorpe (#). **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 SIP route 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. For more information about this field, see topics related to calling party number transformations settings in the *Cisco Unified Communications Manager System Guide*.
Calling Line 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 SIP route 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. For more information about this field, see topics related to calling party number transformations settings in the *Cisco Unified Communications Manager System Guide*.
Connected Party Transformations	

Field	Description
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 SIP route 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. If a call that originates from an IP phone on Cisco Unified Communications Manager encounters a device, such as a trunk, gateway, or route pattern, that has the Connected Line ID Presentation set to Default, the presentation value is automatically set to Allowed. For more information about this field, see topics related to connected party presentation and restriction settings in the *Cisco Unified Communications Manager System Guide*.
Connected Line 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 SIP route 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. For more information about this field, see topics related to connected party presentation and restriction settings in the *Cisco Unified Communications Manager System Guide*.

Related Topics

SIP Route Pattern Setup , on page 253
Partition Setup , on page 267



CHAPTER 41

Time Period Setup

This chapter provides information to add, update, copy, or delete a time period.

For additional information, see topics related to time-of-day routing in the *Cisco Unified Communications Manager System Guide*.

About Time Period Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Class of Control** > **Time Period** menu path to configure time periods.

A time period comprises a time range that is defined by a start time and end time. Time periods also specify a repetition interval either as days of the week or a specified date on the yearly calendar. You define time periods and then associate the time periods with time schedules. A particular time period can be associated with multiple time schedules.

You then associate time schedules with partitions to set up time-of-day call routing. For more detailed information on time periods and time schedules, see topics related to time-of-day routing in the *Cisco Unified Communications Manager System Guide*.

Time Period Deletions

You cannot delete time periods that time schedules are using. To find out which time schedules or other items are using the time period, choose Dependency Records from the Related Links drop-down list box that is on the Time Period Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. If you try to delete a time period that is in use, Cisco Unified Communications Manager displays an error message. Before deleting a time period that is currently in use, you must perform either or both of the following tasks:

- Assign a different time period to any time schedules that are using the time period that you want to delete.

- Delete the time schedules that are using the time period that you want to delete.

Related Topics

About Time Schedule Setup , on page 263
Time Schedule Deletions, on page 263
Access Dependency Records , on page 982

Time Period Settings

The following table describes the time period settings.

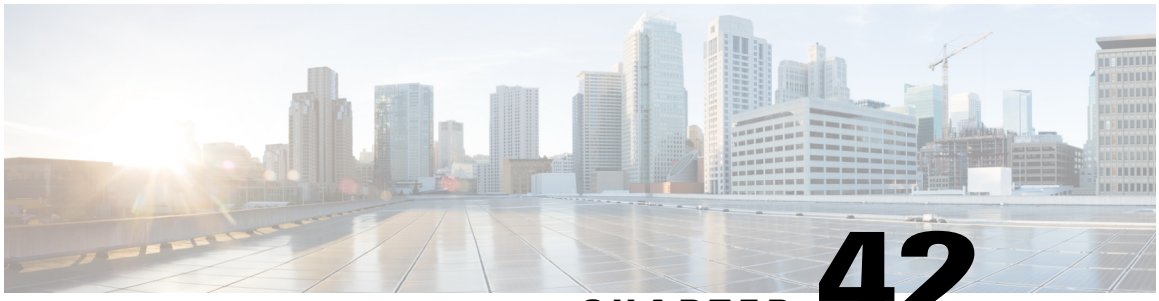
Table 43: Time Period Settings

Field	Description
Time Period Information	
Name	Enter a name in the Time Period 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 time period name is unique to the plan. **Note** Use concise and descriptive names for your time periods. The hours_or_days format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a time period. For example, office_M_to_F identifies a time period for the business hours of an office from Monday to Friday. Cisco Unified Communications Manager provides the All the time time period. This special, system time period includes all hours, is published to end users, and cannot be deleted; this time period can be copied.
Description	Enter a description for this time period.
Time Of Day Start	From the drop-down list box, choose the time when this time period starts. The available listed start times comprise 15-minute intervals throughout a 24-hour day. The default value is No Office Hours. **Note** To start a time period at midnight, choose the 00:00 value.
Time of Day End	From the drop-down list box, choose the time when this time period ends. The available listed end times comprise 15-minute intervals throughout a 24-hour day. The default value is No Office Hours. **Note** You must choose an End Time that is later than the Start Time that you chose. **Note** To end a time period at midnight, choose the 24:00 value.

Field	Description
Repeat Every	Click on one of the radio buttons: • Week from—If you click on the Week from radio button, use the drop-down list boxes next to from and through to choose the days of the week during which this time period applies.Examples: Choose a from value of Mon(day) and a through value of Fri(day) to define a time period that applies from Monday through Friday. Choose a from value of Sat(urday) and a through value of Sat(urday) to define a time period that applies only on Saturdays. • Year on—If you click on the Year on radio button, use the drop-down list boxes next to Year on and until to choose the month-and-day combinations of the year during which this time period applies.Example: Choose a Year on value of Jan and 15 and an until value of Mar and 15 to choose the days from January 15 to March 15 during which this time period applies.Choose a Year on value of Jan and 1 and an until value of Jan and 1 to specify January 1st as the only day during which this time period applies.
Clear Repeat	Click this button to clear the previously chosen Repeat Every values from the time period that you are modifying.

Related Topics

Time Period Setup , on page 259



CHAPTER 42

Time Schedule Setup

This chapter provides information to find, add, update, copy, or delete a time schedule:

For additional information, see topics related to time-of-day routing in the *Cisco Unified Communications Manager System Guide*.

About Time Schedule Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Class of Control** > **Time Schedule** menu path to configure time schedules.

A time schedule comprises a group of time periods. Time schedules get assigned to partitions. Time schedules determine the partitions where calling devices search when they are attempting to complete a call during a particular time of day. Multiple time schedules can use a single time period.

For more detailed information on time schedules, see topics related to time-of-day routing in the *Cisco Unified Communications Manager System Guide*.

Time Schedule Deletions

You cannot delete time schedules that partitions are using. To find out which items are using the time schedule, choose Dependency Records from the Related Links drop-down list box that is on the Time Schedule Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. If you try to delete a time schedule that is in use, Cisco Unified Communications Manager displays an error message. Before deleting a time schedule that is currently in use, you must perform either or both of the following tasks:

- Assign a different time schedule to any partitions that are using the time schedule that you want to delete.
- Delete the partitions that are using the time schedule that you want to delete.

Caution Before you delete a time schedule, check carefully to ensure that you are deleting the correct time schedule. You cannot retrieve deleted time schedules. If you accidentally delete a time schedule, you must rebuild it.

Related Topics

About Partition Setup , on page 267
Access Dependency Records , on page 982

Time Schedule Settings

The following table describes the time schedule settings.

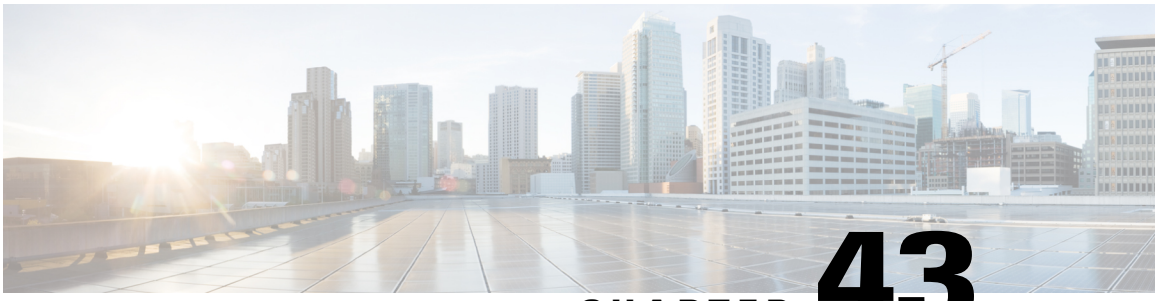
Table 44: Time Schedule Settings

Field	Description
Time Schedule Information	
Name	Enter a name in the 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 time schedule name is unique to the plan. **Note** Use concise and descriptive names for your time schedules. Cisco Unified Communications Manager provides the All the time time schedule. This special, system time schedule includes all days and all hours, is published to end users, and cannot be deleted; this time schedule can be copied.
Description	Enter a description for this time schedule.
Time Period Information	
Available Time Periods	This field displays after a time schedule has been added. Choose a time period in the Available Time Periods list box and add it to the Selected Time Periods list box by clicking the down arrow button between the two list boxes. To add a range of time periods at once, click the first time period in the range; then, hold down the Shift key while clicking the last time period in the range. Click the down arrow button between the two list boxes to add the range of time periods. To add multiple time periods that are not contiguous, hold down the Control (Ctrl) key while clicking multiple time periods. Click the down arrow button between the two list boxes to add the chosen time periods.

Field	Description
Selected Time Periods	This list box lists the time periods that were selected for this time schedule. To remove a time period from the list of selected time periods, choose the time period to remove and click the up arrow between the two list boxes. To reorder the selected time periods, choose a time period and click the up and down arrows to the right of this list box. **Note** If multiple time periods get associated to a time schedule and the time periods overlap, time periods with Day of Year settings take precedence over time periods with Day of Week settings. Day of Year is applicable when **Year on** value is set and the **until** value is left blank. Example: If a Time Period configured for January 1st is configured as No Office Hours and another time period is configured for the same day of the week (for example, Sunday to Saturday) as 08:00 to 17:00, the time period for January 1st gets used. In this example, No Office Hours takes precedence. **Note** Time interval settings take precedence over No Office Hour settings for the same day of the year or day of the week. Example: One time period specifies for Saturday as No Office Hours. Another time period specifies Saturday hours of 08:00 to 12:00. In this example, the resulting time interval specifies 08:00 to 12:00 for Saturday. **Note** If multiple time periods are associated to a time schedule and the time periods overlap, time periods with Day of Week settings take precedence over time periods with Range of Days settings. Range of Days applies to when **Year on** and **until** values are set, even if they are configured for the same day. Example: If a Time Period configured for Day of Week (for example, Sunday to Saturday) is configured as No Office Hours and another time period is configured for January 1st until December 31th as 08:00 to 17:00, the time period for Day of Week is used. In this example, No Office Hours takes precedence.

Related Topics

Time Schedule Setup , on page 263



CHAPTER 43

Partition Setup

This chapter provides information to find, add, update, or delete route partitions.

For additional information, see topics related to local route groups in the *Cisco Unified Communications Manager Features and Services Guide*.

About Partition Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Class of Control** > **Partition** menu path to configure partitions.

A 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 and calling search spaces, see the *Cisco Unified Communications Manager System Guide*.

Partitions Configuration Tips

You can configure multiple partitions. To enter multiple partitions, use one line for each partition entry. You can enter up to 75 partitions at a time; the names and descriptions can have a total of up to 1475 characters. Use a comma (,) to separate the partition name and description on each line. If you do not enter a description, Cisco Unified Communications Manager uses the name as the description.

Timesaver Use concise and descriptive names for your partitions. The CompanynameLocationCalltype format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a partition. For example, CiscoDallasMetroPT identifies a partition for toll-free, inter-local access and transport area (LATA) calls from the Cisco office in Dallas.

If you are updating a partition, click Reset, or use the Apply Config button as described in the procedure to synchronize a partition with affected devices. When you reset devices that are associated with the partition, all calls on affected gateways drop.

Related Topics

Search for Partition , on page 270
Synchronize Partition Settings with Devices , on page 270

Partition Deletions

You cannot delete a 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 partition, choose Dependency Records from the Related Links drop-down list box in the Partition Configuration window and click Go. If the dependency records are not enabled for the system, the dependency records summary window displays a message. 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 partition to any calling search spaces, devices, or other items that are using the partition that you want to delete.
- Delete the calling search spaces, devices, or other items that are using the partition that you want to delete.

Caution Before initiating a deletion, check carefully to ensure that you are deleting the correct partition. You cannot retrieve deleted partitions. If you accidentally delete a partition, you must rebuild it.

Related Topics

Access Dependency Records , on page 982

Partition Settings

The following table describes the partition settings.

Table 45: Partition Settings

Field	Description
Partition Information	

Field	Description
(Partition Name, Description)	Enter a name in the partition name and description box. Ensure each partition name is unique to the route plan. 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 partition names limits the maximum number of partitions that can be added to a calling search space. The calling search space partition limitations table provides examples of the maximum number of partitions that can be added to a calling search space if partition names are of fixed length. Follow the 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 ("), percentage sign (%), ampersand (&), back-slash (\), angle brackets (<>), or brackets ([ ]). If you do not enter a description, Cisco Unified Communications Manager automatically enters the partition name in this field. Use a new line for each partition and description.
Time Schedule	From the drop-down list box, choose a time schedule to associate with this partition. The associated time schedule specifies when the partition is available to receive incoming calls. 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 incoming calls to this partition against the specified time schedule.
Time Zone	Choose one of the following options to associate a 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. These options all specify the Time Zone. When an incoming call 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.

The following table provides examples of the maximum number of partitions that can be added to a calling search space if partition names are of fixed length. See topics related to partition name limitations in the *Cisco Unified Communications Manager System Guide* for details about how this maximum number is calculated.

Table 46: Calling Search Space Partition Limitations

Partition Name Length	Maximum Number of Partitions
2 characters	170

Partition Name Length	Maximum Number of Partitions
3 characters	128
4 characters	102
5 characters	86
. . .	. . .
10 characters	46
15 characters	32

Related Topics

Partition Setup , on page 267

Search for 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 Partition drop-down list box on the Cisco Unified Communications Manager Administration windows where the button appears. Click the Find button to search for the partition that you want.

Procedure

Step 1 Click the Find button next to the Partition drop-down list box.
The Find and List Partitions window displays.

Step 2 In the Find partition where field, choose search criteria and enter a partial partition name.

Step 3 In the list of partitions that displays, click the desired partition name and click OK.

Related Topics

Partition Setup , on page 267

Synchronize Partition Settings with Devices

To synchronize devices with a partition that has undergone configuration changes, perform the following procedure, which applies 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** > **Class of Control** > **Partition**.
The Find and List Partitions window displays.

Step 2 Choose the search criteria to use.

Step 3 Click Find.
The window displays a list of partitions that match the search criteria.

Step 4 Click the partition to which you want to synchronize applicable devices. The Partition Configuration window displays.

Step 5 Make any additional configuration changes.

Step 6 Click Save.

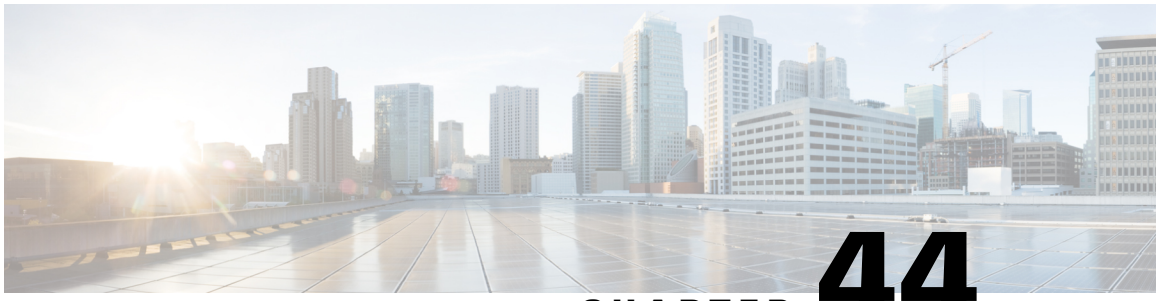
Step 7 Click Apply Config.
The Apply Configuration Information dialog displays.

Note If devices that are associated with the partition get reset, all calls on affected gateways drop.

Step 8 Click OK.

Related Topics

Partition Setup , on page 267



CHAPTER 44

Calling Search Space Setup

This chapter provides information to find, add, update, copy, or delete a calling search space.

For additional information, see topics related to local route groups in the *Cisco Unified Communications Manager Features and Services Guide*.

About Calling Search Space Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Class of Control** > **Calling Search Space** menu path to configure calling search spaces (CSS).

A calling search space comprises an ordered list of route partitions that are typically assigned to devices. 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*.

Calling Search Space Deletions

You cannot delete 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 calling search space, choose the Dependency Records from the Related Links drop-down list box in the 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. If you try to delete a calling search space that is in use, Cisco Unified Communications Manager displays a message. Before deleting a calling search space that is currently in use, you must perform either or both of the following tasks:

- Assign a different calling search space to any devices, lines, or translation patterns that are using the calling search space that you want to delete.
- Delete the devices, lines, or translation patterns that are using the calling search space that you want to delete.

Caution Before initiating this deletion, check carefully to ensure that you are deleting the correct calling search space. You cannot retrieve deleted calling search spaces. If you accidentally delete a calling search space, you must rebuild it.

Related Topics

About Translation Pattern Setup , on page 277
Translation Pattern Deletions, on page 278
Directory Number Setup , on page 289
Remove Directory Number From Phone , on page 322
Access Dependency Records , on page 982

Calling Search Space Settings

The following table describes the calling search space settings.

Table 47: Calling Search Space Settings

Field	Description
Calling Search Space Information	
Name	Enter a name in the 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 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, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
Route Partitions for this Calling Search Space	

Field	Description
Available Partitions	Choose a partition in the Available Partitions list box and add it to the Selected Partitions list box by clicking the arrow button between the two list boxes. To add a range of partitions at once, click the first partition in the range; then, hold down the Shift key while clicking the last partition in the range. Click the arrow button between the two list boxes to add the range of partitions. To add multiple partitions that are not contiguous, hold down the Control (Ctrl) key while clicking multiple partitions. Click the arrow button between the two list boxes to add the chosen partitions. **Note** The length of the partition names limits the maximum number of partitions that can be added to a calling search space. The calling search space partition limitations table provides examples of the maximum number of partitions that can be added to a calling search space if partition names are of fixed length.
Selected Partitions	To change the priority of a partition, choose a partition name in the Selected Partitions list box. Move the partition up or down in the list by clicking the arrows on the right side of the list box.

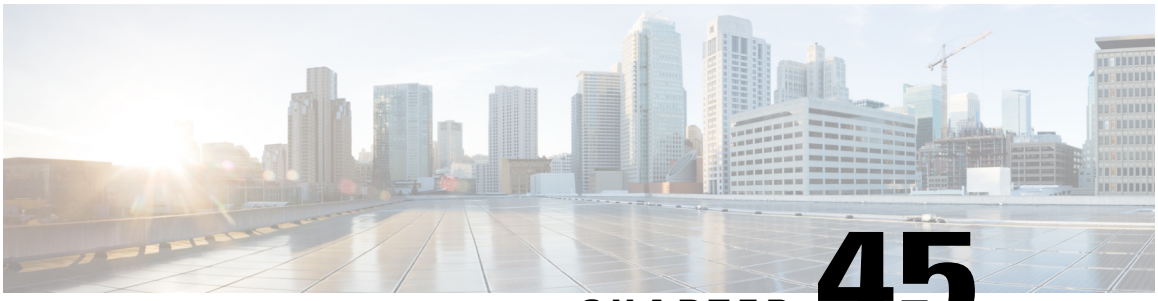
The following table provides examples of the maximum number of partitions that can be added to a calling search space if partition names are of fixed length. See topics related to partition name limitations in the *Cisco Unified Communications Manager System Guide* for details about how this maximum number is calculated.

Table 48: 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

Related Topics

Calling Search Space Setup , on page 273



CHAPTER 45

Translation Pattern Setup

This chapter provides information to add, update, copy, or delete a translation pattern.

For additional information, see topics related to understanding route plans in the *Cisco Unified Communications Manager System Guide*.

About Translation Pattern Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Translation Pattern** menu path to configure translation patterns.

Cisco Unified Communications Manager uses translation patterns to manipulate dialed digits before it routes a call. In some cases, the system does not use the dialed number. In other cases, the public switched telephone network (PSTN) does not recognize the dialed number.

Translation Patterns Configuration Tips

Configure the following Cisco Unified Communications Manager items before configuring a translation pattern:

- Partition
- Route filter
- Calling search space
- Resource-Priority Namespace Network Domain

Note Ensure that the 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.

Translation Pattern Deletions

Check carefully to ensure that you are deleting the correct translation pattern before you initiate this action. You cannot retrieve deleted translation patterns. If you accidentally delete a translation pattern, you must rebuild it.

Translation Pattern Settings

The following table describes the available fields in the Translation Pattern Configuration window.

Table 49: Translation Pattern Settings

Field	Description
Pattern Definition	
Translation Pattern	Enter the translation pattern, including numbers and wildcards (do not use spaces), in the 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 translation pattern, which uses the chosen partition, route filter, and numbering plan combination, is unique. Check the route pattern/hunt pilot, translation pattern, directory number, call park number, call pickup number, or meet-me number if you receive a message that indicates duplicate entries. Alternatively, check the route plan report if you receive a message that indicates duplicate entries.

Field	Description
Partition	Choose a partition. If you do not want to assign a partition, choose <None>. If you choose <None>, you must enter a value in the Translation Pattern field. 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, then find and choose a partition name. **Note** To set the maximum list box items, choose **System** > **Enterprise Parameters** and choose CCMAdmin Parameters. Make sure that the combination of translation pattern, route filter, and partition is unique within the Cisco Unified Communications Manager cluster.
Description	Enter a description for the translation pattern. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), or angle brackets (<>).
Numbering Plan	Choose a numbering plan. If your 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. See topics related to wildcards and special characters in route patterns and hunt pilots in the *Cisco Unified Communications Manager System Guide*, as well as topics related to route filter configuration settings for more information. 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.

Field	Description
MLPP Precedence	Choose an MLPP precedence setting for this 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. **Note** See topics related to multilevel precedence and preemption in the *Cisco Unified Communications Manager Features and Services Guide* for more information.
Resource-Priority Namespace Network Domain	Choose an already configured Resource-Priority Namespace Network Domain from the drop-down list box.
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.

Field	Description
Calling Search Space	From the drop-down list box, choose the calling search space for which you are adding a translation pattern, if necessary. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more 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 a calling search space name. **Note** To set the maximum list box items, choose **System** > **Enterprise Parameters** and choose CCMAdmin Parameters.
Use Originator's Calling Search Space	To use the originator's calling search space for routing a call, check the Use Originator's Calling Search Space check box. When you check this check box, it disables the Calling Search Space drop-down list box. When you save the page, the Calling Search Space box is grayed out and set to <None>. If the originating device is a phone, the originator's calling search space is a resultant of device calling search space (configured on the Phone Configuration window) and line calling search space (configured on the Directory Number Configuration window). Whenever a translation pattern chain is encountered, for subsequent lookups Calling Search Space is selected depending upon the value of this check box at current translation pattern. If you check the Use Originator's Calling Search Space check box at current translation pattern, then originator's Calling Search Space is used and not the Calling Search Space for the previous lookup. If you uncheck the Use Originator's Calling Search Space check box at current translation pattern, then Calling Search Space configured at current translation pattern is used
External Call Control Profile	In Cisco Unified Communications Manager, you enable external call control by assigning an external call control profile to a translation pattern. If the translation pattern has an external call control profile assigned to it, when a call occurs that 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. For more information on external call control, see topics related to external call control in the *Cisco Unified Communications Manager Features and Services Guide*. From the drop-down list box, choose the external call profile that you want to assign to the translation pattern.

Field	Description
Route Option	The Route Option designation indicates whether you want this 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 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 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. **Tip** 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.
Do Not Wait For Interdigit Timeout On Subsequent Hops	When you check this check box along with the Urgent Priority check box and the translation pattern matches with a sequence of dialed digits (or whenever the translation pattern is the only matching pattern), Cisco Unified Communications Manager does not start the interdigit timer after it matches any of the subsequent patterns. **Note**: Cisco Unified Communications Manager does not start the interdigit timer even if subsequent patterns are of variable length or if overlapping patterns exist for subsequent matches. Whenever you check the Do Not Wait For Interdigit Timeout On Subsequent Hops check box that is associated with a translation pattern in a translation pattern chain, Cisco Unified Communications Manager does not start the interdigit timer after it matches any of the subsequent patterns. **Note**: Cisco Unified Communications Manager does not start interdigit timer even if subsequent translation patterns in a chain have Do Not Wait For Interdigit Timeout On Subsequent Hops unchecked.
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.

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 for the National Numbering Plan include the digits 0 through 9, and 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 for the National Numbering Plan include the digits 0 through 9, and the wildcard characters asterisk (*) and octothorpe (#); 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 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. For more information about this field, see topics related to calling party number transformations settings in the *Cisco Unified Communications Manager System Guide* . **Note** Use this parameter and the Connected Line ID Presentation parameter, in combination with the Ignore Presentation Indicators (internal calls only) device-level parameter, to configure call display restrictions. Together, these settings allow you to selectively present or restrict calling and/or connected line display information for each call. See topics related to device profile configuration settings and phone settings for information about the Ignore Presentation Indicators (internal calls only) field. For more information about call display restrictions, see topics related to call display restrictions in the *Cisco Unified Communications Manager System Guide*.

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 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. For more information about this field, see calling party number transformations settings in the *Cisco Unified Communications Manager System Guide*.
Calling Party Number Type	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 Unified Communications Manager—The Cisco Unified Communications Manager sets the directory number type. • Unknown—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.

Field	Description
Calling Party Numbering Plan	Choose the format for the numbering plan in calling party directory numbers. Cisco Unified Communications Manager sets the calling DN numbering plan. 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 PBXs by using routing as a non-national type number. Choose one of the following options: • Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the Numbering Plan in the directory number. • ISDN—Use when you are dialing outside the dialing plan for your country. • National Standard—Use when you are dialing within the dialing plan for your country. • Private—Use when you are dialing within a private network. • Unknown—Use when the dialing plan is unknown.
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 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. If a call that originates from an IP phone on Cisco Unified Communications Manager encounters a device, such as a trunk, gateway, or route pattern, that has the Connected Line ID Presentation set to Default, the presentation value is automatically set to Allowed. For more information about this field, see topics related to connected party presentation and restriction settings in the *Cisco Unified Communications Manager System Guide* .

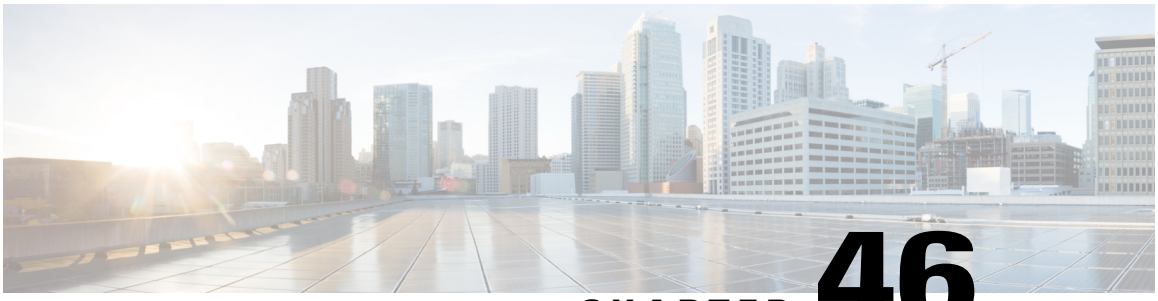
Field	Description
Connected Name Presentation	Cisco Unified Communications Manager uses connected name presentation (CONP/CONR) as a supplementary service to allow or restrict the called party name on a call-by-call basis. Choose whether you want Cisco Unified Communications Manager to allow or restrict the display of the connected party name on the calling party phone display for this 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. For more information about this field, see topics related to connected party presentation and restriction settings in the *Cisco Unified Communications Manager System Guide* .
Called Party Transformations	
Discard Digits	Choose the discard digits instructions that you want to be associated with this translation pattern. See see topics related to discard digits instructions in the *Cisco Unified Communications Manager System Guide* for more information. **Note** The discard digits that display depend on the numbering plan that you choose from the Numbering Plan drop-down list box.
Called Party Transform Mask	Enter a transformation mask value. Valid entries for the National Numbering Plan include the digits 0 through 9, and 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 for the National Numbering Plan include the digits 0 through 9, and 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.

Field	Description
Called Party Number Type	Choose the format for the number type in called party directory numbers. Cisco Unified Communications Manager sets the called 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 called directory number to be encoded to a non-national type numbering plan. Choose one of the following options: • Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the directory number type. • Unknown—Use 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.
Called Party Numbering Plan	Choose the format for the numbering plan in called party directory numbers. Cisco Unified Communications Manager sets the called DN numbering plan. 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 PBXs by using routing as a non-national type number. Choose one of the following options: • Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the Numbering Plan in the directory number. • ISDN—Use when you are dialing outside the dialing plan for your country. • National Standard—Use when you are dialing within the dialing plan for your country. • Private—Use when you are dialing within a private network. • Unknown—Use when the dialing plan is unknown.

Related Topics

About Route List Setup , on page 205

Search for Partition , on page 270
About Calling Search Space Setup , on page 273
Translation Pattern Setup , on page 277
Set Up Speed-dial Buttons or Abbreviated Dialing , on page 625
About Device Profile Setup , on page 713
Phone Settings, on page 583



CHAPTER 46

Directory Number Setup

This chapter provides information about working with and configuring directory numbers (DNs) in Cisco Unified Communications Manager Administration.

For additional information, see topics related to directory numbers, Cisco Unified IP Phones, and phone features in the *Cisco Unified Communications Manager Administration System Guide*; as well as topics related to Cisco Unity connection configuration.

Additional information can also be found in *User Moves, Adds, and Changes Guide for Cisco Unity Connection* and topics related to presence in the *Cisco Unified Communications Manager Administration Features and Services Guide*.

About Directory Number Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Directory Number** menu path to configure directory numbers (DNs).

Using Cisco Unified Communications Manager Administration, you configure and modify directory numbers (DNs) that are assigned to specific phones. Use the Directory Number Configuration window to perform the following tasks:

- Add or remove directory numbers.
- Assign directory URIs to a directory number
- Configure call forward, call pickup, call waiting, and multilevel precedence and preemption (MLPP) options.
- Set the display text that appears on the called party phone when a call is placed from a line.

- Configure ring settings.
- Configure Cisco Unity Connection voice mailboxes.

Shared lines always have identical DN settings, except for the field sections in the Directory Number Configuration window that contain the naming convention "on Device SEPXXXXXXXXXXX," which are maintained/mapped to a specific device. If you add a shared line to a device, the shared DN configuration settings, such as Calling Search Space and Call Forward and Pickup, will display. If these DN configuration settings get changed, the new settings apply to all the shared lines.

Assign Directory URIs to a Directory Number

Use the Directory Number Configuration window to associate directory URIs to a directory number. This allows Cisco Unified Communications Manager to support dialing using either the directory number or the directory URI. Each directory URI address must resolve to a single directory number in a partition.

Directory Number Configuration Tips

You can configure the directory number configuration settings by choosing **Call Routing** > **Directory Number**; you can configure these settings after you add a phone under **Call Routing** > **Phone**; or, you can configure these settings after you add a CTI route point under **Device** > **CTI Route Point**.

If you configure the directory number via **Device** > **Phone** or **Device** > **CTI Route Point**, be aware that only the configuration settings that apply to your phone model or CTI route point display. If you configure the directory number via **Call Routing** > **Directory Number**, all of the directory number settings do not display at the same time; for example, after you configure the directory number and click Save, more configuration settings may display.

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.

You can also add a directory number to a CTI route point by configuring the CTI route point under **Device** > **CTI Route Point**.

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 directory numbers; for example, 352XX. To avoid user confusion when you assign a pattern to a directory number, add text or digits to the DN configuration fields, Line Text Label, Display (Internal Caller ID), and External Phone Number Mask. (These fields display for a directory number only after you add the directory number and you associate the directory number with a phone.)

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.

Tip If you need more than two lines, you can increase the lines by modifying the phone button template for the phone type (such as Cisco IP Phone 7960). Some phone types, however, only support one or two lines (such as Cisco IP Phone 7902).

Note Restart devices as soon as possible. During this process, the system may drop calls on gateways.

Related Topics

Synchronize Directory Number Settings with Devices , on page 320
Set Up Private Line Automatic Ringdown (PLAR) , on page 321
Remove Directory Number From Phone , on page 322
Create Cisco Unity Connection Voice Mailbox , on page 323
Phone Setup , on page 581

Directory Number Settings

The following table describes the fields that are available in the Directory Number Configuration window.

Table 50: Directory Number Settings

Field	Description
Directory Number Information	
Directory Number	Enter a dialable phone number. Values can include route pattern wildcards and numeric characters (0 through 9). Special characters such as a question mark (?), exclamation mark (!), backslash (\), brackets ([ ]), plus sign (+), dash (-), asterisk (*), caret (^), pound sign (#), and an X are also allowable. Special characters that are not allowed are a period (.), at sign (@), dollar sign ($), and percent sign (%). At the beginning of the pattern, enter \+ if you want to use the international escape character +. For this field, \+ does not represent a wildcard; instead, entering \+ represents a dialable digit. **Note** When a pattern is used as a directory number, the display on the phone and the caller ID that displays on the dialed phone will both contain characters other than digits. To avoid this, Cisco recommends that you provide a value for Display (Internal Caller ID), Line text label, and External phone number mask. The directory number that you enter can appear in more than one partition. If you configure this field under **Call Routing** > **Directory Number**, you can enter insert directory numbers in bulk by entering a range (that is, by entering the beginning directory number in the first field and by entering the ending directory number in the second field); by using this method, you can create up to 500 directory numbers at a time.

Field	Description
Urgent Priority	If the dial plan contains overlapping patterns, Cisco Unified Communications Manager does not route the call to the device associated with the directory number until the interdigit timer expires (even if the directory number is a better match for the sequence of digits dialed as compared to the overlapping pattern). Check this check box to interrupt interdigit timing when Cisco Unified Communications Manager must route a call immediately to the device associated with the directory number. By default, the Urgent Priority check box is unchecked.
Route Partition	Choose the partition to which the directory number belongs. Make sure that the directory number that you enter in the Directory Number field is unique within the partition that you choose. If you do not want to restrict access to the directory number, 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, then find and choose a partition name. **Note** To set the maximum list box items, choose **System** > **Enterprise Parameters** and choose CCMAdmin Parameters.
Description	Enter a description of the directory number and 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 when the called phone is ringing. This setting, which supports the Identification Services for the QSIG protocol, applies to shared and nonshared directory numbers. When the phone rings at the terminating PINX, if you configured an alerting name for a directory number with shared-line appearances, the system performs the following tasks: • Forwards the alerting name of the called party, if configured, to the caller. • Applies the Connected Name Restrictions (CONR) that are configured for the translation pattern (if restrictions exist) Depending on the state of the call and your configuration, the alerting name, directory number, or display (internal caller ID) configuration may display on the phone, as described in the following bullets. • Alerting state—The alerting name displays, as configured in the Directory Number window. • Connected state—If you configure the Display (Internal Caller ID) and the Alerting Name fields, the display (internal caller ID) name displays. • Connected State—If you configured the Alerting Name field but not the Display (Internal Caller ID) field, the directory number displays. If you set the Always Display Original Dialed Number service parameter to True, the original dialed number and the alerting name displays during the call. You can choose if the alerting name for the original dialed number or the translated dialed number is displayed using the Cisco CallManager service parameter called Name Display for Original Dialed Number When Translated. The default setting displays the alerting name of the original dialed number before translation. **Note** Do not use the word “Voicemail” anywhere in your Alerting Name or ASCII Alerting Name. Use of the word “Voicemail” can cause Cisco Unity Connection to process the call as a direct call rather than as a forwarded call.
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. **Note** Do not use the word “Voicemail” anywhere in your Alerting Name or ASCII Alerting Name. Use of the word “Voicemail” can cause Cisco Unity Connection to process the call as a direct call rather than as a forwarded call.
Active	To view this check box on the Directory Number Configuration window, access an unassigned directory number from the Route Plan Report window. Checking this check box allows calls to this DN to be forwarded (if forwarding is configured). If check box is not checked, Cisco Unified Communications Manager ignores the DN.

Field	Description
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 directory number is associated If the directory number specifies a shared line, ensure the check box is enabled as long as at least one associated device specifies a combination of device type and protocol that CTI supports.
Line Group	From this drop-down list box, choose a line group with which to associate this DN. To edit or view the line group information for a line group, choose a line group from the drop-down list box and click the Edit Line Group button. **Note** If you configure a DN as part of a line group, you will not be able to associate that DN with a CTI port nor a CTI route point. Conversely, when you configure a CTI port or CTI route point, you will not be able to specify a DN that already belongs to a line group or to a hunt list. Furthermore, if a DN is a member of a line group or hunt list, any device (CTI port, CTI route point, phone that is running SCCP, or phone that is running SIP) that uses that DN should not be associated with a CTI user.
Associated Devices	After you associate this DN with a device(s), this pane displays the devices with which this DN is associated. To edit a device with which this DN 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 DN, 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 DN 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 a DN from a device, this pane displays the device(s) from which you dissociate this DN. 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.
Directory Number Settings	
Voice Mail Profile	Choose from list of Voice Mail Profiles that the Voice Mail Profile Configuration defines. The first option specifies <None>, which represents the current default Voice Mail Profile that is configured in the Voice Mail Profile Configuration.

Field	Description
Calling Search Space	From the drop-down list box, choose the appropriate calling search space. A calling search space comprises a collection of partitions that are searched for numbers that are called from this directory number. The value that you choose applies to all devices that are using this 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. 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. For more information, see topics related to partitions and calling search spaces in the *Cisco Unified Communications Manager System Guide*.
BLF Presence Group	Configure this field with the BLF Presence feature. From the drop-down list box, choose a BLF Presence group for this directory number. The selected group specifies the devices, end users, and application users that can monitor this directory number. The default value for BLF Presence Group specifies Standard Presence group, configured with installation. Presence groups that are configured in Cisco Unified Communications Manager Administration also appear in the drop-down list box. BLF Presence authorization works with presence groups to allow or block presence requests between groups. See topics related to BLF Presence in the *Cisco Unified Communications Manager System Guide* for information about configuring permissions between groups.
User Hold MOH Audio Source	Choose the audio source that plays when a user initiates a hold action.

Field	Description
Network Hold MOH Audio Source	Choose the audio source that plays when the network initiates a hold action.
Auto Answer	Choose one of the following options to activate the Auto Answer feature for this directory number: • Auto Answer Off <Default> • 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.
Reject anonymous calls	Check this check box to reject all anonymous calls for the DN. Anonymous calls are calls with no caller ID or that have caller ID blocked.
Enterprise Alternate Number / +E.164 Alternate Number **Note** The following fields apply to both Enterprise Alternate Numbers and +E.164 Alternate Numbers as the fields are identical for each section.	
Add Alternate Number	Click **Add Enterprise Alternate Number** to add an enterprise alternate number and associate it to this directory number. Click **Add +E.164 Alternate Number** to add an +E.164 alternate number and associate it to this directory number.

Field	Description
Number Mask	In the text box, enter a number mask for the enterprise alternate number or +E.164 alternate number. This field can contain only digits 0-9, X and the plus sign (+). If the Number Mask contains a plus sign, the plus sign must be the first character in the mask. Refer to the Alternate Number field to see how the alternate number appears after the mask is applied. Cisco Unified Communications Manager applies the mask to the directory number and creates an enterprise alternate number or +E.164 alternate number that acts as an alias for the directory number. Other phones can dial this directory number by dialing the enterprise number. **Enterprise Alternate Number Example** If you apply a number mask of 8XXXX to directory number 2000, Cisco Unified Communications Manager creates an enterprise alternate number 82000 as an alias of directory number 2000. If the dialed digits of an incoming call are 82000, Cisco Unified Communications Manager routes the call to the user that is registered to directory number 2000. **+E.164 Alternate Number Example** If you apply a number mask of 1972515XXXX to directory number 2000, Cisco Unified Communications Manager creates an +E.164 alternate number 19725152000 as an alias of directory number 2000. If the dialed digits of an incoming call are 19725152000, Cisco Unified Communications Manager routes the call to the user that is registered to directory number 2000.
Alternate Number	This field displays the enterprise alternate number or +E.164 alternate number after the Number Mask field has been applied. Users are able to dial the phone that is registered to this directory number by dialing this alternate number.
Add to Local Partition	Check this check box to assign this alternate number to a local route partition. Leave the check box unchecked if you do not want to restrict access to this alternate number. **Note** For users in the local cluster to be able to dial this alternate number, the partition to which you assign the alternate number must be in a local calling search space.
Route Partition	From the drop-down list box, choose the local route partition on which you want to assign the alternate number. Make sure that this alternate number is unique on this partition.
Advertise Globally via ILS	Check this check box to enable ILS to advertise this alternate number to remote clusters in the ILS network. If you leave this check box unchecked, Cisco Unified Communications Manager does not replicate this alternate number to remote clusters in the ILS network even if the Global Dial Plan Replication feature is enabled. **Note** In order for Cisco Unified Communications Manager to replicate this alternate number to remote clusters, you must also set up an ILS network and enable the Global Dial Plan Replication feature across the network.

Field	Description
Remove Alternate Number	Click **Remove Enterprise Alternate Number** to delete the enterprise alternate number. After you remove the alternate number, click **Save**. Click **Remove +E.164 Alternate Number** to delete the +E.164 alternate number. After you remove the alternate number, click **Save**.
Directory URIs	
Directory URIs	The fields in this section can be completed to associate directory URIs to a directory number so that users can make calls and identify callers using directory URIs rather than directory numbers. Users can associate up to five separate directory URIs to a single directory number, but they must select a primary URI. To associate a directory URI to the directory number, enter the directory URI in the URI text box, select the partition on which the URI is saved, and click **Save**. The Directory URIs section contains the following fields and buttons: • Primary—Check this radio button to select the primary directory URI for instances where more than one directory URI is associated to a directory number. • URI—Enter the directory URI address in this text box. For detailed information on valid directory URI formats, see Directory URI format. • Partition—From the drop-down menu, choose the partition to which the directory URI belongs. Make sure that the directory URI that you enter is unique within the partition that you choose. If you do not want to restrict access to the URI, choose **<None>** for the partition. • Advertise Globally via ILS—Check this check box to enable ILS to replicate this directory URI to remote clusters in the ILS network. If this check box is left unchecked, ILS will not replicate this directory URI to remote clusters, even if the Global Dial Plan Replication feature is enabled. By default, this check box is checked. **Note** Cisco Unified Communications Manager pauses the recording of learned ILS patterns until replication of cluster is successfully established. • Remove—Click the **(–)** button to delete this directory URI from the directory number configuration. After the directory URI has been deleted, click **Save**. • Add Row—When you want to associate multiple directory URIs to the directory number, click this button to add new rows on which you can enter the additional directory URIs. For detailed information on valid formats for directory URIs, see the "Directory URI Format" topic in the Intercluster Directory URI chapter of the *Cisco Unified Communications Manager Administration Guide.*.
PSTN Failover for Enterprise Alternate Number, +E.164 Alternate Number, and URI Dialing	

Field	Description
Advertised Failover Number	If the local cluster is part of an ILS network, and Global Dial Plan Replication is enabled, the local cluster advertises the PSTN failover to remote clusters in the ILS network. If a remote cluster is unable to route a call via a SIP trunk to one of the advertised directory URIs or alternate numbers that are associated with this directory number (DN), the remote cluster can reroute the call to the advertised PSTN failover number and send the call to a PSTN gateway. From the drop-down list box, choose one of the following options: • <None>—ILS does not advertise a PSTN failover option. • Enterprise Number (<number>)—ILS advertises the enterprise alternate number as the PSTN failover for all the alternate numbers and directory URIs that are associated to this DN. • +E.164 Number (<number>)—ILS advertises the +E.164 alternate number as the PSTN failover for all the alternate numbers and directory URIs that are associated to this DN. **Note** If Global Dial Plan Replication is enabled, ILS advertises the PSTN failover setting to the ILS network, regardless of whether the Advertise Globally via ILS check box is checked for the alternate number that you choose.
AAR Settings	
AAR (Voice Mail, AAR Destination Mask, AAR Group)	The settings in this row of fields specify treatment of calls for which insufficient bandwidth exists to reach the destination. Automated alternate routing (AAR) handles these calls that are routed to the AAR Destination Mask or Voice Mail. Configure the following values: • Voice Mail—Check this check box to use settings in the Voice Mail Profile Configuration window. When this check box is checked, Cisco Unified Communications Manager ignores the settings in the Coverage/Destination box and Calling Search Space. • AAR Destination Mask—Use this setting instead of the external phone number mask to determine the AAR Destination to be dialed. • AAR Group—This setting provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None indicates that no rerouting of blocked calls will be attempted.
Retain this destination in the call forwarding history	This setting determines whether the AAR leg of the call will be present in the call forwarding history. If you uncheck the check box, the AAR leg of the call is not present in the call history. If you check the check box, the AAR leg of the call will be present in the call history. By default, the directory number configuration retains the AAR leg of the call in the call history, which ensures that the AAR forward to voice-messaging system will prompt the user to leave a voice message.
Call Forward and Call Pickup Settings	

Field	Description
Calling Search Space Activation Policy	

Field	Description
	Three possible values exist for this option: • Use System Default • With Configured CSS • With Activating Device/Line CSS If you select the With Configured CSS option, the Forward All Calling Search Space that is explicitly configured in the Directory Number Configuration window controls the forward all activation and call forwarding. If the Forward All Calling Search Space is set to None, no CSS gets configured for Forward All. A forward all activation attempt to any directory number with a partition will fail. No change in the Forward All Calling Search Space and Secondary Calling Search Space for Forward All occurs during the forward all activation. If you prefer to utilize the combination of the Directory Number Calling Search Space and Device Calling Search Space without explicitly configuring a Forward All Calling Search Space, select With Activating Device/Line CSS for the Calling Search Space Activation Policy. With this option, when Forward All is activated from the phone, the Forward All Calling Search Space and Secondary Calling Search Space for Forward All automatically gets populated with the Directory Number Calling Search Space and Device Calling Search Space for the activating device. With this configuration (Calling Search Space Activation Policy set to With Activating Device/Line), if the Forward All Calling Search Space is set to None, when forward all is activated through the phone, the combination of Directory Number Calling Search Space and activating Device Calling Search Space gets used to verify the forward all attempt. If you configure the Calling Search Space Activation Policy to Use System Default, then the CFA CSS Activation Policy cluster-wide service parameter determines which Forward All Calling Search space will be used. If the CFA CSS Activation Policy service parameter gets set to With Configured CSS, then Forward All Calling Search Space and Secondary Calling Search Space for Forward All will be used for Call Forwarding. If CFA CSS Activation Policy service parameter gets set to With Activating Device/Line CSS, then Forward All Calling Search Space and Secondary Calling Search Space for Forward All will be automatically populated with the Directory Number Calling Search Space and Device Calling Search Space for the activating device. CFA CSS Activation Policy Service Parameter: Ensure the CFA CSS Activation Policy service parameter that displays in the Clusterwide Parameters (Feature - Forward) section of the Service Parameter Configuration window is set correctly for call forward all to work as intended. The parameter includes two possible values: • With Configured CSS (default) • With Activating Device/Line CSS When the Calling Search Space Activation Policy is set to Use System Default, the value of the CFA CSS Activation Policy service parameter gets used to determine

Field	Description
	the Call Forward All CSS. When the option With Configured CSS is selected, the primary and secondary CFA Calling Search Space get used. When the option With Activating Device/Line CSS is selected, the primary and secondary CFA Calling Search Space get updated with primary line Calling Search Space and activating Device Calling Search Space. By default, the value of the CFA CSS Activation Policy service parameter is set to With Configured CSS. Roaming: When a device is roaming in the same device mobility group, Cisco Unified Communications Manager uses the Device Mobility CSS to reach the local gateway. If a user sets Call Forward All at the phone, the CFA CSS is set to None, and the CFA CSS Activation Policy is set to With Activating Device/Line CSS, then: • The Device CSS and Line CSS 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.
Forward All	The settings in this row of fields specify the forwarding treatment for calls to this directory number if the directory number is set to forward all calls. The Calling Search Space field gets used to validate the Forward All destination that is entered when the user activates Call Forward All from the phone. This field also gets used to redirect the call to the Call Forward All destination. Specify the following values: • Voice Mail—Check this check box to use settings in the Voice Mail Profile Configuration window. **Note** When this check box is checked, Cisco Unified Communications Manager ignores the settings in the Destination box and Calling Search Space. • Destination—This setting indicates the directory number to which all calls are forwarded. Use any dialable phone number, including an outside destination. • Calling Search Space—This setting applies to all devices that are using this directory number.

Field	Description
Secondary Calling Search Space for Forward All	Because call forwarding is a line-based feature, in cases where the device calling search space is unknown, the system uses only the line calling search space to forward the call. If the line calling search space is restrictive and not routable, the forward attempt fails. Addition of a secondary calling search space for Call Forward All provides a solution to enable forwarding. The primary calling search space for Call Forward All and secondary calling search space for Call Forward All get concatenated (Primary CFA CSS + Secondary CFA CSS). Cisco Unified Communications Manager uses this combination to validate the CFA destination and to forward the call. See the description for the Calling Search Space field for information about how the combination of Primary and Secondary CFA CSSs works

Field	Description
Forward Busy Internal	The settings in this row of fields specify the forwarding treatment for internal calls to this directory number if the directory number is busy. See the description for the Busy Trigger field for information on when a line is considered busy. The call forward destination and Calling Search Space field get used to redirect the call to the forward destination. Specify the following values: • Voice Mail—Check this check box to use settings in the Voice Mail Profile Configuration window for internal calls. **Note** When this check box is checked, the calling search space of the voice mail pilot gets used. Cisco Unified Communications Manager ignores the settings in the Destination box and Calling Search Space. **Note** When this check box is checked for internal calls, the system automatically checks the Voice Mail check box for external calls. If you do not want external calls to forward to the voice-messaging system, you must uncheck the Voice Mail check box for external calls. • Destination—This setting indicates the call forward busy destination for internal calls. Use any dialable phone number, including an outside destination. **Note** When you enter a destination value for internal calls, the system automatically copies this value to the Destination field for external calls. If you want external calls to forward to a different destination, you must enter a different value in the Destination field for external calls. • Calling Search Space—The Forward Busy internal Calling Search Space is used to forward the call to the Forward Busy Internal destination. It applies to all devices that are using this directory number. **Note** If the system is using partitions and calling search spaces, Cisco recommends that you configure the forward calling search spaces. 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. **Note** When you choose a Calling Search Space for internal calls, the system automatically copies this setting to the Calling Search Space setting for external calls. If you want external calls to forward to a different calling search space, you must choose a different setting in the Calling Search Space drop-down list box.

Field	Description
Forward Busy External	The settings in this row of fields specify the forwarding treatment for external calls to this directory number if the directory number is busy. See the description for the Busy Trigger field for information on when a line is considered busy. The call forward destination and Calling Search Space field get used to redirect the call to the forward destination. Specify the following values: • Voice Mail—Check this check box to use settings in the Voice Mail Profile Configuration window for external calls. **Note** When this check box is checked, the calling search space of the voice mail pilot gets used. Cisco Unified Communications Manager ignores the settings in the Destination box and Calling Search Space. **Note** When the Voice Mail check box is checked for internal calls, the system automatically checks the Voice Mail check box for external calls. If you do not want external calls to forward to the voice-messaging system, you must uncheck the Voice Mail check box for external calls. • Destination—This setting indicates the call forward busy destination for external calls. Use any dialable phone number, including an outside destination. **Note** When you enter a destination value for internal calls, the system automatically copies this value to the Destination field for external calls. If you want external calls to forward to a different destination, you must enter a different value in the Destination field for external calls. • Calling Search Space—The Forward Busy external Calling Search Space is used to forward the call to the Forward Busy External destination. It applies to all devices that are using this directory number. **Note** If the system is using partitions and calling search spaces, Cisco recommends that you configure the forward calling search spaces. 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. **Note** When you choose a Calling Search Space for internal calls, the system automatically copies this setting to the Calling Search Space setting for external calls. If you want external calls to forward to a different calling search space, you must choose a different setting in the Calling Search Space drop-down list box.

Field	Description
Forward No Answer Internal	The settings in this row of fields specify the forwarding treatment for internal calls to this directory number if the directory number does not answer. The call forward destination and Calling Search Space field get used to redirect the call to the forward destination. Specify the following values: • Voice Mail—Check this check box to use settings in the Voice Mail Profile Configuration window. **Note** When this check box is checked, the calling search space of the voice mail pilot gets used. Cisco Unified Communications Manager ignores the settings in the Destination box and Calling Search Space. **Note** When this check box is checked for internal calls, the system automatically checks the Voice Mail check box for external calls. If you do not want external calls to forward to the voice-messaging system, you must uncheck the Voice Mail check box for external calls. • Destination—This setting indicates the directory number to which an internal call is forwarded when the call is not answered. Use any dialable phone number, including an outside destination. **Note** When you enter a destination value for internal calls, the system automatically copies this value to the Destination field for external calls. If you want external calls to forward to a different destination, you must enter a different value in the Destination field for external calls. • Calling Search Space—The Forward No Answer internal Calling Search Space is used to forward the call to the Forward No Answer internal destination. It applies to all devices that are using this directory number. **Note** If the system is using partitions and calling search spaces, Cisco recommends that you configure the forward calling search spaces. 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 No Answer destination, you should also configure the Forward No Answer Calling Search Space. If you do not configure the Forward No Answer Calling Search Space, and the Forward No Answer destination is in a partition, the forward operation may fail. **Note** When you choose a Calling Search Space for internal calls, the system automatically copies this setting to the Calling Search Space setting for external calls. If you want external calls to forward to a different calling search space, you must choose a different setting in the Calling Search Space drop-down list box for external calls.

Field	Description
Forward No Answer External	The settings in this row of fields specify the forwarding treatment for external calls to this directory number if the directory number does not answer. The call forward destination and Calling Search Space field get used to redirect the call to the forward destination. Specify the following values: • Voice Mail—Check this check box to use settings in the Voice Mail Profile Configuration window. **Note** When this check box is checked, the calling search space of the voice mail pilot gets used. Cisco Unified Communications Manager ignores the settings in the Destination box and Calling Search Space. **Note** When this check box is checked for internal calls, the system automatically checks the Voice Mail check box for external calls. If you do not want external calls to forward to the voice-messaging system, you must uncheck the Voice Mail check box for external calls. • Destination—This setting indicates the directory number to which an external call is forwarded when the call is not answered. Use any dialable phone number, including an outside destination. **Note** When you enter a destination value for internal calls, the system automatically copies this value to the Destination field for external calls. If you want external calls to forward to a different destination, you must enter a different value in the Destination field for external calls. • Calling Search Space—The Forward No Answer external Calling Search Space is used to forward the call to the Forward No Answer external destination. It applies to all devices that are using this directory number. **Note** If the system is using partitions and calling search spaces, Cisco recommends that you configure the forward calling search spaces. 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 No Answer destination, you should also configure the Forward No Answer Calling Search Space. If you do not configure the Forward No Answer Calling Search Space, and the Forward No Answer destination is in a partition, the forward operation may fail. **Note** When you choose a Calling Search Space for internal calls, the system automatically copies this setting to the Calling Search Space setting for external calls. If you want external calls to forward to a different calling search space, you must choose a different setting in the Calling Search Space drop-down list box for external calls.

Field	Description
Forward No Coverage Internal	For complete information about Call Coverage, the *Cisco Unified Communications Manager System Guide*. The call forward destination and Calling Search Space field get used to redirect the call to the forward destination. Specify the following values: • Voice Mail—Check this check box to use settings in the Voice Mail Profile Configuration window. **Note** When this check box is checked, Cisco Unified Communications Manager ignores the settings in the Destination box and Calling Search Space. When this check box is checked for internal calls, the system automatically checks the Voice Mail check box for external calls. If you do not want external calls to forward to the voice-messaging system, you must uncheck the Voice Mail check box for external calls. • Destination—This setting specifies the directory number to which an internal nonconnected call is forwarded when an application that controls that directory number fails. Use any dialable phone number, including an outside destination. **Note** When you enter a destination value for internal calls, the system automatically copies this value to the Destination field for external calls. If you want external calls to forward to a different destination, you must enter a different value in the Destination field for external calls. • Calling Search Space—The Forward No Coverage internal Calling Search Space is used to forward the call to the Forward No Coverage internal destination. This setting applies to all devices that are using this directory number. **Note** If the system is using partitions and calling search spaces, Cisco recommends that you configure the forward calling search spaces. 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 No Coverage destination, you should also configure the Forward No Coverage Calling Search Space. If you do not configure the Forward No Coverage Calling Search Space, and the Forward No Coverage destination is in a partition, the forward operation may fail. **Note** When you choose a Calling Search Space for internal calls, the system automatically copies this setting to the Calling Search Space setting for external calls. If you want external calls to forward to a different calling search space, choose a different setting in the Calling Search Space for external calls.

Field	Description
Forward No Coverage External	For complete information about Call Coverage, the *Cisco Unified Communications Manager System Guide*. The call forward destination and Calling Search Space field get used to redirect the call to the forward destination. Specify the following values: • Voice Mail—Check this check box to use settings in the Voice Mail Profile Configuration window. **Note** When this check box is checked, Cisco Unified Communications Manager ignores the settings in the Destination box and Calling Search Space. When this check box is checked for internal calls, the system automatically checks the Voice Mail check box for external calls. If you do not want external calls to forward to the voice-messaging system, you must uncheck the Voice Mail check box for external calls. • Destination—This setting specifies the directory number to which an internal nonconnected call is forwarded when an application that controls that directory number fails. Use any dialable phone number, including an outside destination. **Note** When you enter a destination value for internal calls, the system automatically copies this value to the Destination field for external calls. If you want external calls to forward to a different destination, you must enter a different value in the Destination field for external calls. • Calling Search Space—The Forward No Coverage external Calling Search Space is used to forward the call to the Forward No Coverage external destination. This setting applies to all devices that are using this directory number. **Note** If the system is using partitions and calling search spaces, Cisco recommends that you configure the forward calling search spaces. 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 No Coverage destination, you should also configure the Forward No Coverage Calling Search Space. If you do not configure the Forward No Coverage Calling Search Space, and the Forward No Coverage destination is in a partition, the forward operation may fail. **Note** When you choose a Calling Search Space for internal calls, the system automatically copies this setting to the Calling Search Space setting for external calls. If you want external calls to forward to a different calling search space, choose a different setting in the Calling Search Space for external calls.

Field	Description
Forward on CTI Failure	This field applies only to CTI route points and CTI ports. The settings in this row specify the forwarding treatment for external calls to this CTI route point or CTI port if the CTI route point or CTI port fails. Specify the following values: • Voice Mail—Check this check box to use settings in the Voice Mail Profile Configuration window. **Note** When this check box is checked, Cisco Unified Communications Manager ignores the settings in the Destination box and Calling Search Space. • Destination—This setting specifies the directory number to which an internal nonconnected call is forwarded when an application that controls that directory number fails. Use any dialable phone number, including an outside destination. • Calling Search Space—This setting applies to all devices that are using this directory number.
Forward Unregistered Internal	This field applies to unregistered internal DN calls. The calls are rerouted to a specified Destination Number or Voice Mail. **Note** You must also specify the maximum number of forwards in the Service Parameters Configuration window for a Directory Number.
Forward Unregistered External	This field applies to unregistered external DN calls. The calls are rerouted to a specified Destination Number or Voice Mail. **Note** You must also specify the maximum number of forwards in the Service Parameters Configuration window for a Directory Number.
No Answer Ring Duration (seconds)	Used in conjunction with Call Forward No Answer Destination, this field sets the timer for how long the phone will ring before it gets forwarded. Leave this setting blank to use the value that is set in the Cisco CallManager service parameter, Forward No Answer Timer. **Caution** By default, Cisco Unified Communications Manager makes the time for the T301 timer longer than the No Answer Ring Duration time; if the set time for the T301 timer expires before the set time for the No Answer Ring Duration expires, the call ends, and no call forwarding can occur. If you choose to do so, you can configure the time for the No Answer Ring Duration to be greater than the time for the T301 timer. For information on the T301 timer, choose **System** > **Service Parameters**; choose the server, the Cisco CallManager service, and then the parameter in the window that displays.
Call Pickup Group	Choose the number that can be dialed to answer calls to this directory number (in the specified partition).
Park Monitoring	

Field	Description
Park Monitoring Forward No Retrieve Destination External	When the parkee is an external party, the call will be forwarded to the specified destination in this field. If this field value is empty, the parkee will be redirected to the parker's line. Specify the following values: • Voice Mail—Check this check box to use settings in the Voice Mail Profile Configuration window. **Note** When this check box is checked, Cisco Unified Communications Manager ignores the settings in the Destination box and Calling Search Space. • Destination—This setting specifies the directory number to which a parked call (from an external party) is forwarded when the service parameter Park Monitoring Forward No Retrieve Timer expires. Use any dialable phone number, including an outside destination. • Calling Search Space—A calling search space comprises an ordered list of route partitions that are typically assigned to devices. Calling search spaces determine the partitions that calling devices search when they are attempting to complete a call.
Park Monitoring Forward No Retrieve Destination Internal	When the parkee is an internal party, the call will be forwarded to the specified destination in this field. If this field value is empty, the parkee will be redirected to the parker's line. Specify the following values: • Voice Mail—Check this check box to use settings in the Voice Mail Profile Configuration window. **Note** When this check box is checked, Cisco Unified Communications Manager ignores the settings in the Destination box and Calling Search Space. • Destination—This setting specifies the directory number to which a parked call (from an internal party) is forwarded when the service parameter Park Monitoring Forward No Retrieve Timer expires. Use any dialable phone number, including an outside destination. • Calling Search Space—A calling search space comprises an ordered list of route partitions that are typically assigned to devices. Calling search spaces determine the partitions that calling devices search when they are attempting to complete a call.

Field	Description
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. The default is 60 seconds. **Note** If you configure a non-zero value, this value overrides the value of this parameter set in the Service Parameters window. However, if you configure a value of 0 here, then the value in the Service Parameters window will be used.
MLPP Alternate Party Settings	
Target (Destination)	Enter the number to which MLPP precedence calls should be diverted if this directory number receives a precedence call and neither this number nor its call forward destination answers the precedence call. Values can include numeric characters, octothorpe (#), and asterisk (*).
MLPP Calling Search Space	From the drop-down list box, choose the calling search space to associate with the MLPP alternate party target (destination) number.
MLPP No Answer Ring Duration (seconds)	Enter the number of seconds (between 4 and 60) after which an MLPP precedence call will be directed to this directory number alternate party if this directory number and its call-forwarding destination have not answered the precedence call. Leave this setting blank to use the value that is set in the Cisco Unified Communications Manager enterprise parameter, Precedence Alternate Party Timeout.
Confidential Access Level	Select the appropriate CAL value from the drop-down list box.
Confidential Access Mode	From the drop-down list box, select one of the following options to set the CAL mode: • Fixed—CAL value has higher precedence over call completion. • Variable—Call completion has higher precedence over CAL level.
Call Control Agent Profile	Select the Call Control Agent Profile to associate to the directory number user. Configure a Call Control Agent Profile from the **Advanced Features** > **Call Control Agent Profile** menu.
Line Settings for All Devices	
Hold Reversion Ring Duration (seconds)	Enter a number from 0 to 1200 (inclusive) to specify the wait time in seconds before issuing a reverted call alert to the holding party phone. If you enter a value of 0, Cisco Unified Communications Manager does not invoke the reverted call feature for a held call. At installation, this field remains blank. If you leave this setting blank, the Hold Reversion Duration timer setting for the cluster applies.

Field	Description
Hold Reversion Notification Interval (seconds)	Enter a number from 0 to 1200 (inclusive) to specify the interval time in seconds for sending periodic reminder alerts to the holding party phone. If you enter a value of 0, Cisco Unified Communications Manager does not send reminder alerts. At installation, this field remains blank. If you leave this setting blank, the Hold Reversion Notification Interval timer setting for the cluster applies. **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.
Party Entrance Tone	From the Party Entrance Tone drop-down list box, choose one of the following options: • Default—Use the value that you configured in the Party Entrance Tone service parameter. • On—A tone plays on the phone when a basic call changes to a multi-party call; that is, a barge call, cBarge call, ad hoc conference, meet-me conference, or a joined call. In addition, a different tone plays when a party leaves the multi-party call. If the controlling device, that is, the originator of the multi-party call has a built-in bridge, the tone gets played to all parties if you choose On 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. • Off—A tone does not play on the phone when a basic call changes to a multi-party call.
Line [number] on Device [device name] **Note** These fields display only after you associate this directory number with a device.	
Display (Internal Caller ID)	Leave this field blank to have the system display the extension. Use a maximum of 30 characters. Typically, use the user name or the directory number (if using the directory number, the person receiving the call may not see the proper identity of the caller). Setting applies only to the current device unless you check the check box at right (Update Shared Device Settings) and click the Propagate Selected button. (The check box at right displays only if other devices share this directory number.)

Field	Description
ASCII Display (Internal Caller ID)	This field provides the same information as the Display (Internal Caller ID) field, but you must limit input to ASCII characters. Devices that do not support Unicode (internationalized) characters display the content of the ASCII Display (Internal Caller ID) field. Setting applies only to the current device unless you check the check box at right (Update Shared Device Settings) and click the Propagate Selected button. (The check box at right displays only if other devices share this directory number.)
Line Text Label	Use this field only if you do not want the directory number to show on the line appearance. Enter text that identifies this directory number for a line/phone combination. Suggested entries include boss name, department name, or other appropriate information to identify multiple directory numbers to secretary/assistant who monitors multiple directory numbers. Setting applies only to the current device unless you check the check box at right (Update Shared Device Settings) and click the Propagate Selected button. (The check box at right displays only if other devices share this directory number.)
External Phone Number Mask	Indicate phone number (or mask) that is used to send Caller ID information when a call is placed from this line. You can enter a maximum of 24 number, the international escape character +, and "X" characters. The Xs represent the directory number and must appear at the end of the pattern. For example, if you specify a mask of 972813XXXX, an external call from extension 1234 displays a caller ID number of 9728131234. Setting applies only to the current device unless you check the check box at right (Update Shared Device Settings) and click the Propagate Selected button. (The check box at right displays only if other devices share this directory number.)
Visual Message Waiting Indicator Policy	Use this field to configure the handset lamp illumination policy. Choose one of the following options: • Use System Policy (The directory number refers to the service parameter "Message Waiting Lamp Policy" setting.) • Light and Prompt • Prompt Only • Light Only • None Setting applies only to the current device unless you check the check box at right (Update Shared Device Settings) and click the Propagate Selected button. (The check box at right displays only if other devices share this directory number.)

Field	Description
Audible Message Waiting Indicator Policy	Use this field to configure an audible message waiting indicator policy. Choose one of the following options: • Off • On—When you select this option, you will receive a stutter dial tone when you take the handset off hook. • Default—When you select this option, the phone uses the default that was set at the system level.
Ring Setting (Phone Idle)	Use this field to configure the ring setting for the line appearance when an incoming call is received and no other active calls exist on that device. Choose one of the following options: • Use system default • Disable • Flash only • Ring once • Ring Setting applies only to the current device unless you check the check box at right (Update Shared Device Settings) and click the Propagate Selected button. (The check box at right displays only if other devices share this directory number.) **Note** Turning on MLPP Indication (at the enterprise parameter, device pool, or device level) disables normal Ring Setting behavior for the lines on a device, unless MLPP Indication is turned off (overridden) for the device.
Ring Setting (Phone Active)	From the drop-down list box, choose the ring setting that is used when this phone has another active call on a different line. Choose one of the following options: • Use system default • Disable • Flash only • Ring once • Ring • Beep only Setting applies only to the current device unless you check the check box at right (Update Shared Device Settings) and click the Propagate Selected button. (The check box at right displays only if other devices share this directory number.) **Note** Turning on MLPP Indication (at the enterprise parameter, device pool, or device level) disables normal Ring Setting behavior for the lines on a device, unless MLPP Indication is turned off (overridden) for the device.

Field	Description
Call Pickup Group Audio Alert Setting (Phone Idle)	This field determines the type of notification an incoming call sends to members of a call pickup group. If the called phone does not answer, the phones in the call pickup group that are idle will either hear a short ring (ring once) or hear nothing (disabled). • Use System Default—The value of this field gets determined by the setting of the Cisco CallManager service parameter Call Pickup Group Audio Alert Setting of Idle Station. • Disable—No alert is sent to members of the call pickup group. • Ring Once—A short ring is sent to members of the call pickup group.
Call Pickup Group Audio Alert Setting (Phone Active)	This field determines the type of notification an incoming call sends to members of a call pickup group. If the called phone does not answer, the phones in the call pickup group that are busy will either hear a beep (beep beep) or hear nothing (disabled). • Use System Default—The value of this field gets determined by the setting of the Cisco CallManager service parameter Call Pickup Group Audio Alert Setting of Busy Station. • Disable—No alert is sent to member of the call pickup group. • Beep Only—A beep beep is sent to members of the call pickup group.

Field	Description
Recording Option	This field determines the recording option on the line appearance of an agent. The default recording option is Call Recording Disabled. Choose one of the following options: • Call Recording Disabled—Calls made on this line appearance cannot be recorded. • Automatic Call Recording Enabled—Calls made on this line appearance are recorded automatically. • Selective Call Recording Enabled—Calls made on this line appearance can be recorded using a softkey or programmable line key that is assigned to the device, a CTI-enabled application, or both interchangeably. Selective recording supports two modes: • Silent recording—Call recording status is not reflected on the Cisco IP device display. Silent recording is typically used in a call center environment to allow a supervisor to record an agent call. A CTI-enabled application running on the supervisor desktop is generally used to start and stop the recording for an agent-customer call. • User recording—Call recording status is reflected on the Cisco IP device display. A recording can be started or stopped using a softkey, programmable line key, or CTI-enabled application running on the user desktop. To enable user recording, add the Record softkey or programmable line key to the device template. Do not add the Record key if only silent recording is desired. When the recording option is set to either Automatic Call Recording Enabled or Selective Call Recording Enabled, the line appearance can be associated with a recording profile. When automatic recording is enabled, start- and stop-recording requests using a softkey, programmable line key, or CTI-enabled application are rejected.
Recording Profile	This field determines the recording profile on the line appearance of an agent. Choose an existing recording profile from the drop-down list box. To create a recording profile, use the **Device** > **Device Settings** > **Recording Profile** menu option. The default value specifies None.
Recording Media Source	This field determines the recording media source option on the line appearance. Choose one of the following options: • Gateway Preferred—Voice gateway is selected as the recording media source when the call is routed through a recording enabled gateway. • Phone Preferred—Phone is selected as the recording media source **Note** For non-BIB devices, the default option is Gateway Preferred.

Field	Description
Monitoring Calling Search Space	The monitoring calling search space of the supervisor line appearance must include the agent line or device partition to allow monitoring the agent. Set the monitoring calling search space on the supervisor line appearance window. Choose an existing calling search space from the drop-down list box. The default value specifies None.
Log Missed Calls	If the check box displays as checked, which is the default for this setting, Cisco Unified Communications Manager logs missed calls in the call history for the shared line appearance on the phone. If you uncheck the check box, missed calls do not get logged to the shared line appearance.
Multiple Call/Call Waiting Settings on Device [device name] **Note** These fields display only after you associate this directory number with a device.	
Maximum Number of Calls	You can configure up to 200 calls for a line on a device, with the limiting factor being the total number of calls that are configured on the device. As you configure the number of calls for one line, the calls that are available for another line decrease. The default specifies 4. If the phone does not allow multiple calls for each line, the default specifies 2. For CTI route points, you can configure up to 10,000 calls for each port. The default specifies 5000 calls. Use this field in conjunction with the Busy Trigger field. **Note** Although the default specifies 5000 calls for maximum number of active calls that can be configured on a CTI route point, Cisco recommends that you set the maximum number of calls to no more than 200 per route point. This will prevent system performance degradation. If the CTI application needs more than 200 calls, Cisco recommends that you configure multiple CTI route points. **Tip** If you use the external call control feature, and the policies on the policy server dictate that a chaperone must monitor and record calls, make sure that you set the Maximum Number of Calls setting to 2 and set the Busy Trigger setting to 1. **Tip** To review how this setting works for devices with shared line appearances, see topics related to shared line appearance in the *Cisco Unified Communications Manager System Guide*.
Busy Trigger	This setting, which works in conjunction with Maximum Number of Calls and Call Forward Busy, determines the maximum number of calls to be presented at the line. If maximum number of calls is set for 50 and the busy trigger is set to 40, incoming call 41 gets rejected with a busy cause (and will get forwarded if Call Forward Busy is set). If this line is shared, all the lines must be busy before incoming calls get rejected. Use this field in conjunction with Maximum Number of Calls for CTI route points. The default specifies 4500 calls. **Tip** To review how this setting works for devices with shared line appearances, see topics related to shared line appearance in the *Cisco Unified Communications Manager System Guide*.

Field	Description
Forwarded Call Information Display on Device [device name] **Note** These fields display only after you associate this directory number with a device.	
Caller Name	Checking this check box will cause the caller name to display upon call forward.
Caller Number	Checking this check box will cause the caller number to display upon call forward.
Redirected Number	Checking this check box will cause the number that was redirected to display upon call forward.
Dialed Number	Checking this check box will cause the original dialed number to display upon call forward.
Users Associated with Line **Note** This information displays only after you associate this directory number with a device.	
(user name)	This pane displays the end users that are associated with this line. To associate end users with this line, click the Associate End Users button, which causes the Find and List Users popup window to display. In the popup window, you can use the Find function to find end users to associate with this line. After you have found the end users to associate with this line, click the Add Selected button, and the selected end users will be added to the Users Associated with Line pane for this line. For each associated end user, the following information displays: • Full Name—This column displays the last name and first name entries for the associated end user. • User ID—This column displays the user ID of the associated end user. • Permission—Click the i button to display the user privilege information for this end user. After at least one end user has been associated with this line, the following additional buttons display: • Select All—Click this button to select all end users that are associated with this line. • Clear All—Click this button to deselect all end users that are associated with this line. • Delete Selected—After selecting any end users that you wish to dissociate from this line, click this button. Doing so dissociates the end users from this line, but does not delete the end user records.

Related Topics

Service Parameter Setup , on page 151

Line Group Setup , on page 223
Search for Partition , on page 270
Display Calling Search Space , on page 320
Cisco Unified IP Phone Setup , on page 579
Device Profile Setup , on page 713
About End User Setup , on page 841

Display Calling Search Space

You can configure the number of calling search spaces 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 Calling Search Space drop-down list box on the Cisco Unified Communications Manager Administration windows where the button appears. Click the Find button to search for the calling search space that you want.

Note To set the maximum list box items, choose **System** > **Enterprise Parameters** and choose CCMAdmin Parameters.

Related Topics

Directory Number Setup , on page 289

Synchronize Directory Number Settings with Devices

To synchronize devices with a directory number that has undergone configuration changes, perform the following procedure, which applies 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** > **Directory Number Configuration**.
The Find and List Directory Numbers window displays.

Step 2 Choose the search criteria to use.

Step 3 Click Find.
The window displays a list of directory numbers that match the search criteria.

Step 4 Click the directory number to which you want to synchronize applicable devices. The 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.

Note If devices require a restart, the system may drop active calls on gateways.

Step 8 Click OK.

Related Topics

Directory Number Setup , on page 289

Set Up Private Line Automatic Ringdown (PLAR)

You can configure Private Line Automatic Ringdown (PLAR), so when the user goes off hook (or the NewCall softkey or line key gets pressed), the phone immediately dials a preconfigured number. The phone user cannot dial any other number from the phone line that gets configured for PLAR.

PLAR works with features such as barge, cBarge, or single button barge. If you use PLAR with a feature, you must configure the feature as described in the feature documentation, and you must configure the PLAR destination, which is a directory number that is used specifically for PLAR.

See the example of how to configure PLAR, which describes how to enable PLAR functionality for phones that support barge and that are running SCCP and SIP.

Related Topics

Set Up PLAR Example , on page 321

Set Up PLAR Example

This example of how to configure PLAR describes how to enable PLAR functionality for phones that support barge and that are running SCCP and SIP. A and A' represent shared-line devices that you configured for barge, and B1 represents the directory number for the PLAR destination. Follow this example to enable PLAR functionality from A/A'.

Tip Set Up PLAR Example , on page 321 through Set Up PLAR Example , on page 321 apply if you want to configure PLAR for phones that are running SCCP. For phones that are running SIP, you must perform Set Up PLAR Example , on page 321 through Set Up PLAR Example , on page 321. Before you attempt to configure PLAR, verify that your phone model supports PLAR. To determine whether your phone supports PLAR, see the *Cisco Unified IP Phone Administration Guide* that supports your phone model and this release of Cisco Unified Communications Manager.

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 null (blank) translation pattern, for example, TP1, which contains calling search space CSS1 and partition P1. In this null (blank) pattern, 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.)

Related Topics

Directory Number Setup , on page 289

Remove Directory Number From Phone

Perform the following procedure to remove a directory number (DN) from a specific phone.

Before You Begin

If you try to remove a directory number that is in use, Cisco Unified Communications Manager displays a message. To find out which line groups are using the directory number, click the Dependency Records link from the Directory Number Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message.

When you remove a directory number from a phone, the number still exists within Cisco Unified Communications Manager. To see a list of directory numbers that are not associated with phones, use the Route Plan Report menu option.

Procedure

Step 1 Choose **Device** > **Phone**.
The Find and List Phones window displays.

Step 2 To locate a specific phone, enter the search criteria and click Find.
A list of phones that match the search criteria displays.

Step 3 Choose the device name that contains the directory number that you want to remove.
The Phone Configuration window displays.

Step 4 In the Association Information area on the left, choose the line that you want to remove.
The Directory Number Configuration window displays.

Step 5 In the Associated Devices pane, choose the device name of the phone from which you want to remove this directory number.

Step 6 Click the down arrow below the Associated Devices pane.

The phone name moves to the Dissociate Devices pane.

Step 7 Click the Save button at the bottom of the Directory Number Configuration window.
The Phone Configuration window displays with the directory number removed. The change gets automatically applied to the phone; however, you can click Reset Phone.

Related Topics

Directory Number Setup , on page 289
Delete Unassigned Directory Number , on page 335
Phone Setup , on page 581
Access Dependency Records , on page 982

Create Cisco Unity Connection Voice Mailbox

The "Create Cisco Unity Voice Mailbox" link on the Directory Number Configuration window allows administrators to create individual Cisco Unity Connection voice mailboxes from Cisco Unified Communications Manager Administration. If Cisco Unified Communications Manager is integrated with Cisco Unity Connection, this link allows you to create a Cisco Unity Connection voice mailbox.

To configure a voice mailbox and other Cisco Unity Connection settings in Cisco Unity Connection Administration, see the applicable User Moves, Adds, and Changes Guide for Cisco Unity Connection. Ensure that you have defined an appropriate template and selected a class of service (COS) for the users that you plan to add.

Note Before you can create a Cisco Unity Connection voice mailbox for the end user, you must first configure the end user with a phone device association and a primary extension, and the integration between Cisco Unified Communications Manager and Cisco Unity Connection must be complete. For more information, see the Cisco Unified Communications Manager SCCP Integration Guide for Cisco Unity Connection or the Cisco Unified Communications Manager SIP Trunk Integration Guide for Cisco Unity Connection.

Before You Begin

- You must configure Cisco Unified Communications Manager for voice-messaging service. See topics related to Cisco Unity and Cisco Unity Connection Configuration in the *Cisco Unified Communications Manager System Guide*.
- You must configure Cisco Unity Connection servers. See the applicable *Installation Guide for Cisco Unity Connection*.
- For Cisco Unity Connection integration, create an AXL connection via Cisco Unity Connection, as described in the "Managing the Phone System Integrations" chapter in the *System Administration Guide for Cisco Unity Connection*.
- Ensure the Cisco RIS Data Collector service is activated. See the *Cisco Unified Serviceability Administration Guide*.

- On the Directory Number configuration window, ensure the Voice Mail Profile setting is configured and contains a pilot number, or the Voice Mail Profile setting should be set to None. If the Voice Mail Profile is set to No Voice Mail, the "Create Cisco Unity User" link does not display.
- Ensure that you have defined an appropriate template and selected a class of service (COS) for the users you plan to add. For Cisco Unity Connection users, see the User Moves, Adds, and Changes Guide for Cisco Unity Connection.

Note The End User Configuration window also includes the "Create Cisco Unity Voice Mailbox" link.

Procedure

Step 1 Choose **Call Routing** > **Directory Number** and click Add New.

Step 2 Enter the appropriate settings in Table 50: Directory Number Settings , on page 291.

Step 3 From the Related Links drop-down list box, in the upper, right corner of the window, choose the "Create Cisco Unity Voice Mailbox" link and click Go.
The Add Cisco Unity User dialog box displays.

Step 4 From the Application Server drop-down list box, choose the Cisco Unity Connection server on which you want to create a Cisco Unity Connection mailbox and click Next.

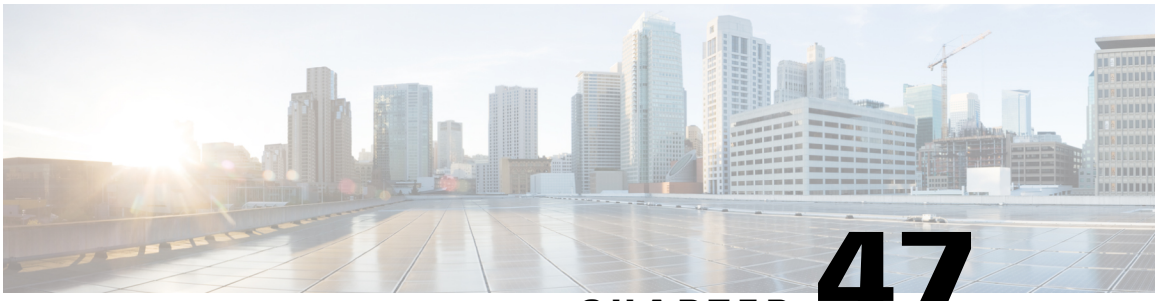
Step 5 From the Subscriber Template drop-down list box, choose the subscriber template that you want to use.

Step 6 Click Save.
The Cisco Unity Connection mailbox gets created.

From Cisco Unity Connection Administration, you can now see the mailbox that you created. See the applicable User Moves, Adds, and Changes Guide for Cisco Unity Connection.

Related Topics

Directory Number Setup , on page 289



CHAPTER 47

Meet-Me Number and Pattern Setup

This chapter provides information about Meet-Me Number and Pattern configuration.

For additional information, see topics related to conference bridges in the *Cisco Unified Communications Manager System Guide*.

About Meet-Me Number and Pattern Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Meet-Me Number/Pattern** menu path to configure meet-me numbers/patterns.

Meet-Me conferences require an allocation of directory numbers. Cisco Unified Communications Manager Administration provides the Meet-Me conference directory number range to users, so they can access the feature.

Meet-Me Numbers and Patterns Configuration Tips

Make sure that the following prerequisites are met before you configure Meet-Me numbers/patterns:

- Configure the server(s).
- Configure the device pools.

Related Topics

Server Setup , on page 27
Device Pool Setup , on page 79

Meet-Me Number and Pattern Settings

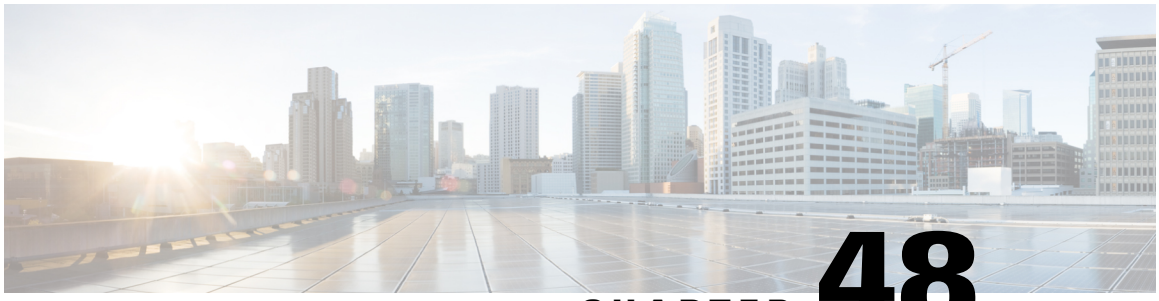
The following table describes the meet-me number/pattern settings.

Table 51: Meet-Me Number and Pattern Settings

Field	Description
Directory Number or Pattern	Enter a Meet-Me Numbers/pattern or a range of numbers. To configure a range, the dash must appear within brackets and follow a digit; for example, to configure the range 1000 to 1050, enter 10[0-5]0.
Description	The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), or angle brackets (<>).
Partition	To use a partition to restrict access to the meet-me/number pattern, choose the desired partition from the drop-down list box. If you do not want to restrict access to the meet-me number/pattern, choose <None> for the partition. See the Partition Setup , on page 267 for more information. 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. Find and choose a partition name by using the procedure in the Search for Partition , on page 270. **Note** To set the maximum list box items, choose **System** > **Enterprise Parameters** and update the Max List Box Items field under CCMAdmin Parameters. **Note** Make sure that the combination of meet-me number/pattern and partition is unique within the Cisco Unified Communications Manager cluster.
Minimum Security Level	Choose the minimum Meet-Me conference security level for this meet-me number or pattern from the drop-down list box. • Choose Authenticated to block participants with nonsecure phones from joining the conference. • Choose Encrypted to block participants with authenticated or nonsecure phones from joining the conference. • Choose Non Secure to allow all participants to join the conference. **Note** To invoke this feature, ensure you have a secure conference bridge that is configured and available. See the *Cisco Unified Communications Manager Security Guide* for more information.

Related Topics

Meet-Me Number and Pattern Setup , on page 325



CHAPTER 48

Dial Plan Installer

This chapter describes how to install, upgrade, or uninstall dial plans on Cisco Unified Communications Manager.

Dial Plan Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Dial Plan** Installer menu path to configure dial plans.

You can install a Cisco International Dial Plan and use it to create a unique numbering plan that is specific to a country, other than one in North America. Cisco Unified Communications Manager provides North American Numbering Plan (NANP) by default. Because dial plan requirements of other countries are unique to those countries, the default NANP configuration may not be the best suited configuration to create a dial plan for those countries. Cisco International Dial Plan allows you to create and update unique dial plans and make them available for use to Cisco customers worldwide.

Before you install a dial plan on the server, you should download the equivalent dial plan COP (Cisco Option Package) file to the Cisco Unified Communications Manager server.

You can find COP files for all the available dial plans that you can download, install, and integrate with Cisco Unified Communications Manager systems on the Cisco website.

For details on installing a COP file, see the *Cisco Unified Communications Manager Dial Plan Guide*.

Related Topics

Install Dial Plan on Cisco Unified Communications Manager , on page 328

Edit Dial Plan

Use the following procedures to install, upgrade, or uninstall dial plans.

Procedure

Step 1 Find the Dial Plan that you want to install.

Step 2 From the list of records, click the Dial Plan name that matches your search criteria.
The Dial Plan Configuration window displays.

Step 3 Complete one of the following tasks:

a) Install a dial plan.
b) Upgrade a dial plan.
c) Uninstall a dial plan.

Related Topics

Dial Plan Installer , on page 327
Install Dial Plan on Cisco Unified Communications Manager , on page 328
Upgrade Dial Plan , on page 329
Uninstall Dial Plan , on page 330

Install Dial Plan on Cisco Unified Communications Manager

After you find a dial plan to install, use the following procedure to install the dial plan.

In the Dial Plan Configuration window, the dial plan name and description display in the Dial Plan and Description fields.

The Installed Version displays the current version that is installed on Cisco Unified Communications Manager server. If no version of the dial plan is installed, the Installed Version displays Not Installed.

Procedure

Step 1 Choose the dial plan version that you want to install from the Available Version drop-down list box.

Step 2 Click Install.
The Status displays that the dial plan has been installed.

The Installed Version field displays the dial plan version that is installed on Cisco Unified Communications Manager server.

Step 3 Repeat Install Dial Plan on Cisco Unified Communications Manager , on page 328 to Install Dial Plan on Cisco Unified Communications Manager , on page 328 to install the dial plans on all the nodes Cisco Unified Communications Manager cluster.

What to Do Next

After installation of the dial plans, restart the Cisco CallManager service to load the dial plan.

Related Topics

Dial Plan Installer , on page 327

Set Up Route Pattern Details for Non-NANP Dial Plan

If you have installed a non-NANP dial plan on your Cisco Unified Communications Manager system, you can choose the required dial plan when you set up route pattern details in the Route Details Configuration window in Cisco Unified Communications Manager.

Note the following points when you configure route pattern details:

1. For a non-NANP dial plan, if you want to retain the settings at the Route Pattern level, make one of the following choices in the Route Details Configuration window:
2. Choose None in the Discard Digits field. Choosing None DDI in the Discard Digits field represents the same as not choosing a dial plan.
3. Choose a non-NANP dial plan:No Digits in the Discard Digits field. (For Example, AMNP:No Digits.)
4. If you want to specify settings at the Route Group level that will override the Route Pattern settings, choose the appropriate DDI for that dial plan from the Discard Digits field. Examples of DDI: NANP:PreDot, AMNP:PreDot.

Related Topics

Dial Plan Installer , on page 327

Upgrade Dial Plan

If you have installed a non-NANP dial plan, you can upgrade the dial plan that is installed on your Cisco Unified Communications Manager system with an upgraded version of the dial plan.

Caution Upgrading a dial plan will fail if you configured one or more tags as a clause for a route filter in the existing version of the dial plan and the upgrade version does not contain these tags. After you upgrade to the new dial plan, the upgrade will list all such tags. You need to disassociate these tags from the route filter and run the dial plan upgrade again on the Cisco Unified Communications Manager system.

Caution Upgrading a dial plan will fail if you have associated one or more DDIs with Route Patterns/Translation Patterns/Route Lists in the existing version of the dial plan and the upgrade version does not contain these DDIs. The dial plan upgrade will list all such DDIs. You need to disassociate these DDIs from Route Patterns/Translation Patterns/Route Lists and run the dial plan upgrade again on the Cisco Unified Communications Manager system.

Note Make sure that you update the dial plans on the first node server of the Cisco Unified Communications Manager cluster before updating them on subscribers or other nodes in the cluster.

After you find a dial plan to upgrade, use the following procedure to upgrade an existing dial plan.

In the Dial Plan Configuration window, the dial plan name and description display in the Dial Plan and Description fields.

The Installed Version displays the current version that is installed on Cisco Unified Communications Manager server. If no version of the dial plan is installed, the Installed Version displays Not Installed.

Procedure

Step 1 Choose the dial plan version that you want to upgrade from the Available Version drop-down list box.

Step 2 Click Install.
The Status displays that the dial plan has been upgraded.

The Installed Version field displays the latest dial plan version.

Step 3 Repeat Step 1, on page 330 to Step 2, on page 330 to upgrade the dial plans on all nodes of Cisco Unified Communications Manager cluster where the Cisco CallManager service is installed.

Note After upgrading the dial plans, restart the Cisco CallManager service for the changes to take effect.

Note To update dial plans, you must install the COP file, as described in the Cisco Unified Communications Manager Dial Plan Guide, and install the dial plans that you want.

Related Topics

Dial Plan Installer , on page 327
Install Dial Plan on Cisco Unified Communications Manager , on page 328
Restart Cisco CallManager Service , on page 331

Uninstall Dial Plan

Caution Before you uninstall a dial plan, ensure that you remove the route patterns, translation patterns, route lists, and route filters that are configured in the dial plan on the Cisco Unified Communications Manager system.

After you find a dial plan to uninstall, use the following procedure to uninstall the dial plan.

The dial plan name and description display in the Dial Plan and Description fields.

The Installed Version displays the current version that is installed on the Cisco Unified Communications Manager server.

Procedure

Step 1 Click Uninstall.

Note Dial plans should be uninstalled first from the first node in the cluster and then from the subsequent nodes.

The Status displays that the dial plan was deleted.

The Installed Version field displays Not Installed.

Step 2 Repeat Step 1, on page 330 to uninstall the dial plans on all nodes of the Cisco Unified Communications Manager cluster.

Related Topics

Dial Plan Installer , on page 327

Restart Cisco CallManager Service

Use the following procedure to restart the Cisco CallManager service.

Procedure

Step 1 In the Cisco Unified Serviceability window, choose **Tools** > **Control Center - Feature Services**.
The Control Center–Feature Services window displays.

Step 2 Choose the Cisco Unified Communications Manager server from the Servers drop-down list box.
In the CM Services area, Cisco CallManager displays in the Service Name column.

Note Click the radio button corresponding to the Cisco CallManager service.

Step 3 If you want to restart the Cisco CallManager service, click Restart.
The service restarts, and the message, Service Successfully Restarted, displays.

Step 4 If you want to start a stopped Cisco CallManager service, click Start.
The service starts, and the message, Service Successfully Started, displays.

Related Topics

Dial Plan Installer , on page 327

CHAPTER 49

Route Plan Report

This chapter provides information about viewing route plan report records and managing unassigned directory numbers.

For additional information, see topics related to route plans and directory number configuration settings in the *Cisco Unified Communications Manager System Guide*. Also see topics related to local route groups in the *Cisco Unified Communications Manager Features and Services Guide*.

About Route Plan Report

The route plan report lists all of the following types of directory and other numbers in the system:

- Unassigned directory numbers (DN)
- Call park numbers
- Conference numbers
- Directory numbers (DN)
- Calling party transformation patterns
- Called party transformation patterns
- Translation patterns
- Call pickup group numbers
- Route patterns
- Message-waiting indicators
- Voice-mail ports

- Domain routing
- IP routing
- Hunt pilots
- Directed call park numbers
- Intercom directory numbers
- Intercom translation patterns
- Handoff numbers (configured in the Mobility Configuration window [**Call Routing** > **Mobility** > **Handoff Configuration**])
- Enterprise Feature Access numbers (configured in the Mobility Configuration window [**Call Routing** > **Mobility** > **Enterprise Feature Access Configuration**])
- Mobile Voice Access numbers (configured in the Service Parameters window [**System** > **Service Parameters**])
- Mobile Voice Access directory numbers (configured in the Mobile Voice Access window [**Media Resources** > **Mobile Voice Access**])

The route plan report allows you to view either a partial or full list and to go directly to the associated configuration windows by clicking the entry in the Pattern/Directory Number, Partition, or Route Detail columns of the report.

In addition, the route plan report allows you to save report data into a .csv file that you can import into other applications. The .csv file contains more detailed information than the web pages, including directory numbers for phones, route patterns, pattern usage, device name, and device description.

Cisco Unified Communications Manager uses the route plan to route both internal calls and external public switched telephone network (PSTN) calls. For more detailed information on the route plan, see topics related to understanding route plans in *Cisco Unified Communications Manager System Guide*.

Note See topics related to local route groups in the *Cisco Unified Communications Manager System Guide* for a discussion of the route plan report and its format when the Local Route Group feature is configured.

Related Topics

Route Plan Report , on page 333
View Route Plan Records , on page 334
Delete Unassigned Directory Number , on page 335
View Route Plan Reports in Files , on page 336

View Route Plan Records

This section describes how to view route plan records. Because you might have several records in your network, Cisco Unified Communications Manager Administration lets you locate specific route plan records on the basis of specific criteria. Use the following procedure to generate customized route plan reports.

Procedure

Step 1 Choose **Call Routing** > **Route Plan Report**.
The Route Plan Report window displays.

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3, on page 335.
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.

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.

Step 4 From the list of records that display, click the link for the record that you want to view.
The window displays the item that you choose.

Related Topics

Route Plan Report , on page 333

Delete Unassigned Directory Number

This section describes how to delete an unassigned directory number from the route plan report. Directory numbers get configured and removed in the Directory Number Configuration window of Cisco Unified Communications Manager Administration. When a directory number gets removed from a device or a phone gets deleted, the directory number still exists in the Cisco Unified Communications Manager database. To delete the directory number from the database, use the Route Plan Report window.

Procedure

Step 1 Choose Call **Call Routing** > **Route Plan Report**.
The Route Plan Report window displays. Use the three drop-down list boxes to specify a route plan report that lists all unassigned DNs.

Step 2 Three ways exist to delete directory numbers:

a) Click the directory number that you want to delete. When the Directory Number Configuration window displays, click Delete.
b) Check the check box next to the directory number that you want to delete. Click Delete Selected.
c) To delete all found unassigned directory numbers, click Delete All Found Items.
A warning message verifies that you want to delete the directory number.

Step 3 To delete the directory number, click OK. To cancel the delete request, click Cancel.

Related Topics

Route Plan Report , on page 333

Update Unassigned Directory Numbers

This section describes how to update the settings of an unassigned directory number from the route plan report. Directory numbers get configured and removed in the Directory Number Configuration window of Cisco Unified Communications Manager Administration. When a directory number gets removed from a device, the directory number still exists in the Cisco Unified Communications Manager database. To update the settings of the directory number, use the Route Plan Report window.

Procedure

Step 1 Choose **Call Routing** > **Route Plan Report**.
The Route Plan Report window displays. Use the three drop-down list boxes to specify a route plan report that lists all unassigned DNs.

Step 2 Click the directory number that you want to update.
The Directory Number Configuration window displays.

Note You can update all the settings of the directory number except the directory number and partition.

Step 3 Make the required updates such as calling search space or forwarding options.

Step 4 Click Save.
The Directory Number Configuration window redisplays, and the directory number field is blank.

Related Topics

Route Plan Report , on page 333

View Route Plan Reports in Files

This section contains information on how to view route plan reports in a .csv file.

Procedure

Step 1 Choose **Call Routing** > **Route Plan Report**.
The Route Plan Report window displays.

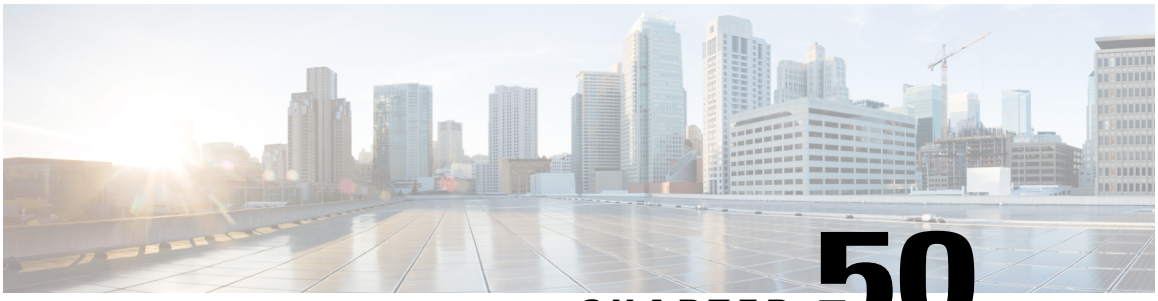
Step 2 Choose View In File from the Related Links drop-down list box on the Route Plan Report window and click Go. A dialog box displays.
From this dialog box, you can either save the file or import it into another application.

Step 3 Click Save.
Another window displays that allows you to save this file to a location of your choice.

Note You may also save the file as a different file name, but the file name must include a .csv extension.

Step 4 Choose the location in which to save the file and click Save. This action should save the file to the location that you designated.

Step 5 Locate the .csv file that you just saved and double-click its icon to view it.



CHAPTER 50

Calling Party Transformation Pattern Setup

This chapter provides information to find, add, update, copy, or delete a calling party transformation pattern.

For additional information, see topics related to calling party number transformations settings, wildcards and special characters in route patterns and hunt pilots in the *Cisco Unified Communications Manager System Guide*. Also see topics related to calling party normalization and local route groups in the *Cisco Unified Communications Manager Features and Services Guide*.

About Calling Party Transformation Pattern Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Transformation Pattern** > **Calling Party Transformation Pattern** menu path to configure calling party transformation patterns.

The parameters in the Calling Party Transformation Patterns window provide appropriate caller information using the Calling Party Transformation calling search space on the destination device. Be aware that calls through transformation patterns are not routable. When this pattern is matched, the call does not route to any device.

You use calling party transformation patterns with the calling party normalization feature. For information on the calling party normalization feature, see topics related to calling party normalization in the *Cisco Unified Communications Manager Features and Services Guide*..

Note See topics related to local route groups in the *Cisco Unified Communications Manager Features and Services Guide* for a discussion of calling party transformation patterns and their use and configuration when the Local Route Group feature is configured.

Calling Party Transformation Pattern Settings

The following table describes the calling party transformation pattern settings.

Table 52: Calling Party Transformation Pattern Settings

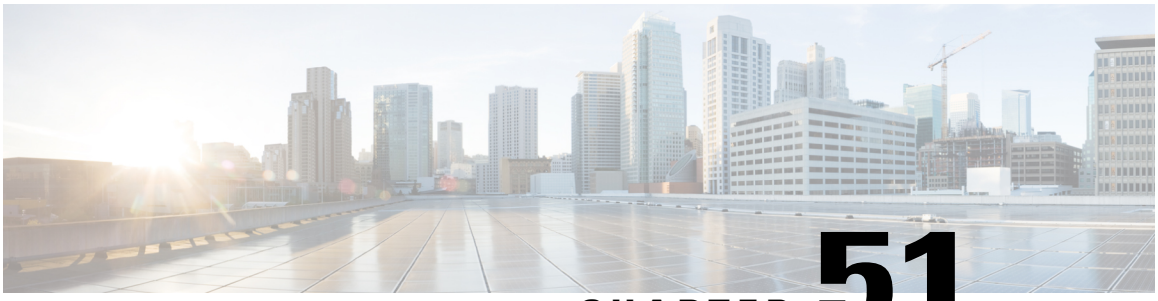
Field	Description
Pattern Definition	
Pattern	Enter the transformation pattern, including numbers and wildcards (do not use spaces); for example, for NANP, enter 9.@ for typical local access or 8XXX for a typical private network numbering plan. Valid characters include the uppercase characters A, B, C, and D and \+, which represents the international escape character +. **Note** Ensure that the pattern is unique. Check the transformation pattern, route pattern, translation pattern, directory number, call park number, call pickup number, message waiting on/off, or meet me number if you receive an error that indicates duplicate entries. You can also check the route plan report. See topics related to wildcards and special characters in route patterns and hunt pilots in the *Cisco Unified Communications Manager System Guide* for more information about wildcards.
Partition	If you want to use a partition to restrict access to the transformation pattern, choose the desired partition from the drop-down list box. 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, then find and choose a partition name. **Note** Configure transformation patterns in different non-null partitions rather than dialing patterns such as route patterns and directory numbers. For transformation pattern lookups, Cisco Unified Communications Manager ignores the patterns in null partitions. **Note** To set the maximum list box items, choose **System** > **Enterprise Parameters** and choose CCMAdmin Parameters. **Note** Make sure that the combination of pattern, route filter, and partition is unique within the Cisco Unified Communications Manager cluster.
Description	Enter a description of the transformation pattern.
Numbering Plan	Choose a numbering plan.
Route Filter	If your transformation pattern includes the @ wildcard, you may choose a route filter. The optional act of choosing a 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. You can configure the number of items that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more route filters 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 Route Filters window, then find and choose a route filter name. **Note** To set the maximum list box items, choose **System** > **Enterprise Parameters** and choose CCMAdmin Parameters.

Field	Description
Urgent Priority	Cisco Unified Communications Manager sets all calling party transformation patterns with urgent priority, and you cannot change the priority of the patterns.
MLPP Preemption Disabled	Check this check box to make the numbers in a transformation pattern nonpreemptable. **Note** For MLPP Preemption Disabled check box to work, create the transformation patterns 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**).
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. You may also configure an External Phone Number Mask on all phone devices.
Discard Digit Instructions	Choose the discard digit instructions that you want to be associated with this calling party transformation pattern. The discard digits that display depend on the numbering plan that you choose from the Numbering Plan drop-down list box.
Calling Party Transform Mask	Enter a transformation mask value. Valid entries include the digits 0 through 9; the wildcard characters X, asterisk (*), and octothorpe (#); and the international escape character +. If the Discard Digit Instructions field is blank, the Prefix Digits (Outgoing Calls) field is blank, the Calling Party Transformation Mask field is blank, and the Use Calling Party's External Phone Number Mask is not checked, no calling party transformation takes place.
Prefix Digits (Outgoing Calls)	Enter prefix digits in the Prefix Digits (Outgoing Calls) field. 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 route 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.

Field	Description
Calling Party Number Type	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 type numbering plan. Choose one of the following options: • Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the directory number type. • Unknown—Use 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.
Calling Party Numbering Plan	Choose the format for the numbering plan in calling party directory numbers. Cisco Unified Communications Manager sets the calling DN numbering plan. 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 PBXs by using routing as a non-national type number. Choose one of the following options: • Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the Numbering Plan in the directory number. • ISDN—Use when you are dialing outside the dialing plan for your country. • National Standard—Use when you are dialing within the dialing plan for your country. • Private—Use when you are dialing within a private network. • Unknown—Use when the dialing plan is unknown.

Related Topics

About Route Filter Setup , on page 189
Partition Setup , on page 267
Search for Partition , on page 270
Calling Party Transformation Pattern Setup , on page 339



CHAPTER 51

Called Party Transformation Pattern Setup

This chapter provides information to configure a called party transformation pattern.

For additional information, see topics related to called party number transformations settings, wildcards and special characters in route patterns and hunt pilots in the *Cisco Unified Communications Manager System Guide*. Also see topics related to local route groups in the *Cisco Unified Communications Manager Features and Services Guide*.

About Called Party Transformation Pattern Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Transformation Pattern** > **Called Party Transformation Pattern** menu path to configure called party transformation patterns.

The parameters in the Called Party Transformation Patterns window provide appropriate caller information by using the Called Party Transformation calling search space on the destination device. Be aware that calls through transformation patterns are not routable. When this pattern is matched, the call does not route to any device.

Note See topics related to local route groups in the *Cisco Unified Communications Manager Features and Services Guide* for a discussion of called party transformation patterns and their use and configuration when the Local Route Group feature is configured.

Called Party Transformation Pattern Settings

The following table describes the called party transformation pattern settings.

Table 53: Called Party Transformation Pattern Settings

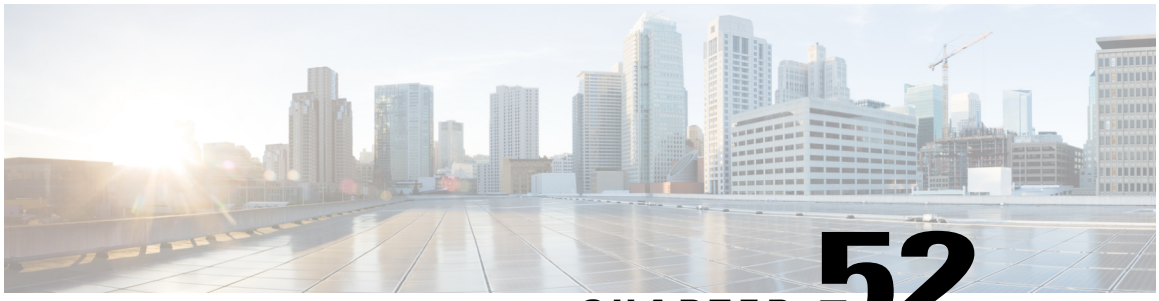
Field	Description
Pattern Definition	
Pattern	Enter the transformation pattern, including numbers and wildcards (do not use spaces); for example, for NANP, enter 9.@ for typical local access, or 8XXX for a typical private network numbering plan. Valid characters include the uppercase letters A, B, C, and D and \+, which represents the international escape character +. **Note** Ensure that the pattern is unique. Check the transformation pattern, route pattern, translation pattern, directory number, call park number, call pickup number, message waiting on/off, or meet me number if you receive an error that indicates duplicate entries. You can also check the route plan report. See topics related to wildcards and special characters in route patterns and hunt pilots in the *Cisco Unified Communications Manager System Guide* for more information about wildcards.
Partition	If you want to use a partition to restrict access to the transformation pattern, choose the desired partition from the drop-down list box. If you do not want to restrict access to the transformation pattern, 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, then find and choose a partition name. **Note** Transformation patterns should be configured in different non- NULL partitions than dialing patterns such as route patterns and directory numbers. For transformation pattern lookups, the patterns in NULL partitions get ignored. **Note** To set the maximum list box items, choose **System** > **Enterprise Parameters** and choose CCMAdmin Parameters. **Note** Make sure that the combination of pattern, route filter, and partition is unique within the Cisco Unified Communications Manager cluster.
Description	Enter a description of the transformation 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.

Field	Description
Route Filter	If your transformation pattern includes the @ wildcard, you may choose a route filter. The optional act of choosing a 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. You can configure the number of items that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more route filters 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 Route Filters window, then find and choose a route filter name. **Note** To set the maximum list box items, choose **System** > **Enterprise Parameters** and choose CCMAdmin Parameters.
Urgent Priority	Cisco Unified Communications Manager sets all called party transformation patterns with urgent priority, and you cannot change the priority of the patterns.
Called Party Transformations	
Discard Digits	Choose the discard digits instructions that you want to be associated with this called party transformation pattern. 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 X, asterisk (*), and octothorpe (#); the international escape character +; and blank. If this field is blank and the preceding field is not checked, no transformation takes place.
Prefix Digits	Enter prefix digits in the Prefix Digits (Outgoing Calls) field. 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 get routed to the assigned device.

Field	Description
Called Party Number Type	Choose the format for the number type in called party directory numbers. Cisco Unified Communications Manager sets the called party 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 called directory number to be encoded to a non national type numbering plan. Choose one of the following options: • Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the directory number type. • Unknown—Use 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.
Called Party Numbering Plan	Choose the format for the numbering plan in called party directory numbers. Cisco Unified Communications Manager sets the called DN numbering plan. 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 PBXs by using routing as a non national type number. Choose one of the following options: • Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the Numbering Plan in the directory number. • ISDN—Use when you are dialing outside the dialing plan for your country. • National Standard—Use when you are dialing within the dialing plan for your country. • Private—Use when you are dialing within a private network. • Unknown—Use when the dialing plan is unknown.

Related Topics

About Route Filter Setup , on page 189
Partition Setup , on page 267
Search for Partition , on page 270
Called Party Transformation Pattern Setup , on page 343



CHAPTER 52

Other Call Routing Menu Options

This chapter provide brief descriptions of selected Call Routing menu options. A pointer to documents that contain a more detailed description for each of these Call Routing menu options is provided.

Intercom Partition Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Intercom** > **Intercom Route Partition** menu path to configure 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*.

For more information about intercom partitions, see the *Cisco Unified Communications Manager System Guide*.

Intercom Calling Search Space Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Intercom** > **Intercom Calling Search Space** menu path to configure intercom calling search spaces.

An intercom calling search space comprises an ordered list of intercom calling search spaces 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*. For more information about intercom and intercom calling search spaces, see the *Cisco Unified Communications Manager System Guide*.

Intercom Directory Number Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Intercom** > **Intercom Directory Number** menu path to configure intercom directory numbers.

Using Cisco Unified Communications Manager Administration, configure and modify intercom directory numbers (DNs) that are assigned to specific phones.

For more information on how to configure intercom directory numbers, see the *Cisco Unified Communications Manager System Guide*.

Intercom Translation Pattern Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Intercom** > **Intercom Translation Pattern** menu path to configure intercom translation patterns.

Cisco Unified Communications Manager uses translation patterns to manipulate dialed digits before it routes a call. In some cases, the system does not use the dialed number. In other cases, the public switched telephone network (PSTN) does not recognize the dialed number.

For more information on how to configure intercom translation patterns, see the *Cisco Unified Communications Manager System Guide*.

Access List Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Class of Control** > **Access List** menu path to configure access lists.

Cisco Unified Mobility allows users to manage business calls using a single phone number and pick up in-progress calls on the desktop phone and cellular phone. Access lists determine the phone numbers that are explicitly allowed or blocked for in-progress call transfers.

For more information about Cisco Unified Mobility and how to configure access lists, see the *Cisco Unified Communications Manager System Guide*.

Client Matter Code Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Client Matter Codes** menu path to configure client matter codes.

Client Matter Codes (CMC) assist with call accounting and billing for billable clients. CMC 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 CMC feature requires that you make changes to route patterns and update your dial plan documents to reflect that you enabled or disabled CMC for each route pattern. You can access the Client Matter Codes search and configuration windows from **Call Routing** > **Client Matter Codes** in Cisco Unified Communications Manager Administration.

For detailed information about client matter codes, see the *Cisco Unified Communications Manager System Guide*.

Additional Cisco Documentation

- *Cisco Unified Communications Manager Bulk Administration Guide*
- *Cisco Unified Serviceability Administration Guide*

Forced Authorization Code Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Forced Authorization Codes** menu path to configure forced authorization codes.

Forced Authorization Codes (FAC) allow you to manage call access and accounting. This feature regulates the types of calls that certain users can place by forcing the user to enter a valid authorization code before the call completes.

The FAC feature requires that you make changes to route patterns and update your dial plan documents to reflect that you enabled or disabled FAC for each route pattern. You can access the Forced Authorization Code search and configuration windows from **Call Routing** > **Forced Authorization Codes** in Cisco Unified Communications Manager Administration.

For detailed information about forced authorization codes, see the *Cisco Unified Communications Manager System Guide*.

Additional Cisco Documentation

- *Cisco Unified Communications Manager Bulk Administration Guide*
- *Cisco Unified Serviceability Administration Guide*

Call Park Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Call Par** menu path to configure call park numbers.

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.

For more information on how to use and configure the Call Park feature, see the *Cisco Unified Communications Manager System Guide*.

Directed Call Park Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Directed Call Park** menu path to configure directed call park numbers.

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.

A user can retrieve a parked call by dialing a configured retrieval prefix followed by the directed call park number where the call is parked.

For more information on how to use and configure the directed call park feature, see the *Cisco Unified Communications Manager System Guide*.

Call Pickup Group Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Call Pickup Group** menu path to configure call pickup groups.

The Call Pickup Group menu option allows administrators to configure call pickup groups. After end users are configured as member s of a call pickup group, these users can answer a call that comes in on a directory number other than their own. When a user hears an incoming call ringing on another phone, the user can redirect the call to their own phone by using one of the call pickup phone features.

Cisco Unified IP Phones that are running SCCP and SIP provide several types of 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 a user activates this feature on a phone.
- 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 they activate this feature on a phone.
- The Other Group Pickup feature allows users to pick up incoming calls in a group that is associated with their own group. When a phone rings in a group that is associated with the user group, Cisco Unified

Communications Manager automatically searches for the incoming call in the associated groups when they activate this feature on a phone.

- The Directed Call Pickup feature allows a user to pick up an incoming call on a directory number (DN) directly by pressing the GPickUp softkey and entering the directory number.
- The Busy Lamp Field (BLF) Call Pickup feature allows a user to pick up a call that is directed to the DN that is associated with the BLF button that is configured on the user Cisco Unified IP Phone.

For more information on how to use and configure the various Call Pickup features and how to configure call pickup groups, see the *Cisco Unified Communications Manager System Guide*.

Transformation Profile Setup

Cisco Intercompany Media Engine configuration comprises configuration of transformation profiles.

For more information, see the *Cisco Intercompany Media Engine Installation and Configuration Guide*.

Mobility Setup

In Cisco Unified Communications Manager Administration, use the following menu paths to configure Cisco Unified Mobility configuration:

- **Call Routing** > **Mobility** > **Enterprise Feature Access Configuration**
- **Call Routing** > **Mobility** > **Handoff Configuration**
  Call Routing > Mobility > Handoff Configuration
- **Call Routing** > **Mobility** > **Mobility Profile**

Cisco Unified Mobility allows users to manage business calls using a single phone number and pick up in-progress calls on the desktop phone and cellular phone. The Mobility Configuration window contains dual mode phone handoff settings for call transfers between a user desktop phone and mobile phone.

The Enterprise Feature Access Configuration window allows you to configure the Enterprise Feature Access (EFA) number for Cisco Unified Mobility calls.

The Handoff Mobility Configuration window allows you to configure the handoff number that the system uses to hand off Cisco Unified Mobility calls.

The Mobility Profile Configuration window allows you to configure mobility profiles for Cisco Unified Mobility users. The mobility profile of a user determines whether user mobility calls use the Dial-via-Office Forward or Dial-via-Office Reverse Callback feature for mobility calls.

For more information on Cisco Unified Mobility and how to configure mobility settings for dual-mode phones, see the *Cisco Unified Communications Manager System Guide*.

Logical Partitioning Policy Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Logical Partitioning Policy Configuration** menu path to configure logical partitioning policies.

You use logical partitioning policies with geographic locations and geographic location filters to provision logical partitioning.

For more information on how to use the Logical Partitioning Policy Configuration window, see the *Cisco Unified Communications Manager System Guide*.

Call Control Discovery Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Call Control Discovery** > **Feature Configuration** menu path to configure call control discovery feature parameters.

External Call Control Profile Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **External Call Control Profile** menu path to configure external call control profiles.

Video QoS Reservation Setup

Note This feature is limited to use in lab environments for demonstration purposes only. Cisco Technical Assistance Center (TAC) does not provide support for this feature.

The Video Quality of Service (QoS) Reservation feature reserves bandwidth in a mobile network, through a third party HTTP service, when a mobile device makes a call. This reservation is only for VoIP calls made through Cisco Unified Communications Manager, not for other voice calls already classified by the mobile network as voice calls.

For each device with its MSISDN configured, Unified Communications Manager requests its connection type. If the connection type for the device is supported, Unified Communications Manager reserves the bandwidth with its MSISDN and the connected IP address. A video call has two reservations, one for the audio portion and one for the video portion, both with the QoS Class Identifier (QCI) value set to 2. An audio call has one reservation, with the QCI value set to 1.

This feature only supports Unified Communications Manager SIP line side devices, such as CSF client (Jabber for Tablet) and Cius.

To enable the Video QoS feature, use the **System** > **Service Parameters** menu path to configure the parameters for the device. In the **Clusterwide Parameters** section, set **External QoS Enabled** to True.

To configure a MSISDN for the device, use the **Device** > **Phone** menu path. Enter the MSISDN in the **Mobile Subscriber ISDN(MSISDN)** field.

HTTP Profile

Use the **Call Routing** > **HTTP Profile** menu path to configure an HTTP profile.

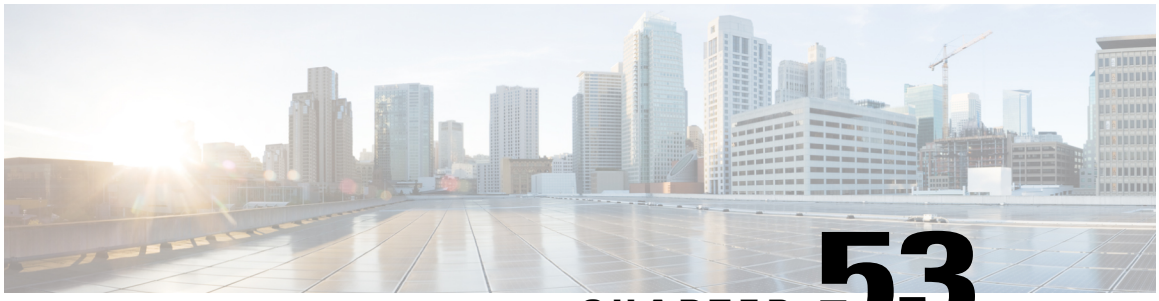
Table 54: HTTP Profile Settings

Field	Description
Name	Enter a name for the HTTP profile.

Field	Description
User Name	Enter a user name.
Password	Enter a password.
Request Timer	Enter an amount for the request timer in milliseconds.
Web Service Root URI	Enter the Web Service Root URI.
QoS Connection Type	Used in conjunction with Web Service Root URI to query the device connection type.
QoS URI	Used in conjunction with Web Service Root URI to reserve bandwidth for the device.

PART IV

Media Resource Setup



CHAPTER 53

Annunciator Setup

This chapter provides information to find and update annunciators. For additional information, see topics related to annunciators and trusted relay points in the *Cisco Unified Communications Manager System Guide*. Also see topics related to multilevel precedence and preemption in the *Cisco Unified Communications Manager Features and Services Guide*.

About Annunciator Setup

In Cisco Unified Communications Manager Administration, use the **Media Resources** > **Annunciator** menu path to configure annunciators.

An annunciator, an SCCP device that uses the Cisco Media Streaming Application service, enables Cisco Unified Communications Manager to play prerecorded announcements (.wav files) and tones to Cisco Unified IP Phones and gateways. The annunciator, which works with Cisco Multilevel Precedence and Preemption (MLPP), enables Cisco Unified Communications Manager to alert callers as to why the call fails. Annunciator can also play tones for some transferred calls and some conferences.

Annunciator Configuration Tips

Verify that you have activated the Cisco IP Voice Media Streaming Application service on the server where you plan to configure the annunciator. For information on activating services, see the Cisco Unified Serviceability Administration Guide.

Tip When you add a Cisco Unified Communications Manager server, the annunciator for the sever automatically gets added to the database. After you activate the Cisco IP Voice Media Streaming Application service, the annunciator device registers with Cisco Unified Communications Manager.

Tip The annunciator provided by the Cisco IP Voice Media Streaming Application service supports both IPv4 and IPv6 audio media connections. The annunciator is configured automatically in dual mode when the platform is configured for IPv6 and the IPv6 enterprise parameter is enabled. The annunciator supports only IPv4 for the TCP control channel. The annunciator supports secure media SRTP connections to both IPv4 and IPv6 addresses.

Before you begin to configure an annunciator, verify that you have completed the following tasks:

- Configured the appropriate servers
- Configured device pools

Related Topics

Synchronize Annunciators , on page 360

Annunciator Deletion

You cannot delete an annunciator if other devices are using it. If you find that any devices are using the annunciator that you want to delete, you must first update those devices to use a different annunciator.

To find which devices are using the annunciator, choose Dependency Records from the Related Links drop-down list menu and click Go. If the dependency records are not enabled for the system, the dependency records summary window displays a message.

Related Topics

Access Dependency Records , on page 982

Annunciator Settings

The following table describes the annunciator settings.

Table 55: Annunciator Settings

Field	Description
Server	The system automatically displays the preconfigured server (servers get added at installation).
Name	This field designates the name that is used when the device registers with the Cisco Unified Communications Manager. Enter a name of up to 15 alphanumeric characters (you can use periods, dashes, and underscores).
Description	Enter a description of up to 128 alphanumeric characters (you can use periods, dashes, and underscores). Default uses the server name, which includes the prefix ANN_.
Device Pool	Choose Default or choose a device pool from the drop-down list of configured device pools.

Field	Description
Location	Use locations to implement call admission control (CAC) in a centralized call-processing system. CAC allows you to regulate audio quality and video availability by limiting the 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 box, choose the appropriate location for this annunciator. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this annunciator consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the **System** > **Location** menu option. For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*.
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified Communications Manager inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values: • Off—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. Cisco Unified Communications Manager places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVPAgent). If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. For details of call behavior, see *Cisco Unified Communications Manager System Guide*. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified Communications Manager first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified Communications Manager first tries to find a transcoder that is also designated as a TRP. See the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.

Related Topics

Location Setup , on page 127
Annunciator Setup , on page 357

Synchronize Annunciators

To synchronize an annunciator with the most recent configuration changes, perform the following procedure, which applies 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** > **Annunciator**.
The Find and List Annunciators window displays.

Step 2 Choose the search criteria to use.

Step 3 Click Find.
The window displays a list of annunciators that match the search criteria.

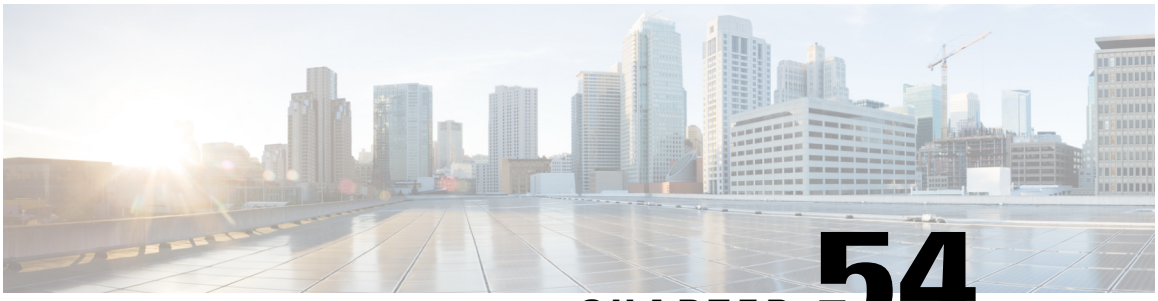
Step 4 Check the check boxes next to the annunciators that you want to synchronize. To choose all annunciators in the window, check the check box in the matching records title bar.

Step 5 Click Apply Config to Selected.
The Apply Configuration Information dialog displays.

Step 6 Click OK.

Related Topics

Annunciator Setup , on page 357



CHAPTER 54

Conference Bridge Setup

This chapter provides information to configure conference bridges using Cisco Unified Communications Manager Administration.

See the following for additional information:

- Conference bridges and trusted relay points in the *Cisco Unified Communications Manager System Guide*
- Configuring Secure Conference Bridge in Cisco Unified Communications Manager Administration, *Cisco Unified Communications Manager Features and Services Guide*.
- Configuring Secure Conference Bridge in Cisco Unified Communications Manager Administration, *Cisco Unified Communications Manager Security Guide*
- *Cisco Unified Videoconferencing 3511 MCU and Cisco Unified Videoconferencing 3540 MCU Module Administrator Guide*
- *Cisco Unified Serviceability Administration Guide*

About Conference Bridge Setup

In Cisco Unified Communications Manager Administration, use the **Media Resources** > **Conference Bridge** menu path to configure conference bridges.

Conference Bridge Configuration Tips

Make sure that the following prerequisites are met before you proceed with configuration of a conference bridge:

- Configure the device pools.

Note Software conference bridges automatically get created when the Cisco Unified Communications Manager server gets created. You cannot add software conference bridges to Cisco Unified Communications Manager Administration.

- For software conference bridges, activate the Cisco IP Voice Media Streaming Application service. See the *Cisco Unified Serviceability Administration Guide*.

The software conference bridge provided by the Cisco IP Voice Media Streaming Application service supports both IPv4 and IPv6 audio media connections. The software conference bridge is configured automatically in dual mode when the platform is configured for IPv6 and the IPv6 enterprise parameter is enabled. The software conference bridge supports only IPv4 for the TCP control channel.

Related Topics

Device Pool Deletion , on page 80
Software Conference Bridge Settings, on page 363
Synchronize Conference Device Settings , on page 385

Conference Bridge Deletion

Keep in mind that you cannot delete Cisco Unified Communications Manager Conference Bridge Software.

Cisco Unified Communications Manager allows you to delete devices that may be associated with components such as media resource groups. To find out what dependencies the conference device may have, choose the Dependency Records link from the drop-down list box and click Go from the Conference Bridge Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message.

Related Topics

Conference Bridge Setup , on page 361
Access Dependency Records , on page 982

Conference Bridge Settings

Consult the conference bridge configuration settings table that corresponds to the type of conference bridge that you are configuring.

Related Topics

Conference Bridge Setup , on page 361
Software Conference Bridge Settings, on page 363
Hardware Conference Bridge Settings , on page 365
Cisco IOS Conference Bridge Settings , on page 367
Cisco Video Conference Bridge Settings , on page 369
Cisco Conference Bridge (WS-SVC-CMM) Settings , on page 372
Cisco IOS Heterogeneous Video Conference Bridge Settings , on page 374

Cisco IOS Guaranteed Audio Video Conference Bridge Settings , on page 376
Cisco IOS Homogeneous Video Conference Bridge Settings , on page 378
Cisco TelePresence MCU Settings

Software Conference Bridge Settings

Conference Bridge for Cisco Unified Communications Manager, a software or hardware application, allows both ad hoc and meet-me voice conferencing. Each conference bridge can host several simultaneous, multiparty conferences.

Be aware that both hardware and software conference bridges can be active at the same time. Software and hardware conference devices differ in the number of streams and the types of codec that they support.

You cannot add software conference bridges to Cisco Unified Communications Manager by using Conference Bridge Configuration. Software conference bridges automatically get added when a Cisco Unified Communications Manager server gets added. After a Cisco Unified Communications Manager server gets added, the software conference bridge gets displayed in the Find/List Conference Bridges window (by default, the first software conference bridge gets configured during Cisco Unified Communications Manager installation) when you perform a search. You can update software conference bridges, but you cannot delete them.

See the *Cisco Unified Communications Manager System Guide* for more information about conference bridges.

The following table describes the software conference bridge configuration settings.

Table 56: Software Conference Bridge Configuration Settings

Field	Description
Conference Bridge Type	This field automatically displays Cisco Conference Bridge Software.
Host Server	This field automatically displays the Cisco Unified Communications Manager server for this software conference bridge.
Conference Bridge Name	This field automatically displays the software conference bridge name. The format of the name specifies CFB_ followed by a digit that represents the value of the software conference bridge; for example, CFB_3 represents the third conference bridge in the Cisco Unified Communications Manager system.
Description	This field automatically displays a description, but the administrator can update this field.
Device Pool	Choose a device pool that has the highest priority within the Cisco Unified Communications Manager group that you are using or choose Default.
Common Device Configuration	Choose the common device configuration to assign to the conference bridge. The common device configuration includes attributes, such as MOH audio source, that support features and services for phone users. Device configurations that are configured in the Common Device Configuration window display in the drop-down list.

Field	Description
Location	Use locations to implement call admission control (CAC) in a centralized call-processing system. CAC enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location. From the drop-down list box, choose the appropriate location for this conference bridge. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this conference bridge consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the **System** > **Location** menu option. For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*.
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values: • Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates. • Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified CM 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 topics related to TRP insertion in Cisco Unified Communications Manager in the *Cisco Unified Communications Manager System Guide* for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified CM first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified CM first tries to find a transcoder that is also designated as a TRP. See topics related to trusted relay points and media resource management in the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.

Related Topics

About Server Setup , on page 27
Location Setup , on page 127
Conference Bridge Setup , on page 361
Common Device Setup , on page 763

Hardware Conference Bridge Settings

Conference Bridge for Cisco Unified Communications Manager, a software or hardware application, allows both ad hoc and meet-me voice conferencing. Each conference bridge can host several simultaneous, multiparty conferences.

Be aware that both hardware and software conference bridges can be active at the same time. Software and hardware conference devices differ in the number of streams and the types of codec that they support.

Note The hardware model type for Conference Bridge contains a specific Media Access Control (MAC) address and device pool information.

See the *Cisco Unified Communications Manager System Guide* for more information about conference bridges.

The following table describes the hardware conference bridge configuration settings.

Table 57: Hardware Conference Bridge Configuration Settings

Field	Description
Conference Bridge Type	Choose Cisco Conference Bridge Hardware. For a description of this type, see the *Cisco Unified Communications Manager System Guide*.
MAC Address	Enter a unique device MAC address in this required field. MAC addresses comprise 12 hexadecimal digits (0-9, A-F). Example 1231123245AB
Description	This field automatically generates from the MAC address that you provide. You can update this field if you choose.
Device Pool	Choose a device pool that has the highest priority within the Cisco Unified Communications Manager group that you are using or choose Default.
Common Device Configuration	Choose the common device configuration to assign to the conference bridge. The common device configuration includes attributes, such as MOH audio source, that support features and services for phone users. Device configurations that are configured in the Common Device Configuration window display in the drop-down list.

Field	Description
Location	Use locations to implement call admission control (CAC) in a centralized call-processing system. CAC enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location. From the drop-down list box, choose the appropriate location for this conference bridge. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this conference bridge consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the **System** > **Location** menu option. For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*.
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values: • Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates. • Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified CM 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 *Cisco Unified Communications Manager System Guide* for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified CM first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified CM first tries to find a transcoder that is also designated as a TRP. See the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.
Special Load Information	Enter any special load information or leave blank to use default.

Related Topics

Location Setup , on page 127
Common Device Setup , on page 763

Cisco IOS Conference Bridge Settings

Conference Bridge for Cisco Unified Communications Manager, a software or hardware application, allows both ad hoc and meet-me voice conferencing. Each conference bridge can host several simultaneous, multiparty conferences.

Be aware that both hardware and software conference bridges can be active at the same time. Software and hardware conference devices differ in the number of streams and the types of codec that they support.

See the *Cisco Unified Communications Manager System Guide* for more information about conference bridges.

The following table describes the Cisco IOS conference bridge configuration settings.

Table 58: Cisco IOS Conference Bridge Configuration Settings

Field	Description
Conference Bridge Type	Choose Cisco IOS Conference Bridge or Cisco IOS Enhanced Conference Bridge. For a description of these types, see the *Cisco Unified Communications Manager System Guide*.
Conference Bridge Name	Enter the same name that exists in the gateway Command Line Interface (CLI). You can enter up to 15 characters. Valid characters comprise alphanumeric characters (a-z, A-Z, 0-9), as well as dot (.), dash (-),and underscore (_).
Description	This field automatically generates from the conference bridge name that you provide. You can update this field if you choose.
Device Pool	Choose a device pool or choose Default.
Common Device Configuration	Choose the common device configuration to assign to the conference bridge. The common device configuration includes attributes, such as MOH audio source, that support features and services for phone users. Device configurations that are configured in the Common Device Configuration window display in the drop-down list.

Field	Description
Location	Use locations to implement call admission control (CAC) in a centralized call-processing system. CAC enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location. From the drop-down list box, choose the appropriate location for this conference bridge. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this conference bridge consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the **System** > **Location** menu option. For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*.
Device Security Mode	This field displays for Cisco IOS Enhanced Conference Bridge only. If you choose Non Secure Conference Bridge, the nonsecure conference establishes a TCP port connection to Cisco Unified Communications Manager on port 2000. **Tip** Ensure this setting matches the security setting on the conference bridge, or the call will fail. The Encrypted Conference Bridge setting supports the secure conference feature. See the *Cisco Unified Communications Manager System Guide* for secure conference bridge configuration procedures.

Field	Description
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values: • Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates. • Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified CM 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 *Cisco Unified Communications Manager System Guide* for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified CM first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified CM first tries to find a transcoder that is also designated as a TRP. See the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.

Related Topics

Location Setup , on page 127
Conference Bridge Setup , on page 361
Common Device Setup , on page 763

Cisco Video Conference Bridge Settings

Conference Bridge for Cisco Unified Communications Manager, a software or hardware application, allows both ad hoc and meet-me voice conferencing. Each conference bridge can host several simultaneous, multiparty conferences.

Be aware that both hardware and software conference bridges can be active at the same time. Software and hardware conference devices differ in the number of streams and the types of codec that they support.

See the *Cisco Unified Communications Manager System Guide* for more information about conference bridges.

The following table describes the Cisco video conference bridge configuration settings.

Table 59: Cisco Video Conference Bridge Configuration Settings

Field	Description
Conference Bridge Type	Choose Cisco Video Conference Bridge (IPVC-35xx). For a description of this type, see the *Cisco Unified Communications Manager System Guide*.
MAC Address	Enter a unique device MAC address in this required field. MAC addresses comprise 12 hexadecimal digits (0-9, A-F). Example 1231123245AB
Description	This field automatically generates from the conference bridge name that you provide. You can update this field if you choose.
Device Pool	Choose a device pool or choose Default.
Common Device Configuration	Choose the common device configuration to assign to the conference bridge. The common device configuration includes attributes, such as MOH audio source, that support features and services for phone users. Device configurations that are configured in the Common Device Configuration window display in the drop-down list.
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 box, choose the appropriate location for this conference bridge. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this conference bridge consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the **System** > **Location** menu option. For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*.

Field	Description
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values: • Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates. • Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified CM 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 *Cisco Unified Communications Manager System Guide* for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified CM first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified CM first tries to find a transcoder that is also designated as a TRP. See the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.
Product-Specific Configuration	
Model-specific configuration fields that the device manufacturer defines	The device manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the "?" information icon under the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, see the documentation for the specific device that you are configuring or contact the manufacturer.

Related Topics

Location Setup , on page 127
Conference Bridge Setup , on page 361
Common Device Setup , on page 763

Cisco Conference Bridge (WS-SVC-CMM) Settings

Conference Bridge for Cisco Unified Communications Manager, a software or hardware application, allows both ad hoc and meet-me voice conferencing. Each conference bridge can host several simultaneous, multiparty conferences.

Be aware that both hardware and software conference bridges can be active at the same time. Software and hardware conference devices differ in the number of streams and the types of codec that they support.

See the *Cisco Unified Communications Manager System Guide* for more information about conference bridges.

The following table describes the Cisco Conference Bridge (WS-SVC-CMM) configuration settings.

Table 60: Cisco Conference Bridge (WS-SVC-CMM) Configuration Settings

Field	Description
Conference Bridge Type	Choose Cisco Conference Bridge (WS-SVC-CMM). For a description of this type, see the *Cisco Unified Communications Manager System Guide*.
Description	Enter a description (up to 50 characters) or leave blank to generate automatically from the MAC address that you provide. Invalid characters comprise quotes (“), angle brackets (<>), backslash (), ampersand,(&), and percent sign (%).
MAC Address	Enter a unique device MAC address in this required field. MAC addresses comprise 12 hexadecimal digits (0-9, A-F). Example 1231123245AB
Subunit	From the drop-down list box, choose the value for the daughter card for a given slot on the Communication Media Module card.
Device Pool	Choose a device pool or choose Default.
Common Device Configuration	Choose the common device configuration to assign to the conference bridge. The common device configuration includes attributes, such as MOH audio source, that support features and services for phone users. Device configurations that are configured in the Common Device Configuration window display in the drop-down list.

Field	Description
Location	Use locations to implement call admission control (CAC) in a centralized call-processing system. CAC enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location. From the drop-down list box, choose the appropriate location for this conference bridge. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this conference bridge consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the **System** > **Location** menu option. For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*.
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values: • Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates. • Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified CM 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 *Cisco Unified Communications Manager System Guide* for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified CM first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified CM first tries to find a transcoder that is also designated as a TRP. See the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.
Maximum Capacity	Choose the maximum number of streams for a given service on a daughter card. Possible values include 32, 64, 96, and 128 streams. Ensure that each daughter card has as many ports as the value that you choose.
Product-Specific Configuration	

Field	Description
Model-specific configuration fields that the device manufacturer defines	To view field descriptions and help for product-specific configuration items, click the "?" information icon under the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, see the documentation for the specific device that you are configuring or contact the manufacturer.

Related Topics

Location Setup , on page 127
Conference Bridge Setup , on page 361
Common Device Setup , on page 763

Cisco IOS Heterogeneous Video Conference Bridge Settings

Cisco Integrated Services Routers Generation 2 (ISR G2) can act as IOS-based conference bridges that support ad hoc and meet-me video conferencing. DSP modules must be installed on the router to enable the router as a conference bridge.

Cisco IOS Heterogeneous Video Conference Bridge specifies the IOS-based conference bridge type that supports heterogeneous video conferences. In a heterogeneous video conference, all the conference participants connect to the conference bridge with phones that use different video format attributes. In heterogeneous conferences, transcoding and transsizing features are required from the DSP to convert the signal between the various formats.

For heterogeneous video conferences, callers connect to the conference as audio participants under either of the following conditions:

- Insufficient DSP resources.
- The conference bridge is not configured to support the video capabilities of the phone.

See the *Cisco Unified Communications Manager System Guide* for more information about conference bridges.

The following table describes the Cisco IOS Heterogeneous Video Conference Bridge configuration settings.

Table 61: Cisco IOS Heterogeneous Video Conference Bridge Settings

Field	Description
Conference Bridge Name	Enter a name for your conference bridge.
Description	Enter a description for your conference bridge
Device Pool	Choose a device pool or choose Default.

Field	Description
Common Device Configuration	Choose the common device configuration to assign to the conference bridge. The common device configuration includes attributes, such as MOH audio source, that support features and services for phone users. Device configurations that are configured in the Common Device Configuration window display in the drop-down list.
Location	Use location 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 box, choose the appropriate location for this conference bridge. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this conference bridge consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the **System** > **Location** menu option. For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*.
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. • Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates. • Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified CM 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 *Cisco Unified Communications Manager System Guide* for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified CM first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified CM first tries to find a transcoder that is also designated as a TRP. See the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.

Related Topics

Location Setup , on page 127
Conference Bridge Setup , on page 361
Common Device Setup , on page 763

Cisco IOS Guaranteed Audio Video Conference Bridge Settings

Cisco Integrated Services Routers Generation 2 (ISR G2) can act as IOS-based conference bridges that support ad hoc and meet-me voice and video conferencing. DSP modules must be installed on the router to enable the router as a conference bridge.

Cisco IOS Guaranteed Audio Video Conference Bridge specifies the IOS-based video conference bridge type where DSP resources are reserved for the audio portion of the conference, and video service is not guaranteed. Callers on video phones may have video service if DSP resources are available at the start of the conference. Otherwise, the callers connect to the conference as audio participants.

See the *Cisco Unified Communications Manager System Guide* for more information about conference bridges.

The following table describes the Cisco IOS Heterogeneous Video Conference Bridge configuration settings.

Table 62: Cisco IOS Guaranteed Audio Video Conference Bridge Settings

Field	Description
Conference Bridge Name	Enter a name for your conference bridge
Description	Enter a description for your conference bridge
Device Pool	Choose a device pool or choose Default.
Common Device Configuration	Choose the common device configuration to assign to the conference bridge. The common device configuration includes attributes, such as MOH audio source, that support features and services for phone users. Device configurations that are configured in the Common Device Configuration window display in the drop-down list.

Field	Description
Location	Use location 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 box, choose the appropriate location for this conference bridge. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this conference bridge consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the **System** > **Location** menu option. For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*.
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. • Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates. • Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified CM 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 *Cisco Unified Communications Manager System Guide* for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified CM first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified CM first tries to find a transcoder that is also designated as a TRP. See the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.

Related Topics

Location Setup , on page 127
Conference Bridge Setup , on page 361

Common Device Setup , on page 763

Cisco IOS Homogeneous Video Conference Bridge Settings

Cisco Integrated Services Routers Generation 2 (ISR G2) can act as IOS-based conference bridges that support ad hoc and meet-me video conferencing. DSP modules must be installed on the router to enable the router as a conference bridge.

Cisco IOS Homogeneous Video Conference Bridge specifies the IOS-based conference bridge type that supports homogeneous video conferences. A homogeneous video conference is a video conference in which all participants connect using the same video format attributes. All the video phones support the same video format and the conference bridge sends the same data stream format to all the video participants.

If the conference bridge is not configured to support the video format of a phone, the caller on that phone connects to the conference as an audio only participant.

See the *Cisco Unified Communications Manager System Guide* for more information about conference bridges.

The following table describes the Cisco IOS Homogeneous Video Conference Bridge configuration settings.

Table 63: Cisco IOS Homogeneous Video Conference Bridge Settings

Field	Description
Conference Bridge Name	Enter a name for your conference bridge.
Description	Enter a description for your conference bridge
Device Pool	Choose a device pool or choose Default.
Common Device Configuration	Choose the common device configuration to assign to the conference bridge. The common device configuration includes attributes, such as MOH audio source, that support features and services for phone users. Device configurations that are configured in the Common Device Configuration window display in the drop-down list.
Location	Use location 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 box, choose the appropriate location for this conference bridge. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this conference bridge consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the **System** > **Location** menu option. For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*.

Field	Description
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. • Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates. • Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified CM 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 *Cisco Unified Communications Manager System Guide* for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified CM first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified CM first tries to find a transcoder that is also designated as a TRP. See the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.

Related Topics

Location Setup , on page 127
Conference Bridge Setup , on page 361
Common Device Setup , on page 763

Cisco TelePresence MCU Settings

Cisco TelePresence MCU refers to a set of hardware conference bridges for Cisco Unified Communications Manager.

The Cisco TelePresence MCU is a high-definition (HD) multipoint video conferencing bridge. It delivers up to 1080p at 30 frames per second, full continuous presence for all conferences, full trans-coding, and is ideal for mixed HD endpoint environments.

The Cisco TelePresence MCU supports SIP as the signaling call control protocol. It has a built in Web Server that allows for complete configuration, control and monitoring of the system and conferences. The Cisco TelePresence MCU provides XML management API over HTTP.

Cisco TelePresence MCU allows both ad hoc and meet-me voice and video conferencing. Each conference bridge can host several simultaneous, multiparty conferences.

See the *Cisco Unified Communications Manager System Guide* for more information about conference bridges.

Field	Description
Conference Bridge Name	Enter a name for your conference bridge
Description	Enter a description for your conference bridge
Username	Enter the Cisco TelePresence MCU administrator username.
Password	Enter the Cisco TelePresence MCU administrator password.
Confirm Password	Enter the Cisco TelePresence MCU administrator password.
Use HTTPS	Check this check box if you want to create a secure HTTPS connection between Cisco Unified Communications Manager and Cisco TelePresence MCU. The default HTTPS port is 443. For information on how to create a TLS connection between Cisco Unified Communications Manager and Cisco TelePresence MCU, see topics related to setting up a TLS connection with Cisco TelePresence MCU.
HTTP Port	Enter the Cisco TelePresence MCU HTTP port. The default port is 80.

Note The HTTP configuration must match what is configured on the Cisco TelePresence MCU. This information allows Cisco Unified Communications Manager to invoke the remote management API on the Cisco TelePresence MCU.

Cisco TelePresence Conductor Settings

Cisco TelePresence Conductor provides intelligent conference administrative controls and is scalable, supporting device clustering for load balancing across MCUs and multiple device availability. Administrators can implement the Cisco TelePresence Conductor as either an appliance or a virtualized application on VMware with support for Cisco Unified Computing System (Cisco UCS) platforms or third-party-based platforms. Multiway conferencing, that allows for dynamic two-way to three-way conferencing, is also supported.

Cisco TelePresence Conductor supports both ad hoc and meet-me voice and video conferencing. Cisco TelePresence Conductor dynamically selects the most appropriate Cisco TelePresence resource for each new conference. Ad hoc, “MeetMe” and scheduled voice and video conferences can dynamically grow and exceed the capacity of individual MCUs. One Cisco TelePresence Conductor appliance or Cisco TelePresence

Conductor cluster has a system capacity of 30 MCUs or 2400 MCU ports. Up to three Cisco TelePresence Conductor appliances or virtualized applications may be clustered to provide greater resilience.

Cisco TelePresence Conductor also provides the XML management API over HTTP, and has a built-in Web Server for complete configuration, control and monitoring of the system and conferences. For more information, see the *Cisco TelePresence Conductor Administrator Guide* and the *Cisco Unified Communications Manager System Guide*.

Note If you are using encryption with Cisco TelePresence Conductor, select cisco-telepresence-conductor-interop as the default normalization script.

The following table describes the Cisco TelePresence Conductor configuration settings.

Table 64: Cisco TelePresence Conductor Configuration Settings

Field	Description
Conference Bridge Name	Enter a name for your conference bridge.
Description	Enter a description for your conference bridge.
Conference Bridge Prefix	The Conference Bridge Prefix is used only for centralized deployments when the conference resources are deployed across a Small Medium Enterprise (SME) and the HTTP and SIP signaling are intended for different destinations. Do not set this parameter unless your video conference device supports this function. See the documentation that came with your conference bridge device for details.
SIP Trunk	Select a SIP trunk to use for this conference bridge from a list of existing SIP trunks.
HTTP Interface Info	
Override SIP Trunk Destination	Check this check box to override the SIP trunk destination. Use this feature if the HTTP and SIP signaling are intended for different destination IP addresses, for example, when the device is used in a centralized deployment. Click the "+" and "-" buttons to add or remove IP addresses and hostnames. Do not set this parameter unless your video conference device supports this function. See the documentation that came with your conference bridge device for details.
Hostname/IP Address	Enter one or more hostnames or IP addresses for the HTTP signaling destination if you have selected to override the SIP trunk destination.
Username	Enter the Cisco TelePresence Conductor administrator username.
Password	Enter the Cisco TelePresence Conductor administrator password.
Confirm Password	Enter the Cisco TelePresence Conductor administrator password

Field	Description
Use HTTPS	Check this check box if you want to create a secure HTTPS connection between Cisco Unified Communications Manager and Cisco TelePresence Conductor. The default HTTPS port is 443.
HTTP Port	Enter the Cisco TelePresence Conductor HTTP port. The default port is 80.

CSCub65671 Route Class Configuration SIP Information

If the route pattern points to a SIP trunk supporting G.Clear, then specify Data or Hotline as the Route Class.

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.

Set Up TLS and HTTPS Connection with Cisco TelePresence MCU

If you are using SRTP with Cisco TelePresence MCU, you must set up a TLS and HTTPS connection with Cisco TelePresence MCU so that you do not expose keys and other security-related information during call negotiations.

Note This procedure details tasks that are performed in Cisco Unified Communications Manager. For detailed instructions on how to import and export certificates in Cisco TelePresence MCU, see your Cisco TelePresence MCU product documentation.

Note For HTTPS, the IP address of MCU should be configured as Alternate Name in the MCU certificate, because Unified Communications Manager allows only an IP address to be configured for MCU on the conference bridge window.

Procedure

Step 1 Download the Cisco Unified Communications Manager security certificate by performing the following steps:

a) In Cisco Unified Operating System Administration, choose **Security** > **Certificate Management.**
b) Click **Find**.
c) Click **CallManager.pem** to view the certificate.
d) Click **Download** and save the file to a local drive.

Step 2 Upload the Cisco Unified Communications Manager certificate to Cisco TelePresence MCU.

Step 3 Generate self-signed certificates for Cisco TelePresence MCU and save the certificates to a local drive.

Step 4 Upload self-signed certificates to the Cisco TelePresence MCU.

Step 5 Upload Cisco TelePresence MCU certificates to Cisco Unified Communications Manager by doing the following:

a) In Cisco Unified Operating System Administration, choose **Security** > **Certificate Management**.
b) Click **Upload Certificate/Certificate Chain**.
c) From the Certificate Name drop-down list box, choose **CallManager-trust**.
d) Click **Browse** and locate the Cisco TelePresence MCU certificate that you saved locally.
e) Click **Upload File** to upload certificates.

Step 6 In Cisco Unified Communications Manager Administration, choose **System** > **Security** > **SIP Trunk Security Profile** and create a secure SIP Trunk Security Profile that uses the following settings:

- Device Security Mode must be Encrypted
- Incoming Transport Type and Outgoing Transport Type must be TLS
- X.509 Subject Name must be set to the defined Common Name that is used in the Cisco TelePresence MCU certificates

Step 7 On the Cisco TelePresence MCU, configure SIP signaling encryption with TLS, and media encryption with SRTP.

Related Topics

Certificates
SIP trunk security profile setup

Video conference resource setup

SIP Trunk Setup for Video Conference Bridge Devices

The following video conference bridge devices use SIP trunks for video conferences on Cisco Unified Communications Manager clusters:

- Cisco TelePresence MCU
- Cisco TelePresence Conductor

Set the following SIP trunk parameters for use with SIP video conference bridge devices. Use the default setting for all other SIP trunk parameters.

- Device Name
- Description
- Device Pool
- Location
- Destination Address
- Destination Port

Note Multiple IP addresses and ports can be specified.

- SIP Trunk Security Profile: You must select TelePresence Conference as the SIP trunk security profile.
- SIP Profile

Note For improved performance, use the default standard SIP profile for TelePresence conferencing that has the Options ping configured.

- Assign the encryption interworking script to SIP trunks that are used for Cisco TelePresence Conductor if encryption is used.

See topics related to setting up trunks for more details about SIP trunk configuration.

Limitations

- Media Termination Point (MTP) Required: Cisco Unified Communications Manager ignores this configuration for all ad hoc conference calls even if this is selected on the SIP trunk.
- Early Offer Support for Voice and Video calls: Cisco Unified Communications Manager ignores this configuration for all ad hoc conference calls even if this is selected on the SIP profile that is associated with the SIP trunk that is linked to the conferencing resource server.
- SIP Rel1xx Option: Cisco Unified Communications Manager ignores this configuration for ad hoc conference calls even if this is enabled on the SIP profile associated with the SIP trunk that is linked to the conferencing resource server.
- RSVP over SIP: Cisco Unified Communications Manager ignores this configuration for all ad hoc conference calls if this is enabled for E2E. If this is configured for local RSVP, the configuration will be effective.

Set Up TelePresence Video Conference Bridge

Use Cisco Unified Communications Manager Administration to add and configure a video conference bridge device. Each video conference bridge device must be assigned to a SIP trunk when you configure the video conference device for the node.

Before You Begin

Set up a SIP trunk before you proceed. See topics related to trunk setup and SIP trunk setup for video conference bridge devices for details.

Procedure

Step 1 Select **Media Resources** > **Conference Bridge**.
The **Find and List Conference Bridges** window displays.

Step 2 Click **Add New**. The **Conference Bridge Configuration** window displays.

Step 3 Select the type of SIP video conference bridge device from the **Conference Bridge Type** drop-down list.

Step 4 Enter a name and description for the video conference bridge device in the **Device Information** pane.

Note For field descriptions, see topics related to configuration settings for the selected video conference bridge type.

Step 5 Select a SIP trunk from the **SIP Trunk** drop-down list.

Step 6 Enter the following mandatory information HTTP interface username, password, and confirm the password in the **HTTP Interface Info** pane.

- Username
- Password
- Confirm Password
- HTTP Port

Step 7 (Optional) Check the **Use HTTPS** check box.

Step 8 Click **Save**.

Synchronize Conference Device Settings

To synchronize a conference device with the most recent configuration changes, perform the following procedure, which applies 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** > **Conference Bridge**.
The Find and List Conference Bridges window displays.

Step 2 Choose the search criteria to use.

Step 3 Click Find.
The window displays a list of conference bridges that match the search criteria.

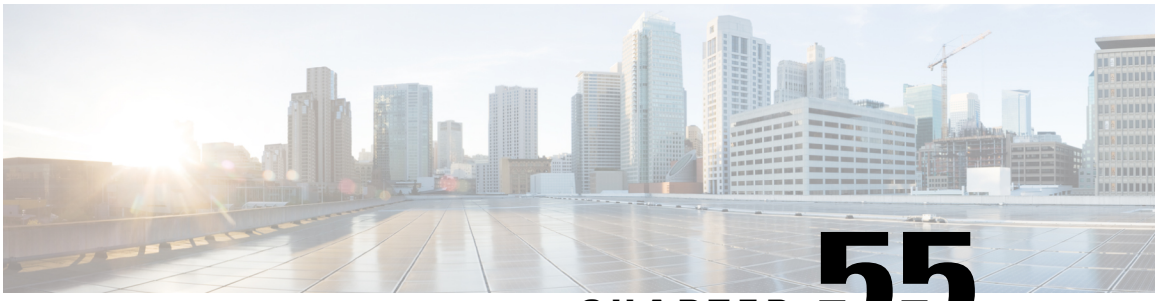
Step 4 Check the check boxes next to the conference bridges that you want to synchronize. To choose all conference bridges in the window, check the check box in the matching records title bar.

Step 5 Click Apply Config to Selected.
The Apply Configuration Information dialog displays.

Step 6 Click OK.

Related Topics

Conference Bridge Setup , on page 361



CHAPTER 55

Media Termination Point Setup

This chapter provides information to add, update, and delete media termination points.

For additional information, see topics related to the following in the *Cisco Unified Communications Manager System Guide*:

- Transcoders
- Media Termination Points
- Resource Reservation Protocol
- Media Resource Management

About Media Termination Point Setup

A Media Termination Point software device allows Cisco Unified Communications Manager to relay calls that are routed through SIP or H.323 endpoints or gateways. You can allocate a media termination point device because of DTMF or RSVP requirements. When a media termination point is allocated for RSVP, you can insert it between any type of endpoint device, including SIP or H.323 devices.

Media termination point, a Cisco software application, installs on a server during the software installation process. You must activate and start the Cisco IP Voice Media Streaming Application service on the server on which you configure the media termination point device. For information on activating and starting services, see the *Cisco Unified Serviceability Administration Guide*.

The Media Termination Point (MTP) device provided by the Cisco IP Voice Media Streaming Application service supports both IPv4 and IPv6 audio media connections. The MTP device is configured automatically in dual mode when the platform is configured for IPv6 and the IPv6 enterprise parameter is enabled. The MTP device supports only IPv4 for the TCP control channel.

Each media termination point device that is defined in the database registers with the Media Resource Manager (MRM). The MRM keeps track of the total available media termination point devices in the system and of which devices have available resources.

During resource reservation, the MRM determines the number of resources and identifies the media resource type (in this case, the media termination point) and the location of the registered media termination point device. The MRM updates its share resource table with the registration information and propagates the registered information to the other Cisco Unified Communications Managers within the cluster.

The media termination point and transcoder can register with the same Cisco Unified Communications Manager.

Each media termination point receives a list of Cisco Unified Communications Managers, in priority order, to which it should attempt to register. Each media termination point can register with only one Cisco Unified Communications Manager at a time.

Note Depending on the capabilities of the SIP endpoint, Cisco Unified Communications Manager may require an RFC 2833 DTMF-compliant media termination point device to make SIP calls. For RSVP calls, the Media Resource Group List (MRGL) that is associated with the endpoint device needs to include the media termination point devices that support RSVP.

Related Topics

Transcoder Setup , on page 391

Cisco IOS Media Termination Point Setup

In Cisco Unified Communications Manager Administration, use the **Media Resources** > **Media Termination Point** menu path to configure media termination points (MTPs).

Media Termination Point Configuration Tips

Make sure that the following prerequisites are met before you proceed with configuration of a media termination point:

- Ensure servers are configured.
- Ensure device pools are configured.

Note You can have only one Media Termination Point device for each Cisco Unified Communications Manager server. When a Cisco Unified Communications Manager Server is added, a media termination point device automatically gets created for the server but is not available for use until the Cisco IP Voice Media Streaming App service gets activated.

Cisco IOS Media Termination Point Deletion

Before deleting a media termination point that is currently in use and is the last device in the Media Resource Group, you should perform either or both of the following tasks:

- Assign a different media termination point to the media resource groups that are using the media termination point that you want to delete.
- Delete the media resource groups that are using the media termination point that you want to delete.

Related Topics

About Media Resource Group Setup , on page 395
Media Resource Group Deletion , on page 396

Cisco IOS Media Termination Point Settings

The following table describes Cisco IOS media termination point settings.

Table 65: Cisco IOS Media Termination Point Settings

Field	Description
Media Termination Point Type	Choose Cisco IOS Enhanced Software Media Termination Point. For specific information on this media termination point type, see the *Cisco Unified Communications Manager System Guide*.
Media Termination Point Name	Enter a name for the media termination point, up to 15 alphanumeric characters. **Note** You cannot use special characters as the MTP name; for example !, @, #, $, or %. **Tip** Ensure that you enter the same media termination point name that exists in the gateway Command Line Interface (CLI).
Description	Enter any description for the media termination point.
Device Pool	Choose a device pool that has the highest priority within the Cisco Unified Communications Manager group that you are using or choose Default.
Trusted Relay Point	Check this check box to designate this media termination point (MTP) as a trusted relay point (TRP) that Cisco Unified Communications Manager can use in a network virtualization environment. See the *Cisco Unified Communications Manager System Guide* for a discussion of trusted relay points.

Related Topics

Media Termination Point Setup , on page 387

Synchronize Media Termination Point

To synchronize a Media Termination Point with the most recent configuration changes, perform the following procedure, which applies 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** > **Media Termination Point**.
The Find and List a Media Termination Points window displays.

Step 2 Choose the search criteria to use.

Step 3 Click Find.
The window displays a list of a Media Termination Points that match the search criteria.

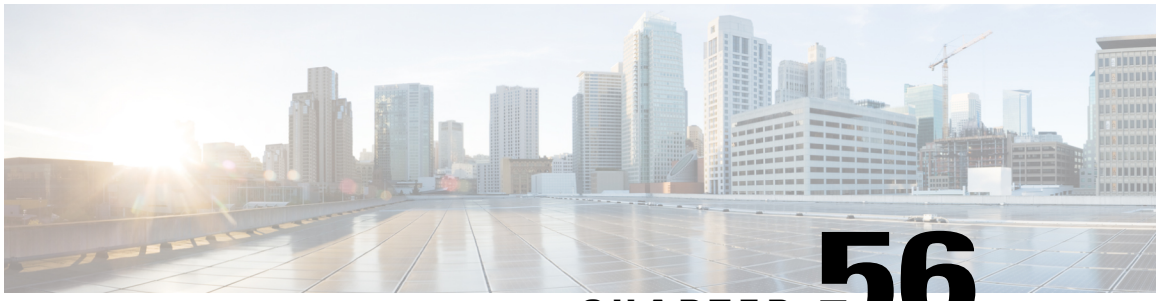
Step 4 Check the check boxes next to the Media Termination Points that you want to synchronize. To choose all Media Termination Points in the window, check the check box in the matching records title bar.

Step 5 Click Apply Config to Selected.
The Apply Configuration Information dialog displays.

Step 6 Click OK.

Related Topics

Media Termination Point Setup , on page 387



CHAPTER 56

Transcoder Setup

This chapter provides information to configure transcoders.

For additional information, see topics related to transcoders and media resource management in the Cisco Unified Communications Manager System Guide.

About Transcoder Setup

In Cisco Unified Communications Manager Administration, use the **Media Resources** > **Transcoder** menu path to configure transcoders.

The Media Resource Manager (MRM) has responsibility for resource registration and resource reservation of transcoders within a Cisco Unified Communications Manager cluster. Cisco Unified Communications Manager simultaneously supports registration of both the Media Termination Point (MTP) and transcoder and concurrent MTP and transcoder functionality within a single call.

The Cisco Unified Communications Manager invokes a transcoder on behalf of endpoint devices when the two devices are using different codecs and would normally not be able to communicate. When inserted into a call, the transcoder converts the data streams between the two disparate codecs to enable communications between them.

A transcoder control process gets created for each transcoder device that is defined in the database. Each transcoder registers with the MRM when it initializes. The MRM keeps track of the transcoder resources and advertises their availability throughout the cluster.

Transcoder Deletion

You cannot delete a transcoder that is assigned to a media resource group. To find out which media resource groups are using the transcoder, from the Transcoder Configuration window, choose Dependency Records from the Related Links drop-down list box and click Go. If the dependency records are not enabled for the

system, the dependency records summary window displays a message. If you try to delete a transcoder that is in use, Cisco Unified Communications Manager displays a message. Before deleting a transcoder that is currently in use, you must remove the transcoder from the media resource group(s) to which it is assigned.

Related Topics

Access Dependency Records , on page 982

Transcoder Settings

The following table describes the transcoder settings.

Table 66: Transcoder Settings

Field	Description
Transcoder Type	Choose the appropriate transcoder type: Cisco Media Termination Point Hardware, Cisco IOS Media Termination Point, Cisco IOS Enhanced Media Termination Point, or Cisco Media Termination Point (WS-SVC-CMM). For specific information on these transcoder types, see the *Cisco Unified Communications Manager System Guide*.
Description	Enter a description (up to 128 characters) or leave blank to generate automatically from the MAC address or device name that you provide.
Device Name	This field displays if you chose Cisco IOS Media Termination Point or Cisco IOS Enhanced Media Termination Point as the transcoder type. Enter the same transcoding name that you entered in the gateway Command Line Interface (CLI). Enter up to 15 characters. Valid characters comprise alphanumeric characters (a-z, A-Z, 0-9), as well as dot (.), dash (-), and underscore (_).
Transcoder Name	For Cisco Media Termination Point (WS-SVC-CMM) transcoders, the system fills in this value based on the MAC address that you provide.
MAC Address	For Cisco media termination point hardware or Cisco Media Termination Point (WS-SVC-CMM), enter a MAC address, which must be 12 characters.
Subunit	For Cisco Media Termination Point (WS-SVC-CMM) transcoders, choose a subunit from the drop-down list box.
Device Pool	From the drop-down list box, choose a device pool. For more detailed information on the chosen device pool, click View Details.
Common Device Configuration	From the drop-down list box, choose a common device configuration. For more detailed information on the chosen common device configuration, click View Details.

Field	Description
Special Load Information	Enter any special load information into the Special Load Information field or leave blank to use default. Valid characters include letters, numbers, dashes, dots (periods), and underscores.
Trusted Relay Point	Check this check box to designate this transcoder as a trusted relay point (TRP) that Cisco Unified Communications Manager can use in a network virtualization environment. See the *Cisco Unified Communications Manager System Guide* for a discussion of trusted relay points.
Maximum Capacity	For Cisco Media Termination Point (WS-SVC-CMM) transcoders, choose a maximum capacity from the drop-down list box.
Product-Specific Configuration Layout	
Model-specific configuration fields defined by the device manufacturer	The device manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the "?" information icon below the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, see the documentation for the specific device that you are configuring or contact the manufacturer.

Related Topics

Transcoder Setup , on page 391

Synchronize Transcoder

To synchronize a transcoder with the most recent configuration changes, perform the following procedure, which applies 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** > **Transcoder**.
The Find and List Transcoders window displays.

Step 2 Choose the search criteria to use.

Step 3 Click Find.
The window displays a list of transcoders that match the search criteria.

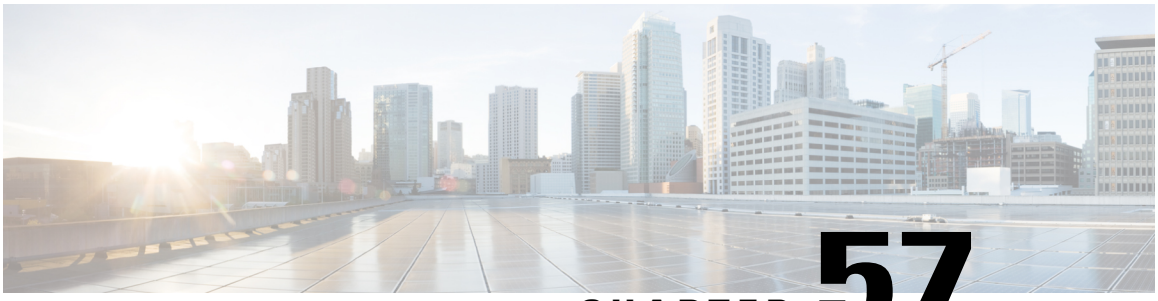
Step 4 Check the check boxes next to the transcoders that you want to synchronize. To choose all transcoders in the window, check the check box in the matching records title bar.

Step 5 Click Apply Config to Selected.
The Apply Configuration Information dialog displays.

Step 6 Click OK.

Related Topics

Transcoder Setup , on page 391



CHAPTER 57

Media Resource Group Setup

This chapter provides information to configure media resource groups. You can group devices of the following types into a single media resource group:

- Conference Bridge (CFB)
- Media Termination Point (MTP)
- Music On Hold Server (MOH)
- Transcoder (XCODE)
- Annunciator (ANN)

For additional information, see topics related to media resources, media resource groups, and media resource group lists in the *Cisco Unified Communications Manager System Guide*.

About Media Resource Group Setup

In Cisco Unified Communications Manager Administration, use the **Media Resources** > **Media Resource Group** menu path to configure media resource groups.

Media resource management comprises working with media resource groups and media resource group lists. Media resource management provides a mechanism for managing media resources, so all Cisco Unified Communications Managers within a cluster can share them. Media resources provide conferencing, transcoding, media termination, annunciator, and music on hold services.

You can associate a media resource group, a logical grouping of media servers, with a geographical location or with a site as desired. You can also form media resource groups to control the usage of servers or the type of service (unicast or multicast) that is desired.

Media Resource Group Configuration Tips

Be aware that you cannot delete a media resource, such as a conference bridge, that is part of a media resource group unless you first remove the resource from the media resource group or you delete the media resource group that contains the media resource.

Media Resource Group Deletion

You cannot delete a media resource group that is assigned to a Media Resource Group List. To find out which media resource groups lists are using the media resource group, in the Media Resource Group Configuration window, from the Related Links drop-down list box, choose Dependency Records and click Go. If the dependency records are not enabled for the system, the dependency records summary window displays a message. If you try to delete a media resource group that is in use, Cisco Unified Communications Manager displays a message. Before deleting a media resource group that is currently in use, you must perform either or both of the following tasks:

- Assign a different media resource group list to any media resource groups that are using the media resource group that you want to delete.
- Delete the media resource group lists that are using the media resource group that you want to delete.

Related Topics

About Media Resource Group List Setup , on page 399
Media Resource Group List Deletion , on page 399
Access Dependency Records , on page 982

Media Resource Group Settings

The following table describes the settings that are used for configuring media resource groups.

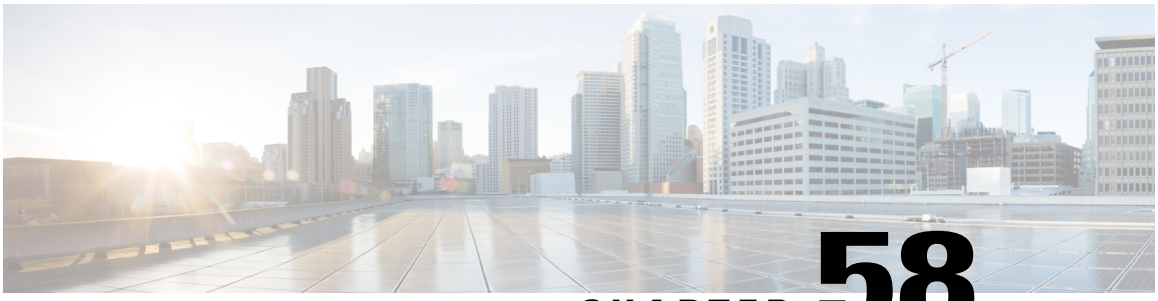
Table 67: Media Resource Group Settings

Field	Description
Name	Enter a unique name in this required field for the Cisco Unified Communications Manager to identify the media resource group. This name can comprise up to 50 characters. Valid characters include letters, numbers, spaces, dashes, dots (periods), and underscores.
Description	Enter a description for the media resource group. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), or angle brackets (<>).
Devices for this Group	This area comprises two panes that are used to define the media resources for a media resource group: Available Media Resources and Selected Media Resources.

Field	Description
Available Media Resources	This pane lists the media resources that can be chosen for a media resource group. The list includes the following media resource types: • Conference Bridges (CFB) • Media Termination Points (MTP) • Music On Hold Servers (MOH) • Transcoders (XCODE) • Annunciator (ANN) Music on hold servers that are configured for multicast get labeled as (MOH)[Multicast]. To add a media resource for this media resource group, choose one from the list and click the down arrow. After a media resource is added, its name moves to the Selected Media Resources pane.
Selected Media Resources	This pane lists the media resources that were chosen for a media resource group. For any media resource group, you must choose at least one media resource. To delete (unselect) a media resource, choose its name in the list and click the up arrow.
Use Multicast for MOH Audio (If at least one multicast MOH resource is available)	To use multicast for Music On Hold Audio, check this check box. To do so, make sure that at least one of the selected media resources is a multicast MOH server. **Note** The system administrator configures or creates multicast audio sources.

Related Topics

Media Resource Group Setup , on page 395



CHAPTER 58

Media Resource Group List Setup

This chapter provides information to configure Media Resource Group Lists.

For additional information, see topics related to media resources, media resource groups, and media resource group lists in the *Cisco Unified Communications Manager System Guide*.

About Media Resource Group List Setup

In Cisco Unified Communications Manager Administration, use the **Media Resources** > **Media Resource Group List** menu path to configure media resource group lists.

Media resource management comprises working with media resource groups and media resource group lists. Media resource management provides a mechanism for managing media resources, so all Cisco Unified Communications Managers within a cluster can share them. Media resources provide conferencing, transcoding, media termination, annunciator, and music on hold services.

A Media Resource Group List provides a prioritized grouping of media resource groups. An application selects the required media resource, such as a music on hold server, from among the available media resources according to the priority order that is defined in a Media Resource Group List.

Media Resource Group List Configuration Tips

Be aware that you cannot delete a media resource group that is assigned to a Media Resource Group List unless you first remove the media resource group from the Media Resource Group List(s) to which it is assigned or you delete the Media Resource Group List.

Media Resource Group List Deletion

Be aware that you cannot delete a Media Resource Group List that is assigned to a device pool(s) or to a device(s). You must first modify the device pool(s) or device(s) to which a Media Resource Group List is assigned.

Media Resource Group List Settings

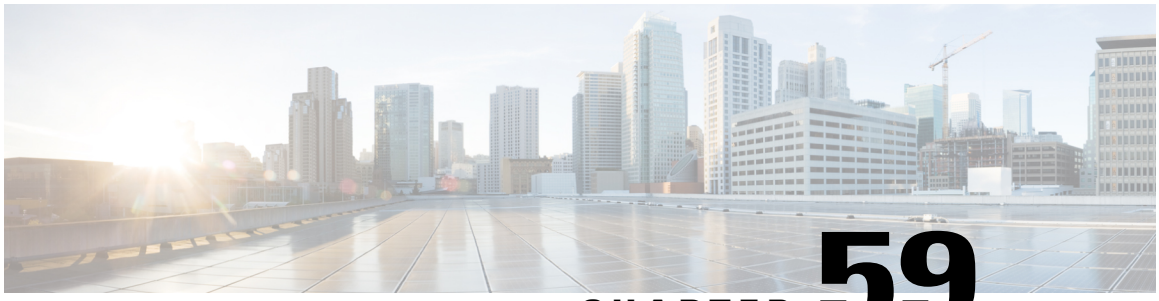
The following table describes the settings that are used for configuring Media Resource Group Lists.

Table 68: Media Resource Group List Settings

Field	Description
Media Resource Group List Information	
Name	Enter a unique name in this required field for the Cisco Unified Communications Manager to identify the Media Resource Group List. This name can comprise up to 50 characters. Valid characters include letters, numbers, spaces, dashes, dots (periods), and underscores.
Media Resource Groups for this List	
Available Media Resource Groups	This window lists the media resource groups that can be chosen for a Media Resource Group List. The list includes only previously defined media resource groups. To add a media resource group for this Media Resource Group List, choose one from the list and click the down arrow that is located between the two panes. After a media resource group is added, its name moves to the Selected Media Resource Groups pane.
Selected Media Resource Groups	This pane lists the media resource groups that were chosen for a Media Resource Group List. For any Media Resource Group List, you must choose at least one media resource group. To delete (unselect) a media resource group, choose its name in the list and click the up arrow that is located between the two panes. Because media resource groups are listed in order of priority (highest to lowest), you must use the up and down arrows that are located to the right of this pane to reorder the media resource group priority. To do so, choose a media resource group in the list and use the up or down arrow to change its priority.

Related Topics

Media Resource Group List Setup , on page 399



CHAPTER 59

Announcement Setup

The chapter provides information about using Cisco-provided announcements and tones.

For additional information, see topics related to External Call Control in the *Cisco Unified Communications Manager Features and Services Guide*.

Cisco-Provided Announcements and Tones

Cisco-provided announcements and tones are installed automatically when you install Cisco Unified Communications Manager. These announcements and tones are displayed in the Find and Lists Announcements window in Cisco Unified Communications Manager Administration.

Announcements can be used for:

- Basic calls
- External call control
- Multilevel Precedence and Preemption (MLPP)

Selecting **Media Resources > Announcements** in Cisco Unified Communications Manager allows you to use the existing Cisco-provided announcements, insert custom announcement .wav files, assign the locale for the announcement, change the description for the announcement, or change the message or tone that you wish an announcement to play.

Related Topics

Announcement Setup , on page 401

About Announcement Setup

In Cisco Unified Communications Manager Administration, use the **Media Resources** > **Announcements** menu path to configure announcements.

There are two classifications of announcements:

- System Announcements
- Feature Announcements

System announcements are pre-defined announcements that are used in normal call processing or provided as sample feature announcements. Feature announcements are used by specific features such as Music On Hold (MoH) in association with Hunt Pilot call queuing or External Call Control.

There are up to 50 feature announcements available using the Add New button. These announcements may be Cisco-provided audio files or uploaded custom wav files. All custom announcement wav files must be uploaded to all servers in the cluster.

Note Announcements are specific to the locale (language). If your installation is using more than one language locale, each custom announcement must be recorded in each language as a separate wav file and uploaded with the correct locale assignment. This also requires that the correct locale package be installed on each server before uploading custom announcement wav files for languages other than United States English.

From the Announcement Listing window, clicking on the announcement identifier for an announcement produces an announcement configuration dialog. Within this dialog you can edit the announcement description and other settings. If one or more custom wav files have been uploaded for the announcement, a list of the custom wav files for each locale (language) is created. Each of these files also have an Enable check-box to indicate if the custom wav file should be used. If the check-box is unchecked, then the selected Cisco audio file is used.

Like MoH audio source files, the recommended format for announcements includes the following specifications:

- 16-bit PCM wav file
- Stereo or mono
- Sample rates of 48 kHz, 44.1 kHz, 32 kHz, 16 kHz, or 8 kHz

Tip When a call is routed to a queuing-enabled Hunt Pilot that is configured with MoH, and has an initial announcement configured (with "Play Always" and early media cut through), the greeting is played to the caller before the called party is alerted about the call. Trunks and gateways must also support early media cut through for the greeting to be played. Cisco PRI/MGCP gateways, H.323 gateways and trunks support early media cut through. For SIP trunk to support early media cut through, you must enable PRACK. Be aware that a greeting may not be played if the device does not support early media cut through.

Announcement Deletions

You cannot delete any System or Feature announcements that are configured for use within Cisco Unified Communications Manager Administration (such as MoH). In these instances, a selection check-box will not appear. To delete a feature announcement, select the check-box and click on the **Delete** button.

Announcement Settings

The following table describes the announcement settings.

Table 69: Announcement Settings

Field	Description
Announcement Configuration and Upload File Windows	
Announcement Identifier	The Announcement Identifier is a text box to assign a meaningful identifying name to the announcement. This field cannot be modified for System Announcements. This field must be unique (different from all other announcements). The Announcement Identifier is used when selecting an announcement for a feature such as Music-on-Hold.
Customized Description	For customized announcements that you are inserting, enter a description for the announcement; for example, enter the text from the customized announcement. You can enter any characters in this field. When you click the Upload File button in the Find and List window, this field displays as blank. When you click the Upload File button in the Announcements Configuration window, the Cisco-provided (default) description for the announcement displays. If you do not update this field in the Announcements Configuration window, the Cisco-provided (default) description displays. After you update this customized description field, the Cisco-provided default description displays in the Find and Lists Announcements window; see the Default Description column in the Find and Lists window for the default description. You can enter up to 50 characters.
Locale	This setting displays in the Upload File window. From the Locale drop-down list box, choose the locale that you want to associate with the announcement. By default, all Cisco-provided announcements support English_United States. If a Cisco Unified Communications Locale has been installed, the Cisco-provided announcements are provided for that locale in addition to other installed locales. **Tip** For a locale to display in the Locale drop-down list box in the Upload File Configuration window, you must install the Cisco Unified Communications Locale Installer that is specific to your locale(s). For more information, see the *Cisco Unified Communications Operating System Administration Guide*.

Field	Description
Default Announcement	From the drop-down list box, choose the Cisco-provided announcement that you want to play when the custom announcement is not used. If <None> is selected from the list box, no Cisco-provided announcement will be used.
Announcement by Locale Pane in the Announcements Configuration Window **Note** This section only appears if a custom announcement wav file has been uploaded for the announcement.	
Enable	This setting displays after you insert a customized announcement. When the Enable check box is checked, Cisco Unified Communications Manager plays the customized announcement for the locale that is shown. If you want Cisco Unified Communications Manager to play the Cisco-provided announcement that is associated with the announcement identifier, uncheck the Enable check box.
Customized Locale Description	This field, which is read-only, displays the description for the customized announcement for the displayed locale. You enter this description when you upload the customized announcement.
Locale	This field, which is read-only, displays the locale that you chose for the customized announcement when you uploaded the .wav file. Each locale is associated with an uploaded custom announcement. You can upload another wav file for the same announcement, but you assign it to a different locale. In this case, two rows display, one for each locale. If you want to update or replace a custom announcement for a locale, you can upload a new wav file with the same locale you want to replace.
Default Cisco Announcement	This field indicates the last uploaded customized announcement file name.

Related Topics

Announcement Setup , on page 401

Announcements in the Find and List Announcements Window

You can upload custom announcement wav files or change the Cisco-provided file for a System announcement, however; you cannot change the announcement identifier. For example, the System announcement (VCA_00121) is played when a caller dials an invalid number. This is commonly known as the "vacant call announcement" and could be modified with an uploaded custom wav file with a different announcement.

You cannot update announcements that are not hyperlinked in the Find and List Announcements window. You can insert customized announcements for Cisco-provided announcements that are underlined with a hyperlink in the Find and List Announcements window; for example, Custom_5001, Custom_5014, MLPP-ICA_00120, or MonitoringWarning_00055. For more information on how to upload a customized announcement, see the following sections:

- About Announcement Setup , on page 402
- Upload Customized Announcement , on page 405

The following table describes the announcements that display in the Find and List Announcements window. This list is an initial example and may change based on feature announcements being inserted and future upgrades.

Table 70: Announcements in the Find and List Announcements Window

Announcement Identifier	Description
Gone_00126	System: Gone
MLPP-BNEA_00123	System: MLPP Busy not equipped
MLPP-BPA_00122	System: MLPP Higher precedence
MLPP-ICA_00120	System: MLPP Service disruption
MLPP-PALA_00119	System: MLPP Precedence access limit
MLPP-UPA_00124	System: MLPP Unauthorized precedence
Mobility_VMA	Please press 1 to be connected
MonitoringWarning_00055	System: Monitoring or Recording
RecordingWarning_00038	System: Recording
TemporaryUnavailable_00125	System: Temporary unavailable
VCA_00121	System: Vacant number / invalid number dialed
Wait_In_Queue_Sample	Builtin: Sample queued caller periodic announcement
Welcome_Greeting_Sample	Builtin: Sample caller greeting

Upload Customized Announcement

Perform the following procedure to upload a customized announcement.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Media Resources** > **Announcements**. The Find and List Announcements window displays.

Step 2 In the Find and List Announcements window, click the hyperlink for the announcement (for example, Wait In Queue Sample). When the Announcements window displays, click **Upload File**.

Step 3 In the Upload File pop-up window, choose the locale, enter the filename or browse to select the .wav file and click **Upload File**.
The upload process begins, and may take a few minutes depending on the file. The Status is updated once processing is complete. Select **Close** to close the upload window.

Step 4 The Announcement Configuration window refreshes to update the uploaded file status.

Step 5 If you want Cisco Unified Communications Manager to play the customized announcement instead of playing the Cisco-provided announcement, make sure that the Enable check box displays as checked in the Announcement by Locale pane in the Announcements Configuration window. If the Enable check box is unchecked, Cisco Unified Communications Manager plays the Cisco-provided announcement.

Step 6 Once the changes have been made in the Announcements Configuration window, click **Save.**

What to Do Next

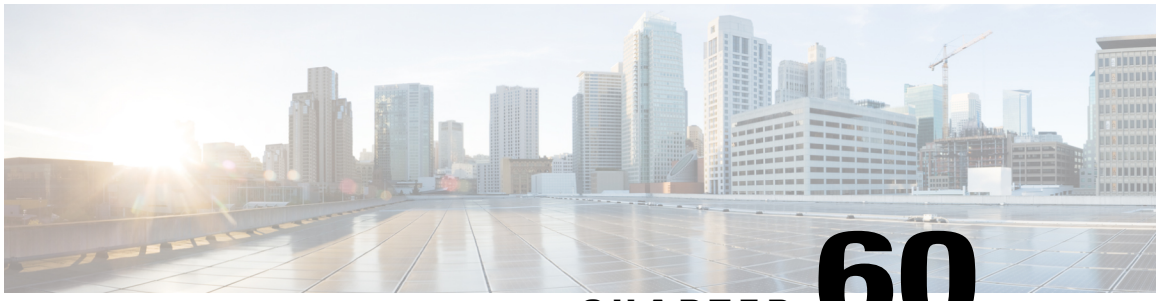
You must upload the announcement on each node in the cluster as the announcement files are not propagated between servers in a cluster. Browse Cisco Unified Communications Manager Administration on each server in the cluster and repeat the upload process.

Related Topics

Announcement Setup , on page 401
About Announcement Setup , on page 402

Play Announcement

After you insert the custom announcement, Cisco Unified Communications Manager automatically plays the custom announcement, unless you uncheck the Enable check box in the Announcements by Locale pane in the Announcements Configuration window (which indicates that you want Cisco Unified Communications Manager to play the Cisco-provided announcement that is associated with the announcement identifier).



CHAPTER 60

Other Media Resource Menu Options

This chapter provides brief descriptions of selected Media Resource menu options. A pointer to the documentation where more detailed information is available for the option is provided.

Music On Hold Audio Source Setup

In Cisco Unified Communications Manager Administration, use the **Media Resources** > **Music On Hold Audio Source** menu path 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 that is 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.

For more information on how to use the Music On Hold Audio Source Configuration window, see the *Cisco Unified Communications Manager Features and Services Guide*.

Fixed MOH Audio Source Setup

In Cisco Unified Communications Manager Administration, use the **Media Resources** > **Fixed MOH Audio Source** menu path to configure the fixed Music On Hold audio source.

The integrated Music On Hold feature provides the ability to place on-net and off-net users on hold with music that is 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. You can also enable a music on hold fixed audio source, and this audio source can allow multicasting.

For more information on how to use the Fixed MOH Audio Source Configuration window, see the *Cisco Unified Communications Manager Features and Services Guide*.

Music On Hold Server Setup

In Cisco Unified Communications Manager Administration, use the **Media Resources** > **Music On Hold Server** menu path to configure fixed Music On Hold servers.

The Cisco Unified Communications Manager Music On Hold feature uses the 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.

For more information on how to use the Music On Hold Server Configuration window, see the *Cisco Unified Communications Manager Features and Services Guide*.

MOH Audio File Management Setup

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.

For more information on how to use the MOH Audio File Management Configuration window, see the *Cisco Unified Communications Manager Features and Services Guide*.

Mobile Voice Access Setup

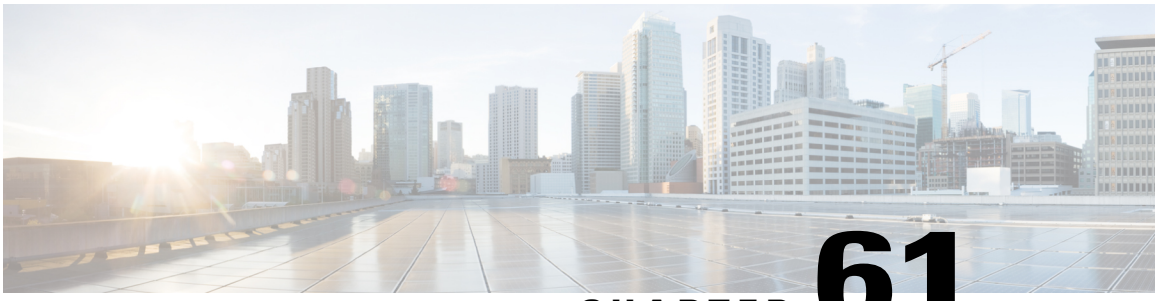
In Cisco Unified Communications Manager Administration, use the **Media Resources** > **Mobile Voice Access** menu path to configure sets of localized user prompts for Mobile Voice Access.

Cisco Unified Mobility allows users to manage business calls using a single phone number and pick up in-progress calls on the desktop phone and cellular phone. Mobile Voice Access is the associated integrated voice response (IVR) system, which allows users to turn Cisco Unified Mobility on or off and to initiate calls from a cellular phone or other remote phone as if the call were initiated from the desktop phone.

The Mobile Voice Access window contains settings for localized user IVR prompts. For more information on how to configure Cisco Unified Mobility and Mobile Voice Access, see the *Cisco Unified Communications Manager Features and Services Guide*.

PART V

Advanced Features Setup



CHAPTER 61

Cisco Voice-Mail Port Setup

This chapter provides information to add and delete Cisco voice-mail ports in the Cisco Unified Communications Manager database without using the Cisco Voice Mail Port Wizard.

For additional information, see the *Cisco Unity and Cisco Unity Connection Configuration Checklist, Cisco Unified Communications Manager System Guide.*

About Cisco Voice-Mail Port Setup

In Cisco Unified Communications Manager Administration, use the **Advanced Features** > **Voice Mail** > **Cisco Voice Mail Port** menu path to configure Cisco voice-mail ports.

The optional Cisco Unity or Cisco Unity Connection software, available as part of Cisco Unified Communications Solutions, provides voice-messaging capability for users when they are unavailable to answer calls. Cisco Unity Connection provides voice-messaging capability for users when they are unavailable to answer calls. This section describes the procedures for adding, configuring, updating, and deleting Cisco voice-mail ports by choosing Voice Mail from the Feature menu of the Cisco Unified Communications Manager Administration window and choosing Cisco Voice Mail Port.

For more information about configuring Cisco Unity, see the applicable Cisco Unified Communications Manager Integration Guide for Cisco Unity.

For more information on voice-messaging connectivity to Cisco Unified Communications Manager, see the *Cisco Unified Communications Manager System Guide*.

Cisco Voice-Mail Ports Configuration Tips

To connect a Cisco voice-messaging system to Cisco Unified Communications Manager, you must add Cisco voice-mail ports to the Cisco Unified Communications Manager database.

Tip You can also use the Cisco Voice Mail Port Wizard to add a new Cisco voice-mail server and ports or to add multiple ports to an existing server rather than using the procedure that is described here.

Related Topics

Cisco Voice Mail Port Wizard, on page 419

Cisco Voice-Mail Port Deletion

When you delete a Cisco voice-mail port that a directory number uses, the number remains in the Cisco Unified Communications Manager database. To determine which directory numbers are using the voice-mail port, in the Voice Mail Port Configuration window, choose Dependency Records from the Related Links drop-down list box and click Go. If the dependency records are not enabled for the system, the dependency records summary window displays a message.

When you delete a voice-mail port that is in use, Cisco Unified Communications Manager displays a message. Before deleting a voice-mail port that is currently in use, you can assign a different voice-mail port to any directory number that is using the voice-mail port that you want to delete.

After you delete the voice-mail port, you can delete the directory number that was using the voice-mail port.

Tip Instead of using the **Advanced Features** > **Voice Mail** > **Cisco Voice Mail Port** menu option, you can use the Cisco Voice Mail Port Wizard to delete ports from an existing server.

Related Topics

About Directory Number Setup , on page 289
Delete Unassigned Directory Number , on page 335
Cisco Voice Mail Port Wizard, on page 419
Access Dependency Records , on page 982

Cisco Voice-Mail Port Settings

The following table describes the Cisco voice-mail port settings.

Table 71: Cisco Voice-Mail Port Settings

Field	Description
Device Information	

Field	Description
Port Name	Enter a name to identify the Cisco voice-mail port. You must add a device for each port on Cisco voice-messaging system. If 24 ports exist, you must define 24 devices. The Port Name field allows 1 to 15 characters, which can include letters, numbers, periods, underscores, and dashes, followed by -VI and the port number. **Note** For Cisco Unity, this name must match the name in the Unity Telephony Integration Manager (UTIM), such as Cisco UM-VI1 or Cisco UM-VI2. For Cisco Unity Connection, this name must match the name in Cisco Unity Connection Administration, such as Cisco UM-VI1 or Cisco UM-VI2.
Description	Enter the purpose of the device.
Device Pool	Choose the default value or a specific device pool.
Common Device Configuration	Choose the common device configuration to which you want this device assigned. The common device configuration includes the attributes (services or features) that are associated with a particular user. Common device configurations are configured in the Common Device Configuration window.
Calling Search Space	From the drop-down list box, choose the appropriate calling search space. A calling search space comprises a collection of partitions that are searched for numbers that were called from this device. Choose the name of the calling search space that allows calls to the subscriber phones and to any network devices. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more 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 ... button to display the Select Calling Search Space window. Enter a partial calling search space name in the List items where Name contains field. Click the desired calling search space name in the list of 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.
AAR Calling Search Space	Choose the appropriate calling search space for the device 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.

Field	Description
Location	Use locations to implement call admission control (CAC) in a centralized call-processing system. CAC enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location. From the drop-down list box, choose the appropriate location for this voice-mail port. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this voice-mail port consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the **System** > **Location** menu option. For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*.
Device Security Mode	From the drop-down list box, choose a security mode to apply to the voice-mail server port. The database predefines these options. The default value specifies Not Selected. For more information on configuring security for the voice-mail server, see the *Cisco Unified Communications Manager System Guide*.

Field	Description
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified Communications Manager inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values: • Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates. • Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified Communications Manager places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVPAgent). If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the *Cisco Unified Communications Manager System Guide* for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified Communications Manager first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified Communications Manager first tries to find a transcoder that is also designated as a TRP. See the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.
Directory Number Information	
Directory Number	Enter the number that is associated with this voice-mail port. Make sure that this field is unique in combination with the Partition field.
Partition	Choose the partition to which the directory number belongs. Choose <None> if partitions are not used. If you choose a partition, you must choose a calling search space that includes that 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, then find and choose a partition name. **Note** To set the maximum list box items, choose **System** > **Enterprise Parameters** and choose CCMAdmin Parameters.

Field	Description
Calling Search Space	From the drop-down list box, choose the appropriate calling search space. A calling search space comprises a collection of partitions that are searched for numbers that are called from this directory number. If you choose a partition, you must choose a calling search space that includes that partition. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more 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, then find and choose a calling search space name. **Note** To set the maximum list box items, choose **System** > **Enterprise Parameters** and choose CCMAdmin Parameters.
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.
Internal Caller ID Display	This field indicates text that displays on the called party phone when a call is placed from this line.
Internal Caller ID Display (ASCII format)	This field indicates text that appears on the called party phone, in ASCII format, when a call is placed from this line.
External Number Mask	Specify the mask that is used to format caller ID information for external (outbound) calls. The mask can contain up to 50 characters. Enter the literal digits that you want to display in the caller ID information and use Xs to represent the directory number of the device. You can also enter the international escape character +. When Automated Alternate Routing (AAR) routes calls due to insufficient bandwidth, Cisco Unified Communications Manager uses the value in this field to place the call if sufficient bandwidth is not available. Example: DN 1000 (external mask 9728131000) calls DN 1001 (external mask 2144131001). If insufficient bandwidth blocks the call, Cisco Unified Communications Manager uses the AAR prefix digits along with 2144131001 to place the call to 1001.

Related Topics

Location Setup , on page 127
Search for Partition , on page 270
About Calling Search Space Setup , on page 273
Common Device Setup , on page 763

Synchronize Cisco Voice-Mail Port with Devices

To synchronize devices with a voice mail port that has undergone configuration changes, perform the following procedure, which applies 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 **Advanced Features** > **Voice Mail** > **Cisco Voice Mail Port**.
The Find and List Voice Mail Ports window displays.

Step 2 Choose the search criteria to use.

Step 3 Click Find.
The window displays a list of voice mail ports that match the search criteria.

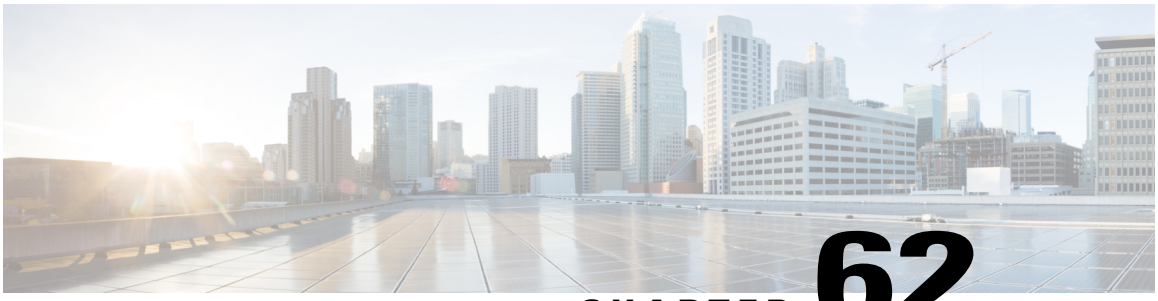
Step 4 Check the check boxes next to the voice mail ports with which you want to synchronize affected devices. To choose all voice mail ports in the window, check the check box in the matching records title bar.

Step 5 Click Apply Config to Selected.
The Apply Configuration Information dialog displays.

Step 6 Click OK.

Related Topics

Cisco Voice-Mail Port Setup , on page 411



CHAPTER 62

Cisco Voice Mail Port Wizard

This chapter provides information to configure Cisco voice-mail ports in the Cisco Unified Communications Manager database using the Cisco Voice Mail Port Wizard.

For additional information, see the *Cisco Unified Communications Manager System Guide.*

Voice-Mail Port Setup Using Wizard

In Cisco Unified Communications Manager Administration, use the **Advanced Features** > **Voice Mail** > **Cisco Voice Mail Port Wizard** menu path to configure voice-mail ports with the help of a wizard tool.

The optional Cisco Unity or Cisco Unity Connection software, available as part of Cisco Unified Communications Solutions, provides voice-messaging capability for users when they are unavailable to answer calls. This section describes the procedures that are required for adding and configuring Cisco voice-mail ports in Cisco Unified Communications Manager for voice-messaging systems.

For more information about configuring Cisco Unity, see the *Cisco Unified Communications Manager SCCP Integration Guide for Cisco Unity* or the *Cisco Unified Communications Manager SIP Trunk Integration Guide for Cisco Unity*.

For more information about configuring Cisco Unity Connection, see the *Cisco Unified Communications Manager SCCP Integration Guide for Cisco Unity Connection* or the *Cisco Unified Communications Manager SIP Trunk Integration Guide for Cisco Unity Connection*.

For more information on voice-messaging connectivity to Cisco Unified Communications Manager, see the *Cisco Unified Communications Manager System Guide*.

The Cisco Voice Mail Port Wizard tool allows Cisco Unified Communications Manager administrators to quickly add and delete ports that are associated with a Cisco voice-mail server to the Cisco Unified Communications Manager database.

Add New Cisco Voice-Mail Server and Ports Using Wizard

To use the Cisco Voice Mail Port Wizard to add a new Cisco voice-mail server and ports to the Cisco Unified Communications Manager database, perform the following steps.

Before You Begin

The Cisco Voice Mail Port Wizard requires a range of consecutive directory numbers for the voice-mail ports. Make sure the voice-mail pilot number and subsequent numbers are available.

Procedure

Step 1 Choose **Advanced Features** > **Voice Mail** > **Cisco Voice Mail Port Wizard**.

Step 2 Choose Create a new Cisco Voice Mail Server and add ports to it.

Step 3 Click Next.

Step 4 Choose Add ports to a new Cisco Voice Mail server using this name.

Step 5 Enter a name for the Cisco voice-mail server.

Note For Cisco Unity, this name must match the name in the Unity Telephony Integration Manager (UTIM), such as Cisco UM-VI1 or Cisco UM-VI2. For Cisco Unity Connection, this name must match the name in Cisco Unity Connection Administration, such as Cisco UM-VI1 or Cisco UM-VI2.

Step 6 Click Next.
The Cisco Voice Mail Ports window displays.

Step 7 From the drop-down list box, choose the number of ports to add.

Step 8 Click Next.
The Cisco Voice Mail Device Information window displays.

Step 9 Enter the appropriate configuration settings, as described in Table 72: Voice Mail Port Wizard Device Information Configuration Settings, on page 421. The wizard applies these configuration settings to all the new ports.

Step 10 Click Next.
The Cisco Voice Mail Directory Numbers window displays.

Step 11 Enter the directory number settings for the new Cisco voice-mail server as described in Table 73: Voice Mail Port Wizard Directory Number Configuration Settings, on page 423.

Step 12 Click Next.
A window that asks whether you want to add these directory numbers to a line group displays.

Step 13 Choose one of the options that display:

a) If you choose to add directory numbers to a new line group, skip to Step 14, on page 420.
b) If you choose to add directory numbers to an existing line group, skip to Step 16, on page 421.
c) If you choose to add directory numbers to a line group later, skip to Step 18, on page 421.

Step 14 Choose the “Yes. Add directory numbers to a new Line Group” option and click Next.

Step 15 In the Line Group window that displays, enter the name of the new line group and click Next.
The Ready to Add Cisco Voice Mail Ports summary window displays. This summary window lists the settings that you configured in the previous windows. The Cisco Voice Mail Port Wizard automatically assigns the correct values for each port.

Skip to Step 19, on page 421.

Step 16 Choose the "Yes. Add directory numbers to an existing Line Group" option and click Next.

Step 17 In the Line Group window that displays, choose a line group from the Line Group Name drop-down list box and click Next.
The Ready to Add Cisco Voice Mail Ports summary window displays. This summary window lists the settings that you configured in the previous windows. The Cisco Voice Mail Port Wizard automatically assigns the correct values for each port.

Skip to Step 19, on page 421.

Step 18 Choose the "No. I will add them later" option and click Next.
The Ready to Add Cisco Voice Mail Ports summary window displays. This summary window lists the settings that you configured in the previous windows. The Cisco Voice Mail Port Wizard automatically assigns the correct values for each port.

Step 19 If this information is correct, click Finish to add the new ports.
If the information shown is not correct, click the Back button to edit the information or Cancel to quit without adding any ports.

Step 20 After the Cisco Voice Mail Port Wizard finishes adding the new voice-mail ports that you specified, the Cisco Voice Mail Port Wizard Results window displays.
The window directs you to the other steps that you need to complete before you can start using these new voice-mail ports.

What to Do Next

Make sure that you set up the message-waiting indicator (MWI) device. For more information, see topics related to Cisco Unity and Cisco Unity Connection configuration in the *Cisco Unified Communications Manager System Guide*.

Related Topics

Cisco Voice Mail Port Wizard, on page 419
Add Ports to Cisco Voice-Mail Server Using Wizard, on page 424
Delete Ports from Cisco Voice-Mail Server Using Wizard, on page 425

Voice Mail Port Wizard Device Information Setup

The following table describes the Cisco voice-mail port wizard device information configuration settings.

Table 72: Voice Mail Port Wizard Device Information Configuration Settings

Field	Description
Description	Enter the purpose of device.
Device Pool	Choose the default value Default or any defined device pool.

Field	Description
Common Device Configuration	Choose the common device configuration to which you want this device assigned. The common device configuration includes the attributes (services or features) that are associated with a particular user. Common device configurations get configured in the Common Device Configuration window.
Calling Search Space	From the drop-down list box, choose the appropriate calling search space. A calling search space comprises a collection of partitions that are searched for numbers that are called from this directory number. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more 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, then find and choose a calling search space name. **Note** To set the maximum list box items, choose **System** > **Enterprise Parameters** and choose CCMAdmin Parameters.
AAR Calling Search Space	Choose the appropriate calling search space for the device to use when it performs automated alternate routing (AAR). 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.
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 box, choose the appropriate location for this port. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this port consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the **System** > **Location** menu option. For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*.
Device Security Mode	From the drop-down list box, choose a security mode to apply to the voice-mail server port. The database predefines these options. The default value specifies Not Selected. For more information on configuring security for the voice-mail server, see the *Cisco Unified Communications Manager Security Guide*.

Related Topics

Location Setup , on page 127
About Calling Search Space Setup , on page 273
Common Device Setup , on page 763

Voice Mail Port Wizard Directory Number Setup

The following table describes the Cisco voice-mail port wizard directory number configuration settings.

Table 73: Voice Mail Port Wizard Directory Number Configuration Settings

Field	Description
Beginning Directory Number	Enter the number that people call to access the Cisco voice-mail server. Each new port receives the next available directory number.
Partition	Choose the partition to which this set of directory numbers belong. Choose None if partitions are not used. If you choose a partition, you must choose a calling search space that includes that 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. Find and choose a partition name by using the procedure in the Search for Partition , on page 270. **Note** To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters.
Calling Search Space	From the drop-down list box, choose the appropriate calling search space. A calling search space comprises a collection of partitions that are searched for numbers that are called from this directory number. If you choose a partition, you must choose a calling search space that includes that partition. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more 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 a calling search space name (see the About Calling Search Space Setup , on page 273). **Note** To set the maximum list box items, choose **System** > **Enterprise Parameters** and choose CCMAdmin Parameters.
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.

Field	Description
Internal Caller ID Display	This field indicates text that displays on the calling party phone when a call is placed to this line.
Internal Caller ID Display (ASCII format)	This field indicates text that displays on the calling party phone, in ASCII format, when a call is placed to this line.
External Number Mask	Specify the mask that is used to format caller ID information for external (outbound) calls. The mask can contain up to 50 characters. Enter the literal digits that you want to display in the caller ID information and use Xs to represent the directory number of the device. You can also enter the international escape character +.

Add Ports to Cisco Voice-Mail Server Using Wizard

To use the Cisco Voice Mail Port Wizard to add ports to an existing Cisco voice-mail server, perform the following steps.

Before You Begin

The Cisco Voice Mail Port Wizard requires a range of consecutive directory numbers for the voice-mail ports. Make sure that the voice-mail pilot number and subsequent numbers are available.

The voice-mail pilot number designates the number that people call to access the Cisco voice-mail server.

Procedure

Step 1 Choose **Advanced Features** > **Voice Mail** > **Cisco Voice Mail Port Wizard**.

Step 2 Choose Add ports to an existing Cisco Voice Mail server.

Step 3 Click Next.
The Cisco Voice Mail Server window displays.

Step 4 From the drop-down list box, choose the name of an existing Cisco voice-mail server (pilot number) and click Next.
The Cisco Voice Mail Ports window displays and identifies the number of ports that are currently configured.

Step 5 From the drop-down list box, choose the number of ports to add and click Next.
The Cisco Voice Mail Directory Numbers window displays the configuration information for the Cisco voice-mail server to which you added the ports. The Cisco Voice Mail Port Wizard automatically selects consecutive directory numbers following the last port and uses the same Partition, Calling Search Space, Display, AAR Group, and External Number Mask settings as the Cisco voice-mail pilot directory number. You can enter a different range of directory numbers in the New Directory Numbers Start at field.

Step 6 If you need to change the number of ports, click the Back button.

Step 7 Click Next.
The Ready to Add Cisco Voice Mail Ports summary window displays. This summary window lists the settings that you configured in the previous windows. The Cisco Voice Mail Port Wizard automatically assigns the correct values for each port.

Step 8 If this information is correct, click Finish to add the new ports.
If the information shown is not correct, click the Back button to edit the information or click Cancel to quit without adding any ports.

Related Topics

Cisco Voice Mail Port Wizard, on page 419

Delete Ports from Cisco Voice-Mail Server Using Wizard

To delete ports from an existing Cisco voice-mail server, perform the following steps to use the Cisco Voice Mail Port Wizard.

Procedure

Step 1 Choose **Advanced Features** > **Voice Mail** > **Cisco Voice Mail Port Wizard**.

Step 2 Choose Delete ports from an existing Cisco Voice Mail server and click Next.
The Cisco Voice Mail Server window displays.

Step 3 From the drop-down list box, choose the name of an existing Cisco voice-mail server (pilot number) and click Next.
The Cisco Voice Mail Ports window, which indicates the number of ports that are currently configured, displays.

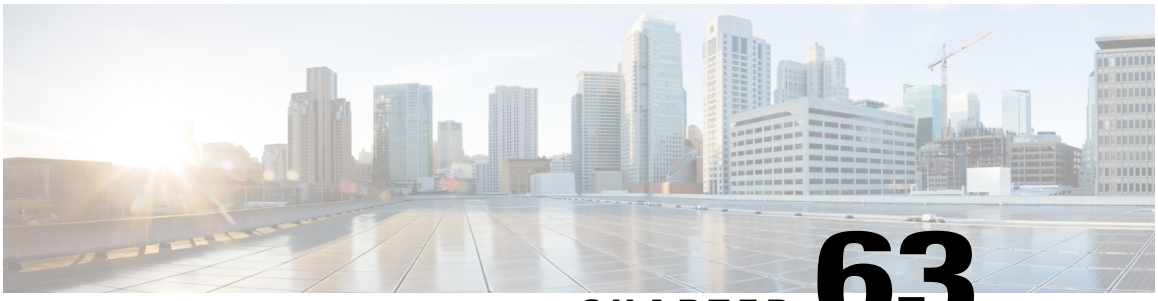
Step 4 From the drop-down list box, choose the number of ports to delete and click Next.
The Ready to Delete Cisco Voice Mail Ports summary window displays.

The summary window provides information about the ports to be deleted. The Cisco Voice Mail Port Wizard automatically updates the port numbers and directory numbers so they are consecutive.

Step 5 If this information is correct, click Finish to delete the selected ports.
If the information shown is not correct, click the Back button to edit the information or to quit without deleting any ports, click Cancel.

Related Topics

Cisco Voice Mail Port Wizard, on page 419



CHAPTER 63

Message Waiting Setup

This chapter provides information about message waiting configuration.

For additional information, see topics related to the Voice Mail Connectivity to Cisco Unified Communications Manager in the *Cisco Unified Communications Manager System Guide*, as well as topics related to Cisco Unity and Cisco Unity connection.

About Message Waiting Setup

In Cisco Unified Communications Manager Administration, use the **Advanced Features** > **Voice Mail** > **Message Waiting** menu path to configure message waiting numbers.

The Message Waiting Configuration window allows you to define a message waiting on or message waiting off directory number that a directory-connected based voice-messaging system uses to determine whether to set or clear a message waiting indication for a particular Cisco Unified IP Phone.

Message Waiting Numbers Configuration Tips

The voice-messaging system only uses the message-waiting on/off directory number to turn on the message-waiting indicator. Because Cisco Unified Communications Manager does not use the Message Waiting on/off number for receiving calls, the Display, Forward All, Forward Busy, and Forward No Answer fields do not get used.

Message Waiting Settings

The following table describes the Message Waiting settings.

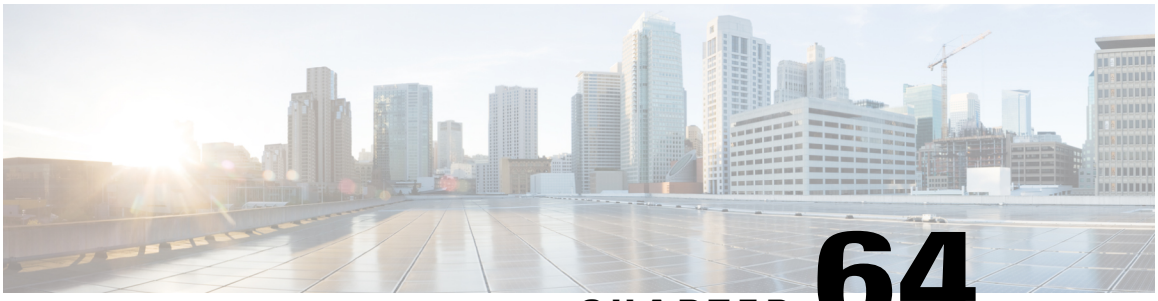
Table 74: Message Waiting Settings

Field Name	Description
Message Waiting Number	Enter the Cisco Message Waiting directory number. Make sure that this number is not used within the Cisco Unified Communications Manager auto-registration range. You may use the following characters: 0 to 9, ?, [,], +, -, *, ^, #, !. At the beginning of the number, you can enter \+ if you want to enter the international escape character.
Description	Enter up to 50 characters for a description of the message-waiting directory number. You may use any characters except the following: "", <, >, &, %.
Message Waiting Indicator	Click On or Off.
Partition	If partitions are being used, choose the appropriate partition from the drop-down list box. If you do not want to restrict access to the message-waiting device directory number, 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, then find and choose a 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 message- waiting device directory number and partition is unique within the Cisco Unified Communications Manager cluster.
Calling Search Space	If partitions and calling search spaces are used, from the drop-down list box, choose a calling search space that includes the partitions of the DNs on all phones whose lamps you want to turn on (the partition that is defined for a phone DN must be in a calling search space that the MWI device uses). You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more 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 a calling search space name (see the About Calling Search Space Setup , on page 273). **Note** To set the maximum list box items, choose **System** > **Enterprise Parameters** and choose CCMAdmin Parameters.

Related Topics

Search for Partition , on page 270

Message Waiting Setup , on page 427



CHAPTER 64

Cisco Voice-Mail Pilot Setup

This chapter provides information on voice-mail pilot configuration.

For additional information, see topics related to the Voice Mail Connectivity to Cisco Unified Communications Manager in the *Cisco Unified Communications Manager System Guide*, as well as topics related to Cisco Unity and Cisco Unity connection.

About Voice-Mail Pilot Setup

In Cisco Unified Communications Manager Administration, use the **Advanced Features** > **Voice Mail** > **Voice Mail Pilot** menu path to configure voice-mail pilots.

The voice mail-pilot number designates the directory number that you dial to access your voice messages. Cisco Unified Communications Manager automatically dials the voice-messaging number when you press the Messages button on your phone. Each pilot number can belong to a different voice-messaging system.

Voice-Mail Pilot Number Deletion

To delete the voice-mail pilot number, perform these procedures. You cannot delete the default or the No Voice Mail profile numbers.

Note If you choose the default or the No Voice Mail pilot numbers, the Delete button does not display.

You cannot delete voice-mail pilot numbers that a voice-mail profile uses. To find out which voice-mail profiles are using the voice-mail pilot, in the Voice Mail Pilot Configuration window, choose Dependency Records from the Related Links drop-down list box and click Go. If the dependency records are not enabled for the system, the dependency records summary window displays a message. If you try to delete a voice-mail pilot that is in use, Cisco Unified Communications Manager displays a message. Before deleting a voice-mail pilot that is currently in use, you must perform either or both of the following tasks:

- Assign a different voice-mail pilot to any voice-mail profiles that are using the voice-mail pilot that you want to delete.
- Delete the voice-mail profiles that are using the voice-mail pilot that you want to delete.

If a voice-mail profile uses this voice-mail pilot number, a message displays and indicates the number of voice-mail profiles that use this voice-mail pilot number.

Related Topics

About Voice-Mail Profile Setup , on page 435
Voice-Mail Profile Deletion, on page 435
Access Dependency Records , on page 982

Voice-Mail Pilot Settings

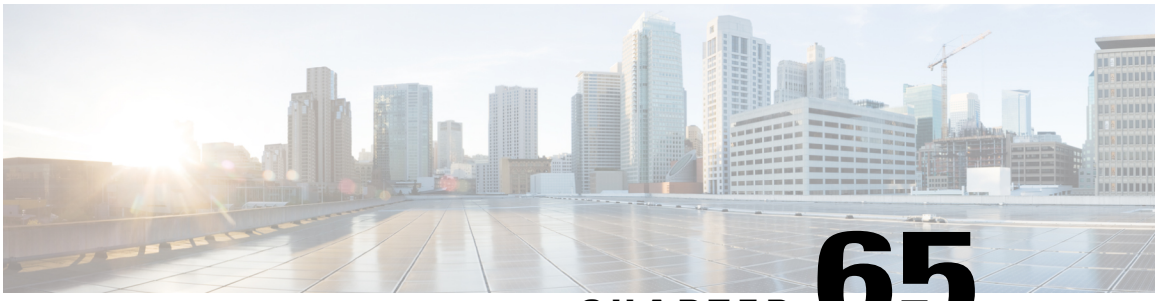
The following table describes the voice-mail pilot settings.

Table 75: Voice-Mail Pilot Settings

Field	Description
Voice Mail Pilot Number	Enter a number to identify the voice mail pilot number. Allowed characters are numeric (0-9), plus (+), asterisk (*), and pound (#). **Note** You cannot save the configuration if both the **Voice Mail Pilot Number** and **Calling Search Space** fields are empty. You must enter a value in one of the two fields.
Calling Search Space	From the drop-down list box, choose the appropriate calling search space. A calling search space comprises a collection of partitions that are searched for numbers that are called from this pilot number. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more 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, then find and choose a calling search space name. **Note** To set the maximum list box items, choose **System** > **Enterprise Parameters** and choose CCMAdmin Parameters.
Description	Enter the description of the pilot number. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), or angle brackets (<>).
Make this the default Voice Mail Pilot for the system	Check the check box to make this pilot number the default Voice Mail Pilot for the system. **Note** If you check the Default box, this voice mail pilot number replaces your current default pilot number.

Related Topics

About Calling Search Space Setup , on page 273
Cisco Voice-Mail Pilot Setup , on page 431



CHAPTER 65

Voice-Mail Profile Setup

This chapter provides information about voice-mail profile configuration.

For additional information, see topics related to the Voice Mail Connectivity to Cisco Unified Communications Manager in the *Cisco Unified Communications Manager System Guide*, as well as topics related to Cisco Unity and Cisco Unity connection.

About Voice-Mail Profile Setup

In Cisco Unified Communications Manager Administration, use the **Advanced Features** > **Voice Mail** > **Voice Mail Profile** menu path to configure voice-mail profiles.

The Voice Mail Profile Configuration window of Cisco Unified Communications Manager Administration allows you to define any line-related voice-messaging information.

Voice-mail Profiles Configuration Tips

A voice-mail profile gets assigned to a directory number, not to a device.

Related Topics

Synchronize Voice-Mail Profile with Devices , on page 437

Voice-Mail Profile Deletion

You cannot delete the default profile or the No Voice Mail profile.

You cannot delete a voice-mail profile that a directory number uses. To find out which directory numbers are using the voice-mail profiles, in the Voice Mail Profile Configuration window, choose Dependency Records from the Related Links drop-down list box and click Go. If the dependency records are not enabled for the system, the dependency records summary window displays a message. If you try to delete a voice-mail profile

that is in use, Cisco Unified Communications Manager displays a message. Before deleting a voice-mail profile that is currently in use, you must perform either or both of the following tasks:

- Assign a different voice-mail profile to any devices that are using the voice-mail profile that you want to delete.
- Delete the devices that are using the voice-mail profile that you want to delete.

Related Topics

Access Dependency Records , on page 982

Voice-Mail Profile Settings

The following table describes the voice-mail profile settings.

Table 76: Voice Mail Profile Settings

Field	Description
Voice Mail Profile Information	
Voice Mail Profile Name	Enter a name to identify the voice-mail profile. Valid characters comprise alphanumeric characters (a-z, A-Z, 0-9), period(.), dash(-), underscore(_).
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 (&), back-slash (\), angle brackets (<>), dollar sign ($), single-quote('), open paren [(], close paren [)], slash (/), colon (:), semi-colon (;), equal sign (=), at sign (@), tilde (~), brackets ({ }), or apostrophe (').
Voice Mail Pilot	Choose the appropriate voice-mail pilot number that is defined in the Voice Mail Pilot Configuration or Use Default.
Voice Mail Box Mask	Specify the mask that is used to format the voice mailbox number for auto-registered phones. When a call is forwarded to a voice-messaging system from a directory line on an auto-registered phone, Cisco Unified Communications Manager applies this mask to the number that is configured in the Voice Mail Box field for that directory line. For example, if you specify a mask of 972813XXXX, the voice mailbox number for directory number 7253 becomes 9728137253. If you do not enter a mask, the voice mailbox number matches the directory number (7253 in this example). By default, Cisco Unified CM sets the voice mailbox number to the same value as the directory number. You can change the voice mailbox number when you are configuring the directory number. **Note** When a call gets redirected from a DN to a voice-mail server/service that is integrated with Cisco Unified CM using a SIP trunk, the voice mailbox mask on the voice-mail profile for the phone modifies the diverting number in the SIP diversion header. This behavior is expected because the diversion header gets used by the Cisco Unified CM server to choose a mailbox.

Field	Description
Make This the Default Voice Mail Profile for the System	Check the check box to make this profile name the default. **Note** If you check the Default check box, this voice-mail profile replaces your current default profile.

Related Topics

Directory Number Setup , on page 289
Voice-Mail Profile Setup , on page 435

Synchronize Voice-Mail Profile with Devices

To synchronize devices with a voice mail profile that has undergone configuration changes, perform the following procedure, which applies 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 **Advanced Features** > **Voice Mail** > **Voice Mail Profile**.
The Find and List Voice Mail Profiles window displays.

Step 2 Choose the search criteria to use.

Step 3 Click Find.
The window displays a list of voice mail profiles that match the search criteria.

Step 4 Click the voice mail profile to which you want to synchronize applicable devices. The Voice Mail Profile Configuration screen displays.

Step 5 Make any additional configuration changes.

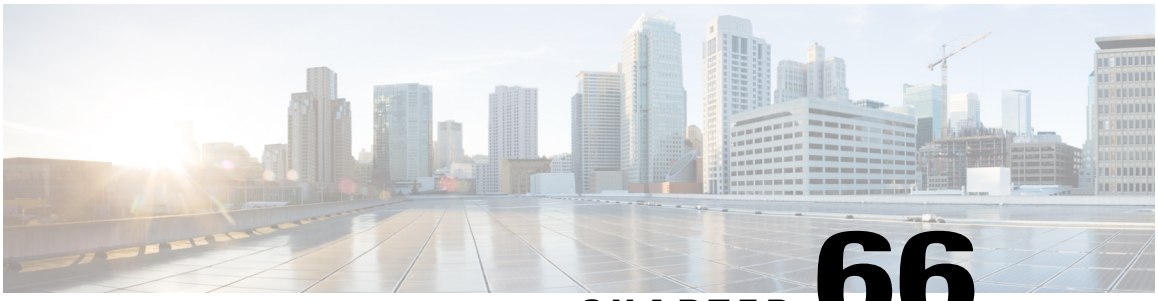
Step 6 Click Save.

Step 7 Click Apply Config.
The Apply Configuration Information dialog displays.

Step 8 Click OK.

Related Topics

Voice-Mail Profile Setup , on page 435



CHAPTER 66

Call Control Agent Profile Setup

This chapter provides information on configuring call control agent profiles.

- Call Control Agent Profile Settings, page 439

Call Control Agent Profile Settings

Note When you associate a Call Control Agent (CCA) profile to a directory number and if ESN and E164 masks are configured on that directory number, then the directory number will be synchronized to the corresponding fields in the external LDAP server that you have configured.

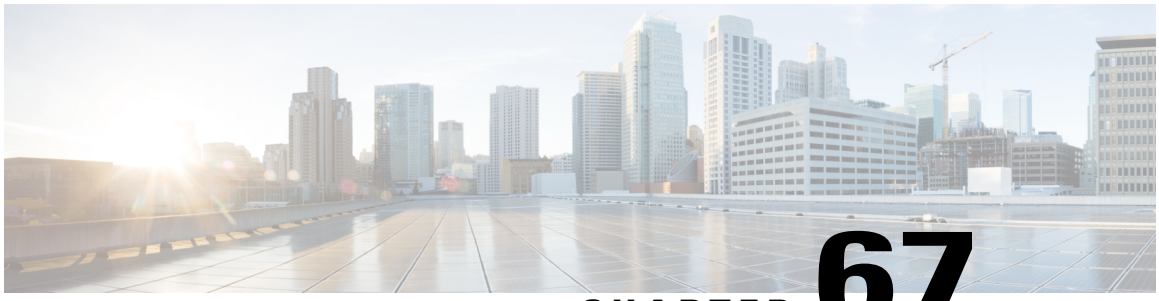
Note Any changes you make to the CCA profile are reflected in the corresponding directory number entries in the LDAP server, that are associated with that profile.

The following table describes the Call Control Agent Profile settings.

Table 77: Call Control Agent Profile Settings

Field	Description
Call Control Agent Profile Configuration	
Call Control Agent Profile ID	Enter the Call Control Agent Profile ID.
Primary Softswitch ID	Enter the primary softswitch ID.
Secondary Softswitch ID	Enter the secondary softswitch ID.
Object Class	Enter the object class name to be synchronized to the external directory server.
Subscriber Type	Enter the subscriber type.

Field	Description
SIP Alias Suffix	Enter the SIP alias suffix. The E.164 number that you specify for the directory number is appended to this suffix.
SIP User Name Suffix	Enter the SIP user name suffix.



CHAPTER 67

About Directory Number Alias Lookup and Sync Setup

In Cisco Unified Communications Manager Administration, use the submenus under the **Advanced Features** > **Directory Number Alias Lookup/Sync** menu path to configure directory number alias lookup and sync servers.

The Directory Number Alias Lookup and Sync setup enables you to route the commercial calls to an alternate number. Routing the commercial calls to an alternate number reduces the commercial cost of calling an external number. You must configure the LDAP server for Directory Number Alias Sync (sync server) if you need to synchronize users from Cisco Unified Communications Manager database to the sync server. You must configure the LDAP server for Directory Number Alias Lookup (lookup server) if you need to route the commercial calls to an alternate number.

- Directory Number Alias Lookup and Sync Settings , page 441
- Configure Directory Number to Synchronize to LDAP Directory Server , page 444
- Access Cisco Directory Number Alias Lookup Service Over HTTPS Connection Using Self-signed Certificate , page 444
- Access Cisco Directory Number Alias Lookup Service Over HTTPS Connection Using CA Signed Certificate , page 445

Directory Number Alias Lookup and Sync Settings

In Cisco Unified Communications Manager Administration, use the submenus under the **Advanced Features** > **Directory Number Alias Lookup/Sync** menu path to configure directory number alias lookup and sync servers.

The following table describes the Directory Number Alias Lookup/Sync settings.

Table 78: Directory Number Alias Lookup/Sync Settings

Field	Description
LDAP Directory Information	

Field	Description
LDAP Configuration Name	Enter a unique name (up to 40 characters) for the LDAP directory.
LDAP Manager Distinguished Name	Enter the user ID (up to 128 characters) of the LDAP Manager, who is an administrative user that has access rights to the LDAP directory in question.
LDAP Password	Enter a password (up to 128 characters) for the LDAP Manager.
Confirm Password	Reenter the password that you provided in the LDAP Password field.
LDAP User Search Base	Enter the location (up to 256 characters) where all LDAP users exist. This location acts as a container or a directory. This information varies depending on customer setup.
LDAP Directory Server Usage	Specify if the LDAP directory server should be used as: • Directory Number Alias Sync and Lookup • Directory Number Alias Sync Only • Directory Number Alias Lookup Only By default, Directory Number Alias Sync and Lookup option is selected. If you choose the *Directory Number Alias Sync and Lookup* option, you cannot add another sync or lookup server.
Directory Number Alias Server Configuration	
Keepalive Search User Distinguished Name	Enter the user ID (up to 128 characters) of the administrative user for which you need to perform the keepalive search and to determine connectivity to server. **Note** If this field is left blank, then the connectivity to the server is determined based on whether the LDAP bind request to the server is successful.
Keepalive Time Interval in Minutes	Specify the time interval at which keepalive messages should be sent to lookup/sync servers to check if those servers are active or not. For example, if you specify the keepalive time interval as 10 minutes and select the LDAP directory server as *DN Alias Lookup only*, keepalive messages will be sent every 10 minutes to all the lookup servers that are configured. If you specify the keepalive time interval as zero, the keepalive messages are not sent to the lookup servers.
SIP Alias Suffix	Enter the SIP alias suffix. The SIP Alias Suffix that you specify is appended to the E.164 directory number. This field is used by the DN Alias Lookup service only.

Field	Description
Enable Caching of Records for Directory Number Alias Lookup	Check this check box to enable caching of records for directory number alias lookup. If you check this check box, you can specify Record Cache Size for Directory Number Lookup Alias and Record Cache Age for Directory Number Alias Lookup in Hours. **Note** If you specify the LDAP directory server as a sync server, the system disables this check box. This field is enabled only if the Lookup server or both (Lookup and Sync) the servers are used as LDAP directory servers. If the Sync server is used as LDAP directory server, this field is disabled.
Record Cache Size for Directory Number Alias Lookup	Specify the number of records that should be cached. You can specify any number within a range of 3000-10000. **Note** This field is enabled only if 'Enable Caching of Records for Directory Number Alias Lookup' check box is checked.
Record Cache Age for Directory Number Alias Lookup in Hours	Specify the time for which the records should be held in the record cache. **Note** This field is enabled only if 'Enable Caching of Records for Directory Number Alias Lookup' check box is checked.
LDAP Server Information	
Host Name or IP Address for Server	Enter the host name or IP address of the server where the data for this LDAP directory resides.
Port	Specify the port number as 389. This is the port on which the LDAP routing database receives the LDAP requests. TLS is supported on this port.
Add Another Redundant LDAP Server	Click this button to add a redundant LDAP server.

Note To enable routing the commercial calls to the internal numbers of the called parties, ensure that Cisco Directory Number Alias Lookup Service is activated. To synchronize users from the Cisco Unified Communications Manager database to the LDAP server for Directory Number Alias Sync server, ensure that Cisco Directory Number Alias Sync Service is activated.

Note You can configure the primary and secondary lookup and sync servers to support failover. If a primary server goes down and if the secondary server is configured, lookup/sync services automatically connect to the secondary server. The failover is supported for both lookup and sync services. When the primary server is restored, the network administrator must restart the lookup/sync service so that the services can connect back to the primary server.

For more information on restarting services, refer *Cisco Unified Communications Manager Administration Guide*.

Note A commercial call is routed to an internal number only if Confidential Access Level (CAL) resolution succeeds on that call. If the CAL resolution fails, the call is redirected to the original destination.

Configure Directory Number to Synchronize to LDAP Directory Server

Procedure

Step 1 From Cisco Unified Communications Manager Administration, select **Call Routing** > **Directory Number**.

Step 2 Perform one of the following:

- Select **Add New** to create a new directory number.
- Open an existing directory number entry.

Step 3 Enter an E.164 mask.

Step 4 Enter an enterprise alternative number (EAN).

Step 5 Select a Call Control Agent Profile from the drop-down list box to create a new Call Control Agent Profile.

What to Do Next

Configure the LDAP server for Directory Number Alias Sync (sync server) if you need to synchronize directory numbers from the Unified Communications Manager database to the sync server.

Access Cisco Directory Number Alias Lookup Service Over HTTPS Connection Using Self-signed Certificate

To access Cisco Directory Number Alias Lookup service over https connection using a self-signed certificate, perform the following steps:

Procedure

Configure External Call Control (ECC) in any of the Cisco Unified Communication Manager clusters. Enter the web service URL as `https://<localhost>:8443/dnaliaslookup` or `https://<hostname of the CUCM>:8443/dnaliaslookup`.

Note The hostname is the Common Name (CN) of the tomcat certificate of Cisco Unified Communications Manager.

Access Cisco Directory Number Alias Lookup Service Over HTTPS Connection Using CA Signed Certificate

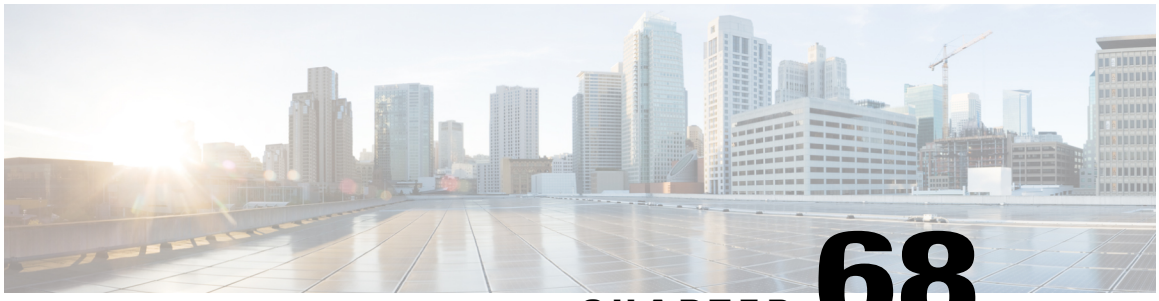
To access Cisco Directory Number Alias Lookup service over https connection using Certificate Authority (CA) signed certificate, perform the following steps:

Procedure

Step 1 Get the tomcat certificate of Cisco Unified Communications Manager signed by Certificate Authority (CA) and restart the tomcat service.

Step 2 Configure External Call Control (ECC) in any of the Cisco Unified Communication Manager clusters. Enter the web service URL as `https://<localhost>:8443/dnaliaslookup` or `https://<hostname of the CUCM>:8443/dnaliaslookup`.

Note The hostname is the Common Name (CN) of the tomcat certificate of Cisco Unified Communications Manager.



CHAPTER 68

Other Advanced Features Menu Options

This chapter provides brief descriptions of selected Advanced Features menu options. A pointer to the document that contains greater details for each Advanced Features menu option is provided.

SAF (Call Control Discovery)

In Cisco Unified Communications Manager Administration, use the submenus under the **Advanced Features** > **SAF** menu path to 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.

For more information, see the VPN Setup, on page 448 chapter in the Cisco Unified Communications Manager Features and Services Guide.

Cisco Extension Mobility Cross Cluster

In Cisco Unified Communications Manager Administration, use the submenus under the **Advanced Features** > **EMCC** menu path to configure the Cisco Extension Mobility Cross Cluster feature.

The Cisco Extension Mobility Cross Cluster feature 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.

For more information, see the *Cisco Unified Communications Manager Features and Services Guide*.

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.

Cisco Intercompany Media Engine

In Cisco Unified Communications Manager Administration, use the submenus under the**Advanced Features** > **Intercompany Media Services** menu path to configure the Cisco Intercompany Media Engine.

Cisco Intercompany Media Engine provides a technique for establishing direct IP connectivity between enterprises by combining peer-to-peer technologies with the existing public switched telephone network (PSTN) infrastructure. Cisco Intercompany Media Engine allows companies that have deployed Cisco Unified Communications Manager to communicate over the Internet rather than the PSTN by creating dynamic Session Initiation Protocol (SIP) trunks between the enterprises.

For more information, see the *Cisco Intercompany Media Engine Installation and Configuration Guide*.

Fallback Setup

In Cisco Unified Communications Manager Administration, use the submenus under the **Advanced Features** > **Fallback** menu path to configure fallback information.

Cisco Intercompany Media Engine configuration comprises configuration of fallback information.

For more information, see the *Cisco Intercompany Media Engine Installation and Configuration Guide*.

Called Party Tracing

In Cisco Unified Communications Manager Administration, use the submenus under the **Advanced Features** > **Called Party Tracing** menu path to configure Called Party Tracing feature.

Called Party Tracing allows you to configure a directory number or list of directory numbers that you want to trace. You can request on-demand tracing of calls using the Session Trace Tool.

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

VPN Setup

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

In Cisco Unified Communications Manager Administration, use the submenus under the **Advanced Features** > **VPN** menu path to configure the VPN feature.

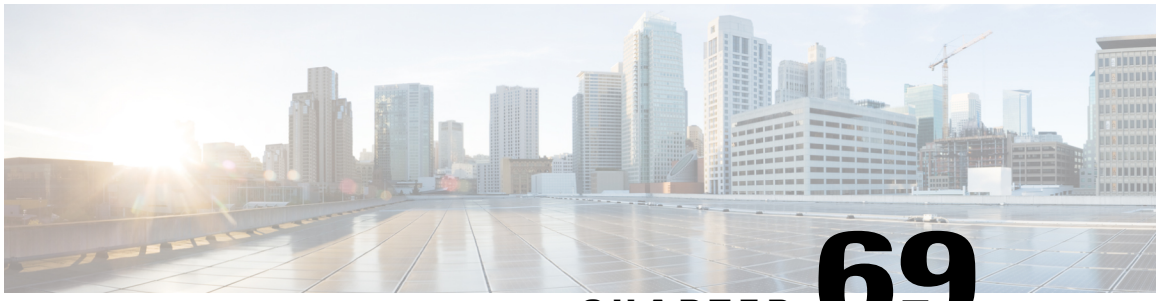
The Cisco VPN Client for Cisco Unified IP Phones adds another option for customers attempting to solve the remote telecommuter problem by complementing other Cisco remote telecommuting offerings.

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

PART VI

Device Setup

- SIP Normalization Script Setup , page 783
- Session Description Protocol Transparency, page 789
- Wireless LAN Profile Setup , page 793
- Wi-Fi Hotspot Profile Setup , page 801
- Other Device Menu Options , page 809



CHAPTER 69

CTI Route Point Setup

This chapter provides information to configure CTI route points and CTI ports.

For additional information, see topics related to computer telephony integration and trusted relay points in the *Cisco Unified Communications Manager System Guide*.

About CTI Route Point Setup

A computer telephony integration (CTI) route point designates a virtual device that can receive multiple, simultaneous calls for application-controlled redirection.

For first-party call control, you can optionally add a CTI port for each active voice line (the CTI application determines this). Applications that use CTI route points and CTI ports include Cisco IP Softphone, Cisco Unified Communications Manager Auto-Attendant, and Cisco IP Interactive Voice Response System. After you add a CTI route point to Cisco Unified Communications Manager Administration, information from the RIS Data Collector service displays in the CTI Route Point Configuration window. When available, the IP address of the device and the name of the Cisco Unified Communications Manager with which the device registered display.

Note You must not associate CTI route points with directory numbers (DNs) that are members of line groups and, by extension, that are members of hunt lists. If a DN is a member of a line group or hunt list, you cannot associate that DN with a CTI route point that you configure with the CTI Route Point Configuration window.

For detailed instructions on how to configure CTI route points and CTI ports that are associated with these applications, see the documentation and online help that is included with these applications.

CTI Route Point Setup

In Cisco Unified Communications Manager Administration, use the **Device** > **CTI Route Point** menu path to configure CTI route points.

A computer telephony integration (CTI) route point designates a virtual device that can receive multiple, simultaneous calls for application-controlled redirection.

For first-party call control, you can optionally add a CTI port for each active voice line (the CTI application determines this). Applications that use CTI route points and CTI ports include Cisco IP Softphone, Cisco Unified Communications Manager Auto-Attendant, and Cisco IP Interactive Voice Response System. After you add a CTI route point to Cisco Unified Communications Manager Administration, information from the RIS Data Collector service displays in the CTI Route Point Configuration window. When available, the IP address of the device and the name of the Cisco Unified Communications Manager with which the device registered display.

Note You must not associate CTI route points with directory numbers (DNs) that are members of line groups and, by extension, that are members of hunt lists. If a DN is a member of a line group or hunt list, you cannot associate that DN with a CTI route point that you configure with the CTI Route Point Configuration window.

For detailed instructions on how to configure CTI route points and CTI ports that are associated with these applications, see the documentation and online help that is included with these applications.

CTI Route Point Configuration Tips

After you add a CTI route point to Cisco Unified Communications Manager Administration, information from the RIS Data Collector service displays in the CTI Route Point Configuration window. When available, the device IP address and the name of the Cisco Unified Communications Manager with which the device registered display.

You can add and configure directory numbers for a CTI route point.

For instructions on how to reset a CTI route point, see the descriptions of the Reset Selected and Reset buttons.

Related Topics

GUI Buttons and Icons , on page 19
About Directory Number Setup , on page 289
Synchronize CTI Route Point , on page 458

CTI Route Point Deletions

Because you can delete a CTI route point that is assigned to one or more directory numbers, you should determine which directory numbers are using the CTI route point. To determine which directory numbers are using the CTI route point, choose Dependency Records link from the Related Links drop-down list box in the CTI Route Point Configuration window and click Go. If the dependency records are not enabled for the system, the dependency records summary window displays a message. If you try to delete a CTI route point that is in use, Cisco Unified Communications Manager displays a message.

If you delete a CTI Route Point that has a directory number assigned to it, you can find the directory number by using the Route Plan Report. You can also delete the directory number by using the Route Plan Report.

Related Topics

Access Dependency Records , on page 982

CTI Route Point Settings

The following table describes the CTI route point settings.

Table 79: CTI Route Point Settings

Field	Description
Device Name	Enter unique identifier for this device, from 1 to 15 characters, including alphanumeric, dot, dash, or underscores.
Description	Enter a descriptive name for the CTI route point. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
Device Pool	Choose the name of a Device Pool. The device pool specifies the collection of properties for this device, including Cisco Unified Communications Manager Group, Date/Time Group, Region, and Calling Search Space for auto-registration.
Common Device Configuration	Choose the common device configuration to which you want this CTI route point assigned. The common device configuration includes the attributes (services or features) that are associated with a particular user. Configure common device configurations in the Common Device Configuration window.
Calling Search Space	From the drop-down list box, choose a calling search space. The calling search space specifies the collection of partitions that are searched to determine how a collected (originating) number should be routed. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more 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, then find and choose a calling search space name. **Note** To set the maximum list box items, choose **System** > **Enterprise Parameters** and choose CCMAdmin Parameters.

Field	Description
Location	Use locations to implement call admission control (CAC) in a centralized call-processing system. CAC enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location. From the drop-down list box, choose the appropriate location for this CTI route point. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this CTI route point consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the **System** > **Location** menu option. For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*.
User Locale	From the drop-down list box, choose the locale that is associated with the CTI route point. The user locale identifies a set of detailed information to support users, including language and font. Cisco Unified Communications Manager makes this field available only for CTI route points 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 that information be displayed (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 Manager locale installer that is in the *Cisco Unified Communications Operating System Administration Guide*.
Media Resource Group List	Choose the appropriate Media Resource Group List. A Media Resource Group List comprises a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from the available media resources according to the priority order that is defined in a Media Resource Group List. If you choose <none>, Cisco Unified Communications Manager uses the Media Resource Group that is defined in the device pool. For more information, see topics related to media resource management in the *Cisco Unified Communications Manager System Guide*.
Network Hold MOH Audio Source	To specify the audio source that plays when the network initiates a hold action, click the drop-down arrow and choose an audio source from the list that displays. If you do not choose an audio source, Cisco Unified Communications Manager uses the audio source that is defined in the device pool or the system default if the device pool does not specify an audio source ID. You define audio sources in the Music On Hold Audio Source Configuration window. For access, choose **Media Resources** > **Music On Hold Audio Source**.

Field	Description
User Hold MOH Audio Source	To specify the audio source that plays when an application initiates a hold action, click the drop-down arrow and choose an audio source from the list that displays. If you do not choose an audio source, Cisco Unified Communications Manager uses the audio source that is defined in the device pool or the system default if the device pool does not specify an audio source ID. You define audio sources in the Music On Hold Audio Source Configuration window. For access, choose **Media Resources** > **Music On Hold Audio Source**.
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified Communications Manager inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values: • Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates. • Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified Communications Manager places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVPAgent). If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the *Cisco Unified Communications Manager System Guide* for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified Communications Manager first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified Communications Manager first tries to find a transcoder that is also designated as a TRP. See the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.

Field	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.
Geolocation	From the drop-down list box, choose a geolocation. You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation. You can also choose a geolocation that has been configured with the **System** > **Geolocation Configuration** menu option. For an explanation of geolocations, including configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocations, see the *Cisco Unified Communications Manager Features and Services Guide*.
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 CTI Route Point Configuration window.

Related Topics

Location Setup , on page 127
About Calling Search Space Setup , on page 273
CTI Route Point Setup , on page 453
Common Device Setup , on page 763

Synchronize CTI Route Point

To synchronize a CTI route point with the most recent configuration changes, perform the following procedure, which applies 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 **Device** > **CTI Route Point**.
The Find and List CTI Route Points window displays.

Step 2 Choose the search criteria to use.

Step 3 Click Find.

The window displays a list of CTI route points that match the search criteria.

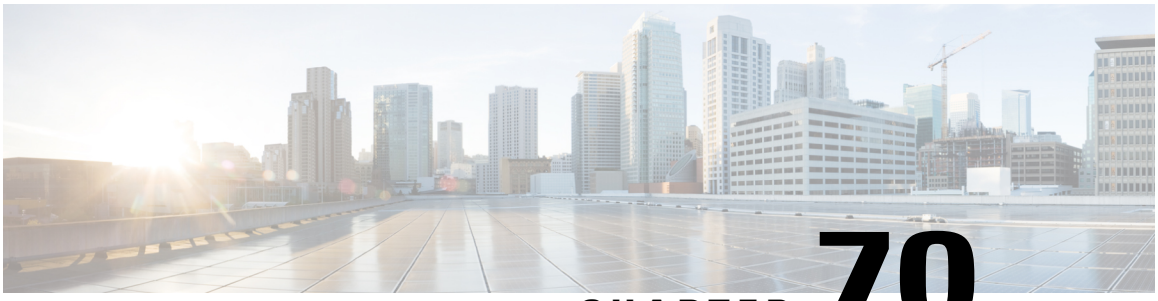
Step 4 Check the check boxes next to the CTI route points that you want to synchronize. To choose all CTI route points in the window, check the check box in the matching records title bar.

Step 5 Click Apply Config to Selected.
The Apply Configuration Information dialog displays.

Step 6 Click OK.

Related Topics

CTI Route Point Setup , on page 453



CHAPTER 70

Gatekeeper Setup

This chapter provides information about gatekeeper configuration using Cisco Unified Communications Manager Administration.

For additional information about gatekeepers and trunks, see the following Cisco documentation:

- *Cisco Unified Communications Manager System Guide*
- *Cisco Unified Communications Solution Reference Network Design (SRND)*
- Cisco IOS Multimedia Conference Manager (Command Reference) documentation

About Gatekeeper Setup

In Cisco Unified Communications Manager Administration, use the **Device** > **Gatekeeper** menu path to configure gatekeepers.

A gatekeeper device, also known as a Cisco Multimedia Conference Manager (MCM), supports the H.225 Registration, Admission, and Status Protocol (RAS) message set that is used for call admission control, bandwidth allocation, and dial pattern resolution (call routing). The gatekeeper provides these services for communications between Cisco Unified Communications Manager clusters and H.323 networks. You can configure multiple gatekeeper devices per Cisco Unified Communications Manager cluster. You can configure alternate gatekeepers for redundancy. See the Cisco Multimedia Conference Manager (MCM) documentation and the Cisco Unified Communications Solution Reference Network Design (SRND) for alternate gatekeeper configuration details.

Gatekeeper configuration comprises components:

- Cisco Unified Communications Manager configuration. Each Cisco Unified Communications Manager cluster can register with one or more gatekeepers. This chapter describes how to configure the gatekeeper

in Cisco Unified Communications Manager. You also need to configure trunk devices on the Trunk Configuration window.

- Gatekeeper configuration on the router. This type of configuration applies to a Cisco IOS Multimedia Conference Manager (MCM) that acts as the gatekeeper. Recommended platforms for the gatekeeper include Cisco 2600, 3600, or 7200 routers with Cisco IOS Release 12.1(3)T or higher. See the MCM documentation for information on configuring the gatekeeper. Alternate gatekeeper configuration occurs in the MCM only, so no configuration is necessary in Cisco Unified Communications Manager.

Note You can configure multiple gatekeeper devices per Cisco Unified Communications Manager cluster.

Gatekeepers Configuration Tips

You can configure multiple gatekeeper devices per Cisco Unified Communications Manager cluster.

Related Topics

Trunk Setup , on page 637

Gatekeeper Reset

Resetting a gatekeeper does not mean that the physical device is reset; instead, resetting forces the Cisco Unified Communications Manager to reset the logical connection to the gatekeeper and to reregister with the gatekeeper. During this time of reregistering and until successful registration, new calls that are made by using this trunk, which uses this gatekeeper, fail.

When you reset a gatekeeper, the Cisco Unified Communications Manager cluster unregisters (URQ) and then reregisters (RRQ) with the gatekeeper.

For instructions on how to reset a gatekeeper, see the descriptions of the Reset Selected and Reset buttons.

Note Resetting a gatekeeper does not cause all active calls that this gatekeeper controls to be dropped; however, new call attempts fail.

Related Topics

GUI Buttons and Icons , on page 19
Synchronize Gatekeeper , on page 464

Gatekeeper Deletions

You cannot delete a gatekeeper that is assigned to one or more trunks. To find out which trunks are using the gatekeeper, choose Dependency Records from the Related Links drop-down list box that is on the Gatekeeper 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. If you try to delete a gatekeeper that is in use, Cisco Unified Communications Manager displays an error message. Before deleting a gatekeeper that is currently in use, you must perform either or both of the following tasks:

- Assign a different gatekeeper to any trunks that are using the gatekeeper that you want to delete.
- Delete the trunks that are using the gatekeeper that you want to delete.

Related Topics

Set Up Trunk , on page 695
Delete Trunk , on page 697
Access Dependency Records , on page 982

Gatekeeper Settings

The following table describes the gatekeeper settings.

Table 80: Gatekeeper Settings

Field	Description
Gatekeeper Information	
Host Name/IP Address	Enter the IP address or host name of the gatekeeper in this required field. You can register multiple gatekeepers per Cisco Unified Communications Manager cluster.
Description	Enter a descriptive name for the gatekeeper. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
Registration Request Time to Live	Do not change this value unless a Cisco TAC engineer instructs you to do so. Enter the time in seconds. The default value specifies 60 seconds. The Registration Request Time to Live field indicates the time that the gatekeeper considers a registration request (RRQ) valid. The system must send a keepalive RRQ to the gatekeeper before the RRQ Time to Live expires. Cisco Unified Communications Manager sends an RRQ to the gatekeeper to register and subsequently to maintain a connection with the gatekeeper. The gatekeeper may confirm (RCF) or deny (RRJ) the request.
Registration Retry Timeout	Do not change this value unless a Cisco TAC engineer instructs you to do so. Enter the time in seconds. The default value specifies 300 seconds. The Registration Retry Timeout field indicates the time that Cisco Unified Communications Manager waits before retrying gatekeeper registration after a failed registration attempt.
Enable Device	This check box allows you to register this gatekeeper with Cisco Unified Communications Manager. By default, this check box remains checked. To unregister the gatekeeper from Cisco Unified Communications Manager gracefully, uncheck this check box. The gatekeeper unregisters within approximately 1 minute of updating this field.

Related Topics

Gatekeeper Setup , on page 461

Synchronize Gatekeeper

To synchronize a gatekeeper with the most recent configuration changes, perform the following procedure, which applies 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 **Device** > **Gatekeeper**.
The Find and List Gatekeepers window displays.

Step 2 Choose the search criteria to use.

Step 3 Click Find.
The window displays a list of gatekeepers that match the search criteria.

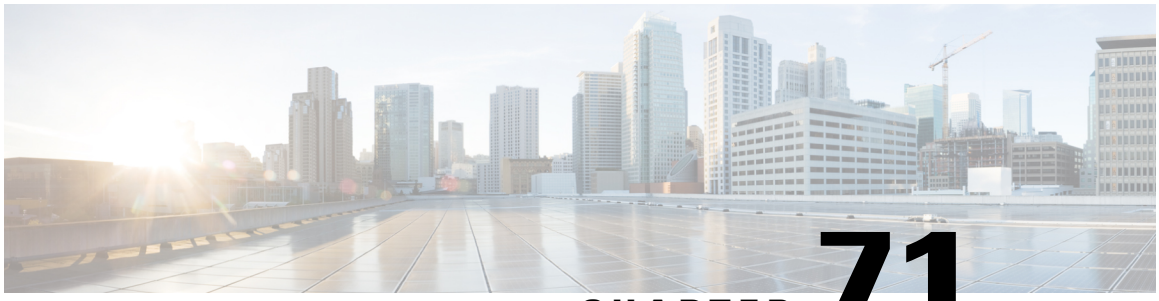
Step 4 Check the check boxes next to the gatekeepers that you want to synchronize. To choose all gatekeepers in the window, check the check box in the matching records title bar.

Step 5 Click Apply Config to Selected.
The Apply Configuration Information dialog displays.

Step 6 Click OK.

Related Topics

Gatekeeper Setup , on page 461



CHAPTER 71

Gateway Setup

This chapter provides information about using Cisco Unified Communications Manager for working with and configuring Cisco gateways.

About Gateway Setup

In Cisco Unified Communications Manager Administration, use the **Device** > **Gateway** menu path to configure gateways.

Cisco Unified Communications gateways enable Cisco Unified Communications Manager to communicate with non-IP telecommunications devices.

Related Topics

MGCP Gateway Settings , on page 467
H.323 Gateway Settings, on page 470
Analog Access Gateway Settings , on page 491
Cisco VG248 Gateway Settings , on page 496
Cisco IOS SCCP Gateway Settings , on page 497
Port Setup , on page 500
Add Gateway to Cisco Unified Communications Manager , on page 563

Gateway Reset

For instructions on how to reset a gateway, see the descriptions of the Reset Selected and Reset buttons.

Note Restarting or resetting an H.323 gateway does not physically restart/reset the gateway; it only reinitializes the configuration that was loaded by Cisco Unified Communications Manager. When you reset any other gateway type, Cisco Unified Communications Manager automatically drops the calls that are using the gateway. When you restart any other gateway type, Cisco Unified Communications Manager attempts to preserve the calls that are using the gateway.

Related Topics

GUI Buttons and Icons , on page 19
Synchronize Gateway , on page 576

Gateway Deletion

Gateways and ports use a variety of configuration information such as partitions, device pools, and directory numbers. Before updating or deleting gateways or ports, you can find configuration information about that gateway and port by using the Dependency Records link. To access the link, choose Dependency Records from the Related Links drop-down list box and click Go.

If you try to delete a gateway that a route group is using, Cisco Unified Communications Manager displays a message. To find out which route groups are using the gateway, choose Dependency Records from the Related Links drop-down list box in the Gateway Configuration window and click Go. If the dependency records are not enabled for the system, the dependency records summary window displays a message. Before deleting a gateway that is currently in use, you must perform either or both of the following tasks:

- Assign a different gateway to any route groups that are using the gateway that you want to delete.
- Delete the route groups that are using the gateway that you want to delete.

Note For each gateway type, the Gateway Configuration window displays either Device is trusted or Device is not trusted, along with a corresponding icon. The system determines whether the device is trusted, based on the device type. You cannot configure whether the device is trusted.

Related Topics

Route Group Deletion , on page 198
Add Devices to Route Group , on page 200
Dependency Records , on page 981
Access Dependency Records , on page 982

Cisco Unified Communications Gateway Settings

Cisco Unified Communications gateways enable Cisco Unified Communications Manager to communicate with non-IP telecommunications devices.

Note For each gateway type, the Gateway Configuration window displays either Device is trusted or Device is not trusted, along with a corresponding icon. The system determines whether the device is trusted, based on the device type. You cannot configure whether the device is trusted.

Related Topics

Port Setup , on page 500

MGCP Gateway Settings

The following table provides detailed descriptions for MGCP gateway configuration settings.

Table 81: MGCP Gateway Configuration Settings

Field	Description
Gateway Details	
Domain Name	Enter a name of up to 64 characters that identifies the Cisco MGCP gateway. Use the Domain Name Service (DNS) host name if it is configured to resolve correctly; otherwise, use the host name as defined on the Cisco MGCP gateway. If you are using the host name as it is configured on the IOS gateway, the name that you enter here must match exactly. For example, if the hostname is configured on the gateway to resolve to vg200-1 and the IP domain name is not configured, enter the hostname in this field (in this case, vg200-1). If the hostname is configured on the gateway as vg200-1 and the IP domain name is configured on the gateway as cisco.com, enter vg200-1.cisco.com in this field.
Description	Enter a description that clarifies the purpose of the device. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
Cisco Unified Communications Manager Group	From the drop-down list box, choose a Cisco Unified Communications Manager redundancy group. A Cisco Unified Communications Manager redundancy group includes a prioritized list of up to three Cisco Unified Communications Managers. The first Cisco Unified Communications Manager in the list serves as the primary Cisco Unified Communications Manager. If the primary Cisco Unified Communications Manager is not available or fails, the gateway attempts to connect with the next Cisco Unified Communications Manager in the list and so on.

Field	Description
Configured Slots, VICs, and Endpoints	
Note	You must specify the beginning port number for some VICs. For example, if the VIC in Subunit 0 begins at 0 and has two ports (0 and 1), the VIC in Subunit 1 must begin at a port number greater than 1 and have two ports (2 and 3 or 4 and 5). The correct number of slots displays for each model of MGCP gateway. (The VG200 gateway has only one slot.) To begin configuring ports on a module, select the module first; then, click Save.

Field	Description
Module in Slot 0 Module in Slot 1 Module in Slot 2 Module in Slot 3 (and so on)	For each available slot on the MGCP gateway, choose the type of module that is installed; for example: • NM-1V—Has one voice interface card (VIC) in Subunit 0 for FXS or FXO. When you use the VIC-2BRI-S/T-TE card with a NM-1V module, you can make two calls because the second BRI port is shut down. • NM-2V—Has two VICs, one in Subunit 0 and one in Subunit 1 for either FXS or FXO. When you use the VIC-2BRI-S/T-TE card with a NM-2V module, you can make four calls. If another VIC is in the second slot of the NM-2V, the second port on the VIC-2BRI-S/T-TE gets shut down. • NM-HDV—Has one VIC in Subunit 0 for either T1-CAS or T1-PRI, or E1-PRI. • NM-HDA—Has three VICs, one in Subunit 0, one in Subunit 1, and one in Subunit 2. • VWIC-SLOT—Has a slot for any of the following modules: VIC (FXS, FXO, or BRI), T1-CAS, T1-PRI, or E1-PRI. • AIM-VOICE-30—Has two VICs, one in Subunit 0 and one in Subunit 1 for T1-CAS, T1-PRI, or E1-PRI. • WS-X6600-24FXS—Has 24 FXS ports. • WS-X6600-6T1—Has six ports for T1 PRI or CAS. • WS-X6600-6E1—Has six ports for E1 PRI. • WS-SVC-CMM-MS—Has two port adapters, one for a T1 interface and one for an E1 interface for Europe and other countries. • None—Has no network modules installed. If you configure the Cisco 881 or the Cisco 888/887/886 for MGCP in the Gateway Configuration window, choose the following options when you configure the subunits: For Cisco 881 • Subunit 1 - VIC3-4FXS-DID • Subunit 3 - VIC2-1FXO For Cisco 888/887/886 • Subunit 1 - VIC3-4FXS-DID • Subunit 2 - VIC2-1BRI
Product-Specific Configuration	

Field	Description
Model-specific configuration fields defined by the gateway manufacturer	The gateway manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the "?" information icon to the right of the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, see the documentation for the specific gateway that you are configuring or contact the manufacturer.

H.323 Gateway Settings

Note After a gateway is registered with Cisco Unified Communications Manager, gateway registration status may display in Cisco Unified Communications Manager Administration as unknown.

The following table lists configuration settings for H.323 gateways.

Table 82: H.323 Gateway Configuration Settings

Field	Description
Device Information	
Device Name	Enter a unique name that Cisco Unified Communications Manager uses to identify the device. Use either the IP address or the host name as the device name.
Description	Enter a description that clarifies the purpose of the device. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
Device Pool	From the drop-down list box, choose the appropriate device pool. The device pool specifies a collection of properties for this device including Communications Manager Group, Date/Time Group, Region, and Calling Search Space for auto-registration of devices.
Common Device Configuration	From the drop-down list box, choose the common device configuration you want to use for this gateway. The common device configuration determines softkey template, MOH, and MLPP settings.

Field	Description
Call Classification	This parameter determines whether an incoming call that is using this gateway is considered off the network (OffNet) or on the network (OnNet). When the Call Classification field is configured as Use System Default, the setting of the Cisco Unified Communications Manager clusterwide service parameter, Call Classification, determines whether the gateway is OnNet or OffNet. This field provides an OnNet or OffNet alerting tone when the call is OnNet or OffNet, respectively.
Media Resource Group List	This list provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, among the available media resources according to the priority order that a Media Resource Group List defines.
Packet Capture Mode	Configure this field only when you need to troubleshoot encrypted signaling information for the H.323 gateway. Configuring packet capturing may cause call-processing interruptions. For more information on this field, see the *Cisco Unified Communications Manager Security Guide* .
Packet Capture Duration	Configure this field only when you need to troubleshoot encrypted signaling information for the H.323 gateway. Configuring packet capturing may cause call-processing interruptions. For more information on this field, see the *Cisco Unified Communications Manager Security Guide* .
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 box, choose the appropriate location for this device. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this device consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the **System** > **Location** menu option. For an explanation of location-based CAC across intercluster trunks, see topics related to location configuration in the *Cisco Unified Communications Manager System Guide* .
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.

Field	Description
Tunneled Protocol	Choose the QSIG option if you want to use H.323 gateways to transport (tunnel) non-H.323 protocol information in H.323 signaling messages from Cisco Unified Communications Manager to other Annex M.1-compliant H.323 PINXs. QSIG tunneling supports the following features: Call Completion, Call Diversion, Call Transfer, Identification Services, Message Waiting Indication, and Path Replacement. **Note** See the *Cisco Unified Communications Manager Software Compatibility Matrix* for information about Annex M.1 feature compatibility with third-party vendor(s).
QSIG Variant	To display the options in the QSIG Variant drop-down list box, choose QSIG from the Tunneled Protocol drop-down list box. This parameter specifies the protocol profile that is sent in outbound QSIG facility information elements. From the drop-down list box, choose one of the following options. Keep this parameter set to the default value unless a Cisco support engineer instructs otherwise. • No Changes • Not Selected • ECMA—If the QSIG Variant is set to ECMA (Protocol Profile 0x91), ensure that the ASN.1 Rose OID Encoding service parameter is set to Use Global Value (ECMA). • ISO—(Default) If the QSIG Variant is set to ISO (Protocol Profile 0x9F), ensure that the ASN.1 Rose OID Encoding service parameter is set to either Use Local Value or Use Global Value (ISO). For more information, see the following information: • Be aware that the QSIG Variant can also be defined as a clusterwide parameter. • For information on QSIG support with Cisco Unified Communications Manager, see the *Cisco Unified Communications Manager System Guide* .

Field	Description
ASN.1 ROSE OID Encoding	To display the options in the ASN.1 ROSE OID Encoding drop-down list box, choose QSIG from the Tunneled Protocol drop-down list box. This parameter specifies how to encode the Invoke Object ID (OID) for remote operations service element (ROSE) operations. From the drop-down list box, choose one of the following options: • No Changes. • Not Selected • Use Global Value (ISO)—Select this option only if the connected PBX does not support Local Value. • Use Global Value (ECMA)—Select this option only if the QSIG Variant service parameter is set to ECMA (Protocol Profile 0x91). • Use Local Value—(Default) Use this option that is supported by most telephony systems when the QSIG Variant service parameter is set to ISO (Protocol Profile 0x9F). For more information, see the following information: • Be aware that ASN.1 ROSE OID Encoding can also be defined as a clusterwide parameter. • For information on QSIG support with Cisco Unified Communications Manager, see the *Cisco Unified Communications Manager System Guide* .

Field	Description
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values: • Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates. • Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified Communications Manager places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVPAgent). If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the *Cisco Unified Communications Manager System Guide* for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified Communications Manager first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified Communications Manager first tries to find a transcoder that is also designated as a TRP. See the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.
Signaling Port	This field applies only to H.323 devices. The value designates the H.225 signaling port that this device uses. Default value specifies 1720. Valid values range from 1 to 65535.
Media Termination Point Required	If you want a Media Termination Point to implement features that H.323 does not support (such as hold and transfer), check the check box. Use this check box only for H.323 clients and H.323 devices that do not support the H.245 Empty Capabilities Set message. If you check this check box to require an MTP and this device becomes the endpoint of a video call, the call will be audio only.

Field	Description
Retry Video Call as Audio	This check box applies only to video endpoints that receive a call. By default, the system checks this check box to specify that this device should immediately retry a video call as an audio call (if it cannot connect as a video call) prior to sending the call to call control for rerouting. If you uncheck this check box, a video call that fails to connect as video does not try to establish as an audio call. The call then fails to call control. Call control reroutes the call within the route/hunt list. If Automatic Alternate Routing (AAR) is configured and enabled, call control also reroutes the call between route/hunt lists.
Wait for Far End H.245 Terminal Capability Set	This field applies only to H.323 devices. By default, system checks this check box to specify that Cisco Unified Communications Manager needs to receive the far-end H.245 Terminal Capability Set before it sends its H.245 Terminal Capability Set. Unchecking this check box specifies that Cisco Unified Communications Manager should initiate capabilities exchange. **Note** Uncheck this check box to allow calls through H.320 gateways for ISDN calls to and from other H.323 and H.320 endpoints.
Path Replacement Support	This check box displays if you choose the QSIG option from the Tunneled Protocol drop-down list box. This setting works with QSIG tunneling (Annex M.1) to ensure that non-H.323 information gets sent on the leg of the call that uses path replacement. **Note** The default setting leaves the check box unchecked. When you choose the QSIG Tunneled Protocol option, the system automatically checks the check box.
Transmit UTF-8 for Calling Party Name	This device uses the user locale setting of the device pool of the device to determine whether to send unicode and whether to translate received unicode information. For the sending device, if you check this check box and the user locale setting in the device pool of the device matches the terminating phone user locale, the device sends unicode. If the user locale settings do not match, the device sends ASCII. The receiving device translates incoming unicode characters based on the user locale setting of the sending device pool of the device. If the user locale setting matches the terminating phone user locale, the phone displays the characters. **Note** The phone may display junk characters if the two ends of the trunk configure user locales that do not belong to the same language group.
SRTP Allowed	Check the SRTP Allowed check box if you want Cisco Unified Communications Manager to allow secure and nonsecure calls over the gateway. If you do not check this check box, Cisco Unified Communications Manager prevents SRTP negotiation with the gateway and uses RTP. **Caution** If you check this check box, Cisco strongly recommends that you configure IPSec, so you do not expose keys and other security-related information during call negotiations. If you do not configure IPSec correctly, signaling between Cisco Unified Communications Manager and the gateway is nonsecure. For more information on encryption for gateways, see the *Cisco Unified Communications Manager Security Guide* .

Field	Description
H.235 Pass Through Allowed	This feature allows Cisco Unified Communications Manager to transparently pass through the shared secret (Diffie-Hellman key) and other H.235 data between two H.235 endpoints, so the two endpoints can establish a secure media channel. To allow H.235 pass through, check the check box.
Multilevel Precedence and Preemption (MLPP) Information	
MLPP Domain	From the drop-down list box, choose an MLPP domain to associate with this device. If you leave the value <None>, this device inherits its MLPP domain from the value that was set for the device pool of the device. If the device pool does not have an MLPP Domain setting, this device inherits its MLPP domain from the value that was set for the MLPP Domain Identifier enterprise parameter.
MLPP Indication	This device type does not have this setting.
Confidential Access Level	Select the appropriate CAL value from the drop-down list box.
Confidential Access Level	Select the appropriate CAL value from the drop-down list box.
Confidential Access Level	Select the appropriate CAL value from the drop-down list box.
Call Routing Information - Inbound Calls	
Significant Digits	Significant digits represent the number of final digits that are retained on inbound calls. Use for the processing of incoming calls and to indicate the number of digits that are used to route calls coming into the device. Choose the number of significant digits to collect, from 0 to 32. Cisco Unified Communications Manager counts significant digits from the right (last digit) of the number called.
Calling Search Space	From the drop-down list box, choose the appropriate calling search space. A calling search space specifies the collection of Route Partitions that are searched to determine how a collected (originating) number should be routed. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more 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, then find and choose a calling search space name. **Note** To set the maximum list box items, choose **System** > **Enterprise Parameters** and choose CCMAdmin Parameters.

Field	Description
AAR Calling Search Space	Choose the appropriate calling search space for the device to use when it performs automated alternate routing (AAR). 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.
Prefix DN	Enter the prefix digits that are appended to the called party number on incoming calls. Cisco Unified Communications Manager adds prefix digits after first truncating the number in accordance with the Significant Digits setting. You can enter the international escape character +.
Redirecting Number IE Delivery—Inbound	Check this check box to accept the Redirecting Number IE in the incoming SETUP message to the Cisco Unified Communications Manager. (The UUIE part of the SETUP message includes the Redirecting Number IE.) Uncheck the check box to exclude the Redirecting Number IE. You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box.
Enable Inbound FastStart	Check this check box to enable the H.323 FastStart call connections on incoming calls. By default, the check box remains unchecked for the H.323 gateway. For intercluster calls, you must check the Enable Inbound FastStart check box on Cisco Unified Communications Manager servers in other clusters for the outbound FastStart feature to work. **Note** If you updated Cisco Communications Manager 3.3(2) servers in other clusters with support patch B, do not enable inbound FastStart because 3.3(2)spB does not support the inbound FastStart feature over intercluster trunks.
Connected Party Settings	
Connected Party Transformation CSS	This setting is applicable only for inbound Calls. This setting allows you to transform the connected party number that Cisco Unified Communications Manager sends in another format, such as a DID or E.164 number. This setting is applicable while sending connected number for basic call as well as sending connected number after inbound call is redirected. Cisco Unified Communications Manager includes the transformed number in the Connected Number Information Element (IE) of CONNECT and NOTIFY messages. Make sure that the Connected Party Transformation CSS that you choose contains the connected party transformation pattern that you want to assign to this device. **Note** If you configure the Connected Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Connected Party Transformation CSS in a non-null partition that is not used for routing.

Field	Description
Use Device Pool Connected Party Transformation CSS	To use the Connected 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 Connected Party Transformation CSS that you configured for this device in the Trunk Configuration window.
Call Routing Information - Outbound Calls	
Calling Party Selection	Any outbound call on a gateway can send directory number information. Choose which directory number is sent: • Originator—Send the directory number of the calling device. • First Redirect Number—Send the directory number of the redirecting device. • Last Redirect Number—Send the directory number of the last device to redirect the call. • First Redirect Number (External)—Send the directory number of the first redirecting device with the external phone mask applied. • Last Redirect Number (External)—Send the directory number of the last redirecting device with the external phone mask applied.
Calling Party Presentation	Choose whether you want the Cisco Unified Communications Manager to allow or restrict the display of the calling party phone number. Choose Default if you do not want to change calling line ID presentation. Choose Allowed if you want Cisco Unified Communications Manager to send “Calling Line ID Allowed” on outbound calls. Choose Restricted if you want Cisco Unified Communications Manager to send “Calling Line ID Restricted” on outbound calls. For more information about this field, see topics related to Calling Search Space configuration settings in the *Cisco Unified Communications Manager System Guide* .

Field	Description
Called party IE Number Type Unknown	Choose the format for the number type in called party directory numbers. Cisco Unified Communications Manager sets the called 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 called directory number to be encoded to a non-national type numbering plan. Choose one of the following options: • Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the directory number type. • Unknown—This option specifies that 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.
Calling party IE Number Type Unknown	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 type numbering plan. Choose one of the following options: • Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the directory number type. • Unknown—This option specifies that 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.

Field	Description
Called Numbering Plan	Choose the format for the numbering plan in called party directory numbers. Cisco Unified Communications Manager sets the called DN numbering plan. 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 PBXs by using routing as a non-national type number. Choose one of the following options: • Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the Numbering Plan in the directory number. • ISDN—Use when you are dialing outside the dialing plan for your country. • National Standard—Use when you are dialing within the dialing plan for your country. • Private—Use when you are dialing within a private network. • Unknown—This option specifies that the dialing plan is unknown.
Calling Numbering Plan	Choose the format for the numbering plan in calling party directory numbers. Cisco Unified Communications Manager sets the calling DN numbering plan. 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 PBXs by using routing as a non-national type number. Choose one of the following options: • Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the Numbering Plan in the directory number. • ISDN—Use when you are dialing outside the dialing plan for your country. • National Standard—Use when you are dialing within the dialing plan for your country. • Private—Use when you are dialing within a private network. • Unknown—This option specifies that the dialing plan is unknown.

Field	Description
Caller ID DN	Enter the pattern that you want to use for calling line ID, from 0 to 24 digits. For example, in North America • 555XXXX = Variable calling line ID, where X equals an extension number. The CO appends the number with the area code if you do not specify it. • 5555000 = Fixed calling line ID. Use when you want the Corporate number to be sent instead of the exact extension from which the call is placed. The CO appends the number with the area code if you do not specify it. You can also enter the international escape character +.
Display IE Delivery	Check the check box to enable delivery of the display IE in SETUP, CONNECT, and NOTIFY messages for the calling and called party name delivery service.
Redirecting Party Transformation CSS	This setting allows you to transform the redirecting party number on the device to another format such as DID or E164 format. Cisco Unified Communications Manager includes the transformed number in the Redirecting Number Information Element of H.323 setup message sent out of Cisco Unified Communications Manager. Make sure that the Redirecting Party Transformation CSS that you choose contains either the calling or called party transformation pattern that you want to assign to this H.323 gateway. **Note** If you configure the Redirecting Party Transformation CSS as None and also uncheck the Use Device Pool Redirecting Party CSS check box, the transformation does not match and does not get applied. Ensure that you configure the Redirecting Party Transformation CSS in a non-null partition that is not used for routing.
Use Device Pool Redirecting Party CSS	To use the Redirecting 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 Redirecting Party Transformation CSS that you configured in the H.323 Gateway Configuration window.
Redirecting Number IE Delivery—Outbound	Check this check box to indicate the first redirecting number and the redirecting reason of the call when the call is forwarded. (The UUIE part of the outgoing SETUP message from the Cisco Unified Communications Manager includes the Redirecting Number IE.) Uncheck the check box to exclude the first redirecting number and the redirecting reason. You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box.
Enable Outbound FastStart	Check this check box to enable the H.323 FastStart feature on outgoing calls. By default, the check box remains unchecked for the H.323 gateway or trunk. **Note** When you check the Enable Outbound FastStart check box, you must set the Media Termination Point Required, Media Resource Group Lists, and Codec for Outbound FastStart.

Field	Description
Codec For Outbound FastStart	Use the drop-down list box to choose the codec for use with the H.323 device for an outbound FastStart call: • G711 u-law 64K (default) • G711 a-law 64K • G723 • G729 • G729AnnexA • G729AnnexB • G729AnnexA-AnnexB **Note** When you check the Enable Outbound FastStart check box, you must choose the codec for supporting outbound FastStart calls. You may need to click Save prior to choosing the Codec For Outbound FastStart.
Called Party Transformation CSS	This setting allows you to send transformed called party number in SETUP message for outgoing calls. Make sure that the Called Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device. **Note** If you configure the Called Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Called Party Transformation CSS in a non-null partition that is not used for routing.
Use Device Pool Called Party Transformation CSS	To use the Called 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 Called Party Transformation CSS that you configured in the H.323 Gateway Configuration window.
Calling Party Transformation CSS	This setting allows you to send transformed calling party number in SETUP message for outgoing calls. Also when redirection occurs for outbound calls, this CSS will be used to transform the connected number sent from Cisco Unified Communications Manager side in outgoing NOTIFY messages. 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** 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.
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 H.323 Gateway Configuration window.
Geolocation Configuration	

Field	Description
Geolocation	From the drop-down list box, choose a geolocation. You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation. You can also choose a geolocation that has been configured with the **System** > **Geolocation Configuration** menu option. For an explanation of geolocations, including configuration details, see the *Cisco Unified Communications Manager Features and Services Guide* . For an overview and details of how logical partitioning uses geolocations, see the *Cisco Unified Communications Manager Features and Services Guide* .
Geolocation Filter	From the drop-down list box, choose a geolocation filter. If you leave the <None> setting, no geolocation filter gets applied for this device. You can also choose a geolocation filter that has been configured with the **System** > **Geolocation Filter** menu option. For an explanation of geolocation filters, including configuration details, see the *Cisco Unified Communications Manager Features and Services Guide* . For an overview and details of how logical partitioning uses geolocation filters, see the *Cisco Unified Communications Manager Features and Services Guide* .
Incoming Calling Party Settings	
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.

Field	Description
National Number	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 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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. • Strip Digits—Enter the number of digits, up to the number 24, 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—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 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. 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. **Tip** For more information on configuring these settings, see topics related to Calling Search Space configuration settings in the *Cisco Unified Communications Manager Features and Services Guide* .

Field	Description
International Number	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 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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. • Strip Digits—Enter the number of digits, up to the number 24, 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— 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 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. 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. **Tip** For more information on configuring these settings, see topics related to Calling Search Space configuration settings in the *Cisco Unified Communications Manager Features and Services Guide* .

Field	Description
Subscriber Number	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 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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. • Strip Digits—Enter the number of digits, up to the number 24, 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 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. 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. **Tip** For more information on configuring these settings, see topics related to Calling Search Space configuration settings in the *Cisco Unified Communications Manager Features and Services Guide* .

Field	Description
Unknown Number	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 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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. • Strip Digits—Enter the number of digits, up to the number 24, 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—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 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. 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. **Tip** For more information on configuring these settings, see topics related to Calling Search Space configuration settings in the *Cisco Unified Communications Manager Features and Services Guide* .
Incoming Called Party Settings The H.323 protocol does not support the international escape character +. To ensure the correct prefixes, including the +, get applied to inbound calls over H.323 gateways, configure the incoming called party settings; that is, configuring the incoming called party settings ensures that when an inbound call comes from a H.323 gateway, Cisco Unified Communications Manager transforms the called party number back to the value that was originally sent over the gateway.	
Clear Prefix Settings	To delete all prefixes for all called party number types, click Clear Prefix Settings.
Default Prefix Settings	To enter the default value for all prefix fields at the same time, click Default Prefix Settings.

Field	Description
National Number	Configure the following settings to transform incoming called party numbers that use National for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called party numbers that use National for the Called Party Numbering Type. You can enter up to 16 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, you cannot configure the Strip Digits field. 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 called party prefix, which supports both the prefix and strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, 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 called party number of National type before it applies the prefixes. • Use Device Pool CSS— 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 the device. • Calling Search Space—This setting allows you to transform the called party number of National called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

Field	Description
International Number	Configure the following settings to transform incoming called party numbers that use International for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called party numbers that use International for the Called Party Numbering Type. You can enter up to 16 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, you cannot configure the Strip Digits field. 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 called party prefix, which supports both the prefix and strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, 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 called party number of International type before it applies the prefixes. • Use Device Pool CSS—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 the device. • Calling Search Space—This setting allows you to transform the called party number of International called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

Field	Description
Unknown Number	Configure the following settings to transform incoming called party numbers that use Unknown for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called numbers that use Unknown for the Called Party Numbering Type. You can enter up to 16 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, you cannot configure the Strip Digits field. 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 called party prefix, which supports both the prefix and strip digit functionality. **Tip** To configure the Strip Digits field, 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 called party number of Unknown type before it applies the prefixes. • Use Device Pool CSS—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 the device. • Calling Search Space—This setting allows you to transform the called party number of Unknown called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

Field	Description
Subscriber Number	Configure the following settings to transform incoming called party numbers that use Subscriber for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called numbers that use Subscriber for the Called Party Numbering Type. You can enter up to 16 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, you cannot configure the Strip Digits field. 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 called party prefix, which supports both the prefix and strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, 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 called 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 transform the called party number of Subscriber called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

Related Topics

Service Parameter Setup , on page 151
About Calling Search Space Setup , on page 273
Gateway Setup , on page 465

Analog Access Gateway Settings

The following table lists configuration settings for Analog Access gateways (Cisco Catalyst 6000 24 port FXS Gateway).

Table 83: Analog Access Gateway Configuration Settings

Field	Description
Device Information	
MAC Address	Enter MAC address of the gateway. The MAC address uniquely identifies the hardware device. You must enter a 12-hexadecimal character value.
Description	Enter the purpose of the device. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
Device Pool	From the drop-down list box, choose the appropriate device pool. The device pool specifies a collection of properties for this device including Communications Manager Group, Date/Time Group, Region, and Calling Search Space for auto-registration of devices.
Common Device Configuration	From the drop-down list box, choose the common device configuration you want to use for this gateway. The common device configuration determines softkey template, MOH, and MLPP settings.
Media Resource Group List	This list provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from among the available media resources according to the priority order that a Media Resource Group List defines.
Calling Search Space	From the drop-down list box, choose the appropriate calling search space. The calling search space specifies a collection of partitions that are searched to determine how a collected (originating) number should be routed. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more 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, then find and choose a calling search space name. **Note** To set the maximum list box items, choose **System** > **Enterprise Parameters** and choose CCMAdmin Parameters.
AAR Calling Search Space	Choose the appropriate calling search space for the device to use when it performs automated alternate routing (AAR). 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.

Field	Description
Location	Use locations to implement call admission control (CAC) in a centralized call-processing system. CAC enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location. From the drop-down list box, choose the appropriate location for this device. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this device consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the **System** > **Location** menu option. For more details about locations, see the *Cisco Unified Communications Manager System Guide*.
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.
Network Locale	From the drop-down list box, choose the locale that is associated with the gateway. The network locale identifies a set of detailed information to support the hardware in a specific location. The network locale contains a definition of the tones and cadences that the device uses in a specific geographic area. **Note** 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. If the device is associated with a network locale that it does not support in the firmware, the device will fail to come up.

Field	Description
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified Communications Manager inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values: • Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates. • Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified Communications Manager places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVPAgent). If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the *Cisco Unified Communications Manager System Guide* for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified Communications Manager first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified Communications Manager first tries to find a transcoder that is also designated as a TRP. See the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.
Port Selection Order	Choose the order in which ports are chosen. If you are not sure which port order to use, choose Top Down: • Top Down—Selects ports in descending order, from port 1 to port 8. • Bottom Up—Selects ports in ascending order, from port 8 to port 1.
Load Information	Enter the appropriate firmware load information for the gateway. The value that you enter here overrides the default firmware load for this gateway type.

Field	Description
Transmit UTF-8 for Calling Party Name	This device uses the user locale setting of the device pool of the device to determine whether to send unicode and whether to translate received unicode information. For the sending device, if you check this check box and the user locale setting in the device pool of the device matches the terminating phone user locale, the device sends unicode. If the user locale settings do not match, the device sends ASCII. The receiving device translates incoming unicode characters based on the user locale setting of the device pool of the sending device. If the user locale setting matches the terminating phone user locale, the phone displays the characters. **Note** The phone may display junk characters if the two ends of the trunk configure user locales that do not belong to the same language group.
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.
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 Gateway Configuration window.
Multilevel Precedence and Preemption (MLPP) Information	
MLPP Domain	From the drop-down list box, choose an MLPP domain to associate with this device. If you leave the value <None>, this device inherits its MLPP domain from the value that was set for the device pool of the device. If the device pool does not have an MLPP Domain setting, this device inherits its MLPP Domain from the value that was set for the MLPP Domain Identifier enterprise parameter.
MLPP Indication	This device type does not have this setting.
MLPP Preemption	This setting does not have this device type.
Product-Specific Configuration	
Model-specific configuration fields that the gateway manufacturer defines	The gateway manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the "?" information icon to the right of the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, see the documentation for the specific gateway that you are configuring or contact the manufacturer.

Field	Description
Geolocation Configuration	
Geolocation	From the drop-down list box, choose a geolocation. You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation. You can also choose a geolocation that has been configured with the **System** > **Geolocation Configuration** menu option. For an explanation of geolocations, including configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocations, see the *Cisco Unified Communications Manager Features and Services Guide*.
Geolocation Filter	From the drop-down list box, choose a geolocation filter. If you leave the <None> setting, no geolocation filter gets applied for this device. You can also choose a geolocation filter that has been configured with the **System** > **Geolocation Filter** menu option. For an explanation of geolocation filters, including configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocation filters, see the *Cisco Unified Communications Manager Features and Services Guide*.

Related Topics

About Calling Search Space Setup , on page 273
Gateway Setup , on page 465

Cisco VG248 Gateway Settings

The following table lists configuration settings for the Cisco VG248 Gateways.

Table 84: Cisco VG248 Gateway Configuration Settings

Field	Description
MAC Address (Last 10 Characters)	Enter the last 10 digits of the Media Access Control (MAC) address for the Cisco VG248. Only one MAC address exists for the Cisco VG248 Analog Phone Gateway, but Cisco Unified Communications Manager requires unique MAC addresses for all devices. When only 10 digits of the MAC address are entered, Cisco Unified Communications Manager can use the MAC address for the gateway and append additional information to it to create the MAC addresses for the VGC phones. The conversion of the MAC address for each device occurs by adding the two-digit port number to the end of the MAC address (to the right of the number) and adding VGC at the beginning of the MAC address. `EXAMPLEMAC Address for the Cisco VG248 is 0039A44218 the MAC address for registered port 12 in Cisco Unified Communications Manager isVGC0039A4421812`
Description	Cisco Unified Communications Manager automatically provides this information by adding VGCGW immediately in front of the MAC address.
Load Information	Enter the firmware version for the Cisco VG248 that is being configured; otherwise, leave blank to use the default.
Configured Slots, VICs and Endpoints **Note** To begin configuring ports on a module, select the module first; then, click Save.	
48_PORTS	From the list of endpoint identifiers, choose one of the ports to configure the VGC_Phone ports.

Related Topics

Gateway Setup , on page 465

Cisco IOS SCCP Gateway Settings

The following table lists configuration settings for the Cisco IOS SCCP gateways.

Table 85: Cisco IOS SCCP Gateway Configuration Settings

Field	Description

MAC Address (last 10 Characters)	Enter the last 10 digits of the Media Access Control (MAC) address for the gateway. Use the MAC address of the interface that the sccp local IOS command specifies on the gateway. Valid characters include the digits 0 through 9 and the uppercase characters A through F.
	
	The conversion of the MAC address for each device occurs by adding the three-digit mapping of the slot/subunit/port to the end of the MAC address (to the right of the number).
	
	`EXAMPLEMAC Address for the gateway is 0006D7E5C7`
	`The MAC address in Cisco Unified Communications Manager is0006D7E5C7281 where 281 is the three-digit mapping of the slot/subunit/port.`
	`The values 2,8 and 1 can be hex digits and each do not necessarily correspond to slot, subunit and port values.`
	The system inserts the following two-character strings before the MAC address to indicate the phone device types:
	• BR—BRI phone
	• AN—Analog phone
	
	The system also inserts SKIGW for the gateway name.

Description	Cisco Unified Communications Manager automatically provides this information by adding SKIGW immediately in front of the MAC address. You can override the description.
Cisco Unified Communications Manager Group	From the drop-down list box, choose a Cisco Unified Communications Manager redundancy group. A Cisco Unified Communications Manager redundancy group includes a prioritized list of up to three Cisco Unified Communications Managers. The first Cisco Unified Communications Manager in the list serves as the primary Cisco Unified Communications Manager. If the primary Cisco Unified Communications Manager is not available or fails, the gateway attempts to connect with the next Cisco Unified Communications Manager in the list, and so on.
Configured Slots, VICS and Endpoints **Note** You must specify the beginning port number for some VICs. For example, if the VIC in Subunit 0 begins at 0 and has two ports (0 and 1), then the VIC in Subunit 1 must begin at a port number greater than 1 and have two ports (2 and 3 or 4 and 5). **Note** The correct number of slots displays for each model of SCCP gateway. **Note** To begin configuring ports on a module, select the module first; then, click Save.	

Field	Description
Module in Slot 0Module in Slot 1Module in Slot 2Module in Slot 3 (and so on)	For each available slot on the chosen SCCP gateway, choose the type of module that is installed. The system supports the following modules: Network Modules (with VIC slots): • NM-2V—Has two VICs, one in Subunit 0 and one in Subunit 1 for FXS-SCCP. • NM-HD-2V—Has two VIC slots, one in Subunit 0 and one in Subunit 1 for FXS-SCCP or for BRI-NT/TE-SCCP. • NM-HD-2VE—Has two VIC slots, one in Subunit 0 and one in Subunit 1 for FXS-SCCP or for BRI-NT/TE-SCCP Network Modules (no VIC slots): • NM-HDA-4FXS—Has 4 FXS directly without VIC and can be extended by up to two expansion modules EM-HDA-8FXS to support 16 FXS ports. • EM-HDA-8FXS—Expansion module for the NM-HDA-4FXS Voice Interface Cards: • VIC-2FXS • VIC-4FXS • VIC2-2FXS • VIC2-2BRI-NT/TE
	At the slot level, these options exist: • NM-2V—Two subunits with option VIC-2FXS-SCCP • NM-HD-2V—Two subunits with options VIC-4FXS-SCCP, VIC2-2FXS-SCCP, VIC2-2BRI-NT/TE-SCCP • NM-HD-2VE—Two subunits with options VIC-4FXS-SCCP, VIC2-2FXS-SCCP, VIC2-2BRI-NT/TE-SCCP • NM-HDA—Three subunits with options NM-HDA-4FXS-SCCP, EM-8FXS-EM0-SCCP, EM-8FXS-EM1-SCCP In NM-HDA, these options do not represent true VICs. The VIC2-2BRI-NT/TE represents the only VIC for BRI phones that are running SCCP. VG224 GW differs from all others. The following option supports only one slot: • ANALOG—One subunit option 24FXS-SCCP (supports 24 FXS ports) The option None means that no network modules are installed.
Product Specific Configuration	

Field	Description
Model-specific configuration fields defined by the gateway manufacturer	The gateway manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the "?" information icon to the right of the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, see the documentation for the specific gateway that you are configuring or contact the manufacturer.

Related Topics

Gateway Setup , on page 465

Port Setup

Tables that list detailed descriptions for all port type configuration fields are provided.

Related Topics

FXS/FXO Port Settings , on page 500
Digital Access PRI Port Settings , on page 507
Digital Access T1 Port Settings , on page 533
BRI Port Settings , on page 540
POTS Port Settings , on page 557
Loop-Start Port Settings , on page 559
Ground-Start Port Settings , on page 560
E and M Port Settings , on page 561

FXS/FXO Port Settings

The following table provides detailed descriptions for FXS/FXO port configuration settings.

Note For the VG200 gateway, not all switch emulation types support the network side. How you configure the gateway switch type determines whether you may or may not be able to set network side.

Table 86: FXS/FXO Port Configuration Settings

Field	Description
Device Information	

Field	Description
Description	Cisco Unified Communications Manager generates a string that uniquely identifies the analog MGCP description. For example: AALN/S0/SU1/1@domain.com You can edit this field.
Device Pool	From the drop-down list box, choose the appropriate device pool. The device pool specifies a collection of properties for this device including Communications Manager Group, Date and Time Group, Region, and Calling Search Space for auto registration of devices.
Media Resource Group List	This list provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from among the available media resources according to the priority order that is defined in a Media Resource Group List.
Packet Capture Mode (for Cisco IOS MGCP gateways only)	Configure this field only when you need to troubleshoot encrypted signaling information for the Cisco IOS MGCP gateway. Configuring packet capturing may cause call-processing interruptions. For more information on this field, see the Cisco Unified Communications Manager Security Guide.
Packet Capture Duration (for Cisco IOS MGCP gateways only)	Configure this field only when you need to troubleshoot encrypted signaling information for the Cisco IOS MGCP gateway. Configuring packet capturing may cause call-processing interruptions. For more information on this field, see the Cisco Unified Communications Manager Security Guide.
Calling Search Space	From the drop-down list box, choose the appropriate calling search space. A calling search space comprises a collection of route partitions that are searched to determine how a collected (originating) number should be routed. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more 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, then find and choose a calling search space name. **Note** To set the maximum list box items, choose **System** > **Enterprise Parameters** and enter a value for Max List Box Items in the CCMAdmin Parameters pane.
AAR Calling Search Space	Choose the appropriate calling search space for the device to use when it performs automated alternate routing (AAR). 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.

Field	Description
Location	Use locations to implement call admission control (CAC) in a centralized call-processing system. CAC enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location. From the drop-down list box, choose the appropriate location for this device. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this device consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the **System** > **Location** menu option. For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*.
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.
Network Locale	From the drop-down list box, choose the locale that is associated with the gateway. The network locale identifies a set of detailed information to support the hardware in a specific location. The network locale contains a definition of the tones and cadences that the device uses in a specific geographic area. **Note** Choose only a network locale that is already installed and that the associated devices support. The list contains all available network locales for this setting, but not all are necessarily installed. If the device is associated with a network locale that it does not support in the firmware, the device will fail to come up.

Field	Description
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified Communications Manager inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values: • Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates. • Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified Communications Manager places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVPAgent). If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the *Cisco Unified Communications Manager System Guide* for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified Communications Manager first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified Communications Manager first tries to find a transcoder that is also designated as a TRP. See the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.
Geolocation	From the drop-down list box, choose a geolocation. You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation. You can also choose a geolocation that has been configured with the **System** > **Geolocation Configuration** menu option. For an explanation of geolocations, including configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocations, see the *Cisco Unified Communications Manager Features and Services Guide*.

Field	Description
Transmit UTF-8 for Calling Party Name	This device uses the user locale setting of the device pool for the device to determine whether to send unicode and whether to translate received unicode information. For the sending device, if you check this check box and the user locale setting in the device pool for the device matches the terminating phone user locale, the device sends unicode. If the user locale settings do not match, the device sends ASCII. The receiving device translates incoming unicode characters based on the user locale setting of the sending device pool for the device. If the user locale setting matches the terminating phone user locale, the phone displays the characters. **Note** The phone may display junk characters if the two ends of the trunk configure user locales that do not belong to the same language group.
Enable Caller ID(for FXS ports)	To enable caller ID on this port, check this check box. Caller ID enables the port to report caller ID information, which can display on the destination phone when an incoming call arrives.
Ring Number(for FXS ports)	Enter the number of rings after which the port will answer an incoming call. The valid values are 1 or 2 rings. The default value is 1 ring.
Timing Guard-out	Enter the timing guard-out value, in milliseconds. This setting is a time window after a call is disconnected that no outgoing call is allowed. The range of valid values is 300 ms to 3000 ms. The default value is 1000 ms. Caller ID support requires a value of 1000 ms or less.
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.
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 Gateway Configuration window. This settings displays for FXS ports, not FXO ports.
Multilevel Precedence and Preemption (MLPP) Information	
MLPP Domain	From the drop-down list box, choose an MLPP domain to associate with this device. If you leave the value <None>, this device inherits its MLPP domain from the value set for the device pool for the device. If the device pool does not have an MLPP Domain setting, this device inherits its MLPP Domain from the value set for the MLPP Domain Identifier enterprise parameter.

Field	Description
MLPP Indication	Be aware that this setting is not available for all devices. If available, this setting specifies whether a device that can play precedence tones will use the capability when it places an MLPP precedence call. From the drop-down list box, choose a setting to assign to this device from the following options: • Default—This device inherits its MLPP indication setting from its device pool. • Off—This device does not handle nor process indication of an MLPP precedence call. • On—This device does handle and process indication of an MLPP precedence call. **Note** Do not configure a device with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful.
MLPP Preemption	Be aware that this setting is not available for all devices. If available, this setting specifies whether a device that can preempt calls in progress will use the capability when it places an MLPP precedence call. From the drop-down list box, choose a setting to assign to this device from the following options: • Default—This device inherits its MLPP preemption setting from its device pool. • Disabled—This device does not allow preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. • Forceful—This device allows preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. **Note** Do not configure a device with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful.
Port Information (POTS)	
Port Direction	Choose the direction of calls that are passing through this port: • Inbound—Use for incoming calls only. • Outbound—Use for outgoing calls. • Bothways—Use for inbound and outbound calls (default).
Prefix DN(for FXS ports)	Enter the prefix digits that are appended to the digits that this trunk receives on incoming calls. Cisco Unified Communications Manager adds prefix digits after first truncating the number in accordance with the Num Digits setting. You can enter the international escape character +.

Field	Description
Num Digits(for FXS ports)	Enter the number of significant digits to collect, from 0 to 32. Cisco Unified Communications Manager counts significant digits from the right (last digit) of the number called. Use this field for the processing of incoming calls and to indicate the number of digits starting from the last digit of the called number that is used to route calls coming into the PRI span. See Prefix DN.
Expected Digits(for FXS ports)	Enter the number of digits that are expected on the inbound side of the trunk. For this rarely used field, leave zero as the default value if you are unsure.
Unattended Port	Check this check box to indicate an unattended port on this device.
Product-Specific Configuration	
Model-specific configuration fields defined by the gateway manufacturer	The gateway manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the "?" information icon to the right of the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, see the documentation for the specific gateway that you are configuring or contact the manufacturer.
Geolocation Configuration	
Geolocation	From the drop-down list box, choose a geolocation. You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation. You can also choose a geolocation that has been configured with the **System** > **Geolocation Configuration** menu option. For an explanation of geolocations, including configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocations, see the *Cisco Unified Communications Manager Features and Services Guide*.
Geolocation Filter	From the drop-down list box, choose a geolocation filter. If you leave the <None> setting, no geolocation filter gets applied for this device. You can also choose a geolocation filter that has been configured with the **System** > **Geolocation Filter** menu option. For an explanation of geolocation filters, including configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocation filters, see the *Cisco Unified Communications Manager Features and Services Guide*.

Field	Description
Incoming Calling Party Settings	
Clear Prefix Settings	To delete all prefixes for all calling party number types, click Clear Prefix Settings.
Default Prefix Settings	To enter the default value for all prefix fields at the same time, click Default Prefix Settings.
Strip Digits	Enter the number of preceding calling party number digits to remove. This value can also get configured by the device's device pool setting or the service parameter Incoming Calling Party Unknown Number Prefix – MGCP, depending on the port's Prefix setting. To configure the service parameter Incoming Calling Party Unknown Number Prefix – MGCP to strip digits, enter a value in the format prefix:stripdigits, where prefix is the digits to prepend and stripdigits is the number of digits to strip.
Prefix	Enter the digits to prepend to the stripped calling party number. If you enter Default, the Strip Digits and Prefix settings get configured by the device pool Prefix setting. If the device pool Prefix setting is also set to Default, the Strip Digits and Prefix settings get configured by the service parameter Incoming Calling Party Unknown Number Prefix – MGCP.
Calling Search Space	Select a calling search space (CSS) from the drop-down list box that gets used to perform calling party number transformation. This setting can get overridden by the Use Devices Pool CSS field.
Use Device Pool CSS	Check this check box to use the device pool Unknown Number CSS to perform calling party number transformation. If this box is unchecked, the setting in the Calling Search Space field gets used.

Related Topics

Location Setup , on page 127
About Calling Search Space Setup , on page 273
Gateway Setup , on page 465

Digital Access PRI Port Settings

The following table provides detailed descriptions for Digital Access PRI port configuration settings.

Note To determine whether your gateway supports the QSIG protocol, see the gateway product documentation. For information about QSIG support with Cisco Unified Communications Manager, see topics related to gateway configuration in the *Cisco Unified Communications Manager System Guide*.

Table 87: Digital Access PRI Port Configuration Settings

Field	Description
Device Information	
Endpoint Name	For MGCP gateways, this display-only field contains a string that is generated by Cisco Unified Communications Manager that uniquely identifies the MGCP endpoint. For example: S1/DS1-0@VG200-2 S1 indicates slot 1, DS1-0 designates the digital interface, and @VG200-2 designates the MGCP domain name.
MAC Address	Enter MAC address of the gateway. The MAC address uniquely identifies the hardware device. You must enter a 12-hexadecimal character value.
Description	Enter a description that clarifies the purpose of the device. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
Device Pool	From the drop-down list box, choose the appropriate device pool. The device pool specifies a collection of properties for this device including Communications Manager Group, Date/Time Group, Region, and Calling Search Space for auto-registration of devices.
Common Device Configuration	From the drop-down list box, choose the common device configuration you want to use for this gateway. The common device configuration determines softkey template, MOH, and MLPP settings.
Call Classification	This parameter determines whether an incoming call that is using this gateway is considered off the network (OffNet) or on the network (OnNet). When the Call Classification field is configured as Use System Default, the setting of the Cisco Unified Communications Manager clusterwide service parameter, Call Classification, determines whether the gateway is OnNet or OffNet. This field provides an OnNet or OffNet alerting tone when the call is OnNet or OffNet, respectively.
Network Locale	From the drop-down list box, choose the locale that is associated with the gateway. The network locale identifies a set of detailed information to support the hardware in a specific location. The network locale contains a definition of the tones and cadences that are used by the device in a specific geographic area. **Note** 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. If the device is associated with a network locale that it does not support in the firmware, the device will fail to come up.

Field	Description
Packet Capture Mode (for Cisco IOS MGCP gateways only)	Configure this field only when you need to troubleshoot encrypted signaling information for the Cisco IOS MGCP gateway. Configuring packet capturing may cause call-processing interruptions. For more information on this field, see the *Cisco Unified Communications Manager Security Guide*.
Packet Capture Duration (for Cisco IOS MGCP gateways only)	Configure this field only when you need to troubleshoot encrypted signaling information for the Cisco IOS MGCP gateway. Configuring packet capturing may cause call-processing interruptions. For more information on this field, see the *Cisco Unified Communications Manager Security Guide*.
Media Resource Group List	This list provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, among the available media resources according to the priority order that is defined in a Media Resource List.
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 box, choose the appropriate location for this device. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this device consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the **System** > **Location** menu option. For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*.
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.
Load Information	Enter the appropriate firmware load information for the gateway. The value that you enter here overrides the default firmware load for this gateway type.

Field	Description
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified Communications Manager inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values: • Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates. • Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified Communications Manager places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVPAgent). If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the *Cisco Unified Communications Manager System Guide* for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified Communications Manager first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified Communications Manager first tries to find a transcoder that is also designated as a TRP. See the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.
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.

Field	Description
Transmit UTF-8 for Calling Party Name	This device uses the user locale setting of the device pool for the device to determine whether to send unicode and whether to translate received unicode information. For the sending device, if you check this check box and the user locale setting in the device pool for the device matches the terminating phone user locale, the device sends unicode. If the user locale settings do not match, the device sends ASCII. The receiving device translates incoming unicode characters based on the user locale setting of the device pool to which the sending device belongs. If the user locale setting matches the terminating phone user locale, the phone displays the characters. **Note** The phone may display junk characters if the two ends of the trunk configure user locales that do not belong to the same language group.
V150 (subset)	Check this box to enable V.150 (subset) modem relay support on the gateways. IP-STEs currently use this feature to support end-to-end secure calls to an ISDN-STE. (Applies only to T1 PRI and T1 CAS.) **Note** This setting supports both V.150 and V.150.1 MER (Minimal Essential Requirements) modem relay functionality. The default value specifies unchecked. **Warning** The MDSTE package must also be enabled on the gateway via a CLI command for this check box to work properly. If you check this box without enabling the gateway, the MDSTE package can cause call attempt failures on the affected gateway trunk.
Multilevel Precedence and Preemption (MLPP) Information	
MLPP Domain	From the drop-down list box, choose an MLPP domain to associate with this device. If you leave the value <None>, this device inherits its MLPP domain from the value that is set for the device pool of the device. If the device pool does not have an MLPP Domain setting, this device inherits its MLPP Domain from the value that is set for the MLPP Domain Identifier enterprise parameter.
MLPP Indication	Be aware that this setting is not available for all devices. If available, this setting specifies whether a device that can play precedence tones will use the capability when it places an MLPP precedence call. From the drop-down list box, choose a setting to assign to this device from the following options: • Default—This device inherits its MLPP indication setting from its device pool. • Off—This device does not handle nor process indication of an MLPP precedence call. • On—This device does handle and process indication of an MLPP precedence call. **Note** Do not configure a device with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful.

Field	Description
MLPP Preemption	Be aware that this setting is not available for all devices. If available, this setting specifies whether a device that can preempt calls in progress will use the capability when it places an MLPP precedence call. From the drop-down list box, choose a setting to assign to this device from the following options: • Default—This device inherits its MLPP preemption setting from its device pool. • Disabled—This device does not allow preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. • Forceful—This device allows preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. **Note** Do not configure a device with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful.
Interface Information	

Field	Description
PRI Protocol Type	Choose the communications protocol for the span. T1 PRI spans provide several options, depending on the carrier or switch; for example: • PRI 4ESS—AT&T Interexchange carrier • PRI 5E8—AT&T family 5ESS ISDN switch that runs in NI-1 or custom mode. • PRI 5E8 Custom—Cisco Unified IP Phone • PRI 5E9—AT&T family local exchange switch or carrier • PRI DMS—MCI family local exchange switch or carrier; Canadian local exchange carrier • PRI ETSI SC—European local exchange carrier on T1; also, Japanese, Taiwan, Korean, and Hong Kong local exchange. • PRI NI2—AT&T family local exchange switch or carrier **Note** If you specify the PRI NI2 PRI protocol type, configure the Cisco IOS gateway with the following command:isdn switch-type primary-ni • PRI NTT—Japanese NTT exchange switch • PRI ISO QSIG T1—PBX T1 tie trunk using ISO QSIG • PRI ISO QSIG E1—PBX E1 tie trunk using ISO QSIG Determine the switch to which you are connecting and the preferred protocol; for example: • Nortel Meridian—DMS, 5E8 Custom • Lucent Definity—4ESS or 5E8 • Madge (Teleos) box—5E8 Teleos • Intecom PBX—5E8 Intecom

Field	Description
QSIG Variant	To display the options in the QSIG Variant drop-down list box, choose QSIG from the Tunneled Protocol drop-down list box. This parameter specifies the protocol profile that is sent in outbound QSIG facility information elements. From the drop-down list box, choose one of the following options. Keep this parameter set to the default value unless a Cisco support engineer instructs otherwise. • No Changes • Not Selected • ECMA—If the QSIG Variant is set to ECMA (Protocol Profile 0x91), ensure the ASN.1 Rose OID Encoding service parameter is set to Use Global Value (ECMA). • ISO—(Default) If the QSIG Variant is set to ISO (Protocol Profile 0x9F), ensure the ASN.1 Rose OID Encoding service parameter is set to either Use Local Value or Use Global Value (ISO). For more information, see the following information: • Be aware that the QSIG Variant can also be defined as a clusterwide parameter. • For information on QSIG support with Cisco Unified Communications Manager, see the *Cisco Unified Communications Manager System Guide*.
ASN.1 ROSE OID Encoding	To display the options in the ASN.1 ROSE OID Encoding drop-down list box, choose QSIG from the Tunneled Protocol drop-down list box. This parameter specifies how to encode the Invoke Object ID (OID) for remote operations service element (ROSE) operations. From the drop-down list box, choose one of the following options: • No Changes. • Not Selected • Use Global Value (ISO)—Select this option only if the connected PBX does not support Local Value. • Use Global Value (ECMA)—Select this option only if the QSIG Variant service parameter is set to ECMA (Protocol Profile 0x91). • Use Local Value—(Default) This option gets supported by most telephony systems and should be used when the QSIG Variant service parameter is set to ISO (Protocol Profile 0x9F). For more information, see the following information: • Be aware that ASN.1 ROSE OID Encoding can also be defined as a clusterwide parameter. • For information on QSIG support with Cisco Unified Communications Manager, see the *Cisco Unified Communications Manager System Guide*.

Field	Description
Protocol Side	Choose the appropriate protocol side. This setting specifies whether the gateway connects to a Central Office/Network device or to a User device. Make sure that the two ends of the PRI connection use opposite settings. For example, if you connect to a PBX and the PBX uses User as its protocol side, choose Network for this device. Typically, use User for this option for central office connections.
Channel Selection Order	Choose the order in which channels or ports are enabled from first (lowest number port) to last (highest number port), or from last to first. Valid entries include TOP_DOWN (first to last) or BOTTOM_UP (last to first). If you are not sure which port order to use, choose TOP_DOWN.
Channel IE Type	Choose one of the following values to specify whether channel selection is presented as a channel map or a slot map: • Timeslot Number—B-channel usage always indicates actual timeslot map format (such as 1-15 and 17-31 for E1). • Slotmap—B-channel usage always indicates a slot map format. • Use Number When 1B—Channel usage indicates a channel map for one B-channel but indicates a slot map if more than one B-channel exists. • Continuous Number—Configures a continuous range of slot numbers (1-30) as the E1 logical channel number instead of the noncontinuous actual timeslot number (1-15 and 17-31).
PCM Type	Specify the digital encoding format. Choose one of the following formats: • a-law: Use for Europe and other countries, except North America, Hong Kong, Taiwan, and Japan. • mu-law: Use for North America, Hong Kong, Taiwan, and Japan.
Delay for first restart (1/8 sec ticks)	Enter the rate at which the spans are brought in service. The delay occurs when many PRI spans are enabled on a system and the Inhibit Restarts at PRI Initialization check box is unchecked. For example, set the first five cards to 0 and set the next five cards to 16. (Wait 2 seconds before bringing them in service.)
Delay between restarts (1/8 sec ticks)	Enter the time between restarts. The delay occurs when a PRI RESTART gets sent if the Inhibit Restarts check box is unchecked.
Inhibit restarts at PRI initialization	A RESTART or SERVICE message confirms the status of the ports on a PRI span. If RESTART or SERVICE messages are not sent, Cisco Unified Communications Manager assumes the ports are in service. When the D-Channel successfully connects with another PRI D-Channel, it sends a RESTART or SERVICE message when this check box is unchecked.

Field	Description
Enable status poll	Check the check box to enable the Cisco Unified Communications Manager advanced service parameter, Change B-Channel Maintenance Status. This service parameter allows you to take individual B-channels out of service for an MGCP T1/E1 PRI gateway in real time. Uncheck this check box to disable the service parameter, Change B-Channel Maintenance Status. **Note** Default leaves this field unchecked.
Unattended Port	Check this check box to indicate an unattended port on this device.
Enable G.Clear	Check this box to enable G. Clear Codec support for MGCP T1 PRI gateways and SIP trunks. When you enable G. Clear Codec, echo cancellation and zero suppression for outbound calls get disabled. **Note** Fast Start and Media Termination Point Required options in Cisco Unified Communications Manager Administration do not work. To enable G. Clear Code support on SIP trunks between clusters, you must configure the SIP Clear Channel Data Route Class Label and SIP Route Class Naming Authority service parameters. If you have low bandwidth codec regions, you must enable the G. Clear Bandwidth Override service parameter. The following functionality does not support the G. Clear Codec: • T1 and E1 CAS • H.323 Intercluster Trunks • SCCP devices • RSVP • Frame aligning individual DS-0 circuits
Call Routing Information - Inbound Calls	

Significant Digits	Choose the number of significant digits to collect, from 0 to 32 or All. Cisco Unified Communications Manager counts significant digits from the right (last digit) of the number that is called. If you choose All, the Cisco Unified Communications Manager does not truncate the inbound number.
	`EXAMPLEDigits received are 123456.`
	`Significant digits setting is 4.`
	`Digits translated are 3456.`
	Use for the processing of incoming calls and to indicate the number of digits, starting from the last digit of the called number, that are used to route calls that are coming into the PRI span. See Prefix DN.

Field	Description
Calling Search Space	From the drop-down list box, choose the appropriate calling search space. A calling search space designates a collection of route partitions that are searched to determine how a collected (originating) number should be routed. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more 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, then find and choose a calling search space name. **Note** To set the maximum list box items, choose **System** > **Enterprise Parameters** and choose CCMAdmin Parameters.
AAR Calling Search Space	Choose the appropriate calling search space for the device 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.
Prefix DN	Enter the prefix digits that are appended to the digits that this gateway receives on incoming calls. The Cisco Unified Communications Manager adds prefix digits after first truncating the number in accordance with the Num Digits setting. You can enter the international escape character +.
Call Routing Information - Outbound Calls	
Calling Party Presentation	Choose whether you want the Cisco Unified Communications Manager to allow or restrict the display of the calling party phone number. Choose Default if you do not want to change calling line ID presentation. Choose Allowed if you want Cisco Unified Communications Manager to send “Calling Line ID Allowed” on outbound calls. Choose Restricted if you want Cisco Unified Communications Manager to send “Calling Line ID Restricted” on outbound calls. For more information about this field, see the *Cisco Unified Communications Manager System Guide*.
Calling Party Selection	Any outbound call on a gateway can send directory number information. Choose which directory number is sent: • Originator—Send the directory number of the calling device. • First Redirect Number—Send the directory number of the redirecting device. • Last Redirect Number—Send the directory number of the last device to redirect the call. • First Redirect Number (External)—Send the directory number of the first redirecting device with the external phone mask applied. • Last Redirect Number (External)—Send the directory number of the last redirecting device with the external phone mask applied.

Field	Description
Called party IE number type unknown	Choose the format for the number type in called party directory numbers. Cisco Unified Communications Manager sets the called 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 called directory number to be encoded to a non-national type numbering plan. Choose one of the following options: • Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the directory number type. • Unknown—Use 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.
Calling party IE number type unknown	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 type numbering plan. Choose one of the following options: • Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the directory number type. • Unknown—Use 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.

Field	Description
Called Numbering Plan	Choose the format for the numbering plan in called party directory numbers. Cisco Unified Communications Manager sets the called DN numbering plan. 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 PBXs by using routing as a non-national type number. Choose one of the following options: • Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the Numbering Plan in the directory number. • ISDN—Use when you are dialing outside the dialing plan for your country. • National Standard—Use when you are dialing within the dialing plan for your country. • Private—Use when you are dialing within a private network. • Unknown—Use when the dialing plan is unknown.
Calling Numbering Plan	Choose the format for the numbering plan in calling party directory numbers. Cisco Unified Communications Manager sets the calling DN numbering plan. 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 PBXs by using routing as a non-national type number. Choose one of the following options: • Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the Numbering Plan in the directory number. • ISDN—Use when you are dialing outside the dialing plan for your country. • National Standard—Use when you are dialing within the dialing plan for your country. • Private—Use when you are dialing within a private network. • Unknown—Use when the dialing plan is unknown.
Number of digits to strip	Choose the number of digits to strip on outbound calls, from 0 to 32. For example, when 8889725551234 is dialed, and the number of digits to strip is 3, Cisco Unified Communications Manager strips 888 from the outbound number.

Field	Description
Caller ID DN	Enter the pattern that you want to use for calling line ID, from 0 to 24 digits. For example, in North America • 555XXXX = Variable calling line ID, where X equals an extension number. The CO appends the number with the area code if you do not specify it. • 5555000 = Fixed calling line ID, where you want the Corporate number to be sent instead of the exact extension from which the call is placed. The CO appends the number with the area code if you do not specify it. You can also enter the international escape character +.
Called Party Transformation CSS	This setting allows you to send transformed called party number in SETUP message for outgoing calls. Make sure that the Called Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device. **Note** If you configure the Called Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Called Party Transformation pattern in a non-null partition that is not used for routing.
Use Device Pool Called Party Transformation CSS	To use the Called 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 Called Party Transformation CSS that you configured in the PRI Port Gateway Configuration window.
Calling Party Transformation CSS	This setting allows you to send transformed calling party number in SETUP message for outgoing calls. Also when redirection occurs for outbound calls, this CSS will be used to transform the connected number sent from Cisco Unified Communications Manager side in outgoing NOTIFY messages. [For PRI DMS - 100 and DMS - 200]. 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** 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.
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 PRI Port Gateway Configuration window.
PRI Protocol Type Specific Information	
Display IE Delivery	Check the check box to enable delivery of the display information element (IE) in SETUP and NOTIFY messages (for DMS protocol) for the calling and connected party name delivery service.

Field	Description
Redirecting Number IE Delivery—Outbound	Check this check box to indicate the first redirecting number and the redirecting reason of the call when the call is forwarded. (The UUIE part of the outgoing SETUP message from the Cisco Unified Communications Manager includes the Redirecting Number IE.) Uncheck the check box to exclude the first redirecting number and the redirecting reason. You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box.
Redirecting Party Transformation CSS	This setting allows you to transform the redirecting party number on the device to another format such as DID or E164 format. Cisco Unified Communications Manager includes the transformed number in the Redirecting Number Information Element of MGCP setup message sent out of Cisco Unified Communications Manager. Make sure that the Redirecting Party Transformation CSS that you choose contains either the calling or called party transformation pattern that you want to assign to this MGCP gateway. **Note** If you configure the Redirecting Party Transformation CSS as None and also uncheck the Use Device Pool Redirecting Party CSS check box, the transformation does not match and does not get applied. Ensure that you configure the Redirecting Party Transformation CSS in a non-null partition that is not used for routing.
Use Device Pool Redirecting Party Transformation CSS	To use the Redirecting 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 Redirecting Party Transformation CSS that you configured in the MGCP Gateway Configuration window.
Redirecting Number IE Delivery—Inbound	Check this check box to accept the Redirecting Number IE in the incoming SETUP message to the Cisco Unified Communications Manager. (The UUIE part of the SETUP message includes the Redirecting Number IE.) Uncheck the check box to exclude the Redirecting Number IE. You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box.
Send Extra Leading Character in Display IE	Check this check box to include a special leading character byte (non ASCII, nondisplayable) in the DisplayIE field. Uncheck this check box to exclude this character byte from the Display IE field. This check box only applies to the DMS-100 protocol and the DMS-250 protocol. Default leaves this setting disabled (unchecked).

Field	Description
Setup non-ISDN Progress Indicator IE Enable	Default leaves this setting disabled (unchecked). Enable this setting only if users are not receiving ringback tones on outbound calls. When this setting is enabled, the Cisco Unified Communications Manager sends Q.931 Setup messages out digital (that is, non-H.323) gateways with the Progress Indicator field set to non-ISDN. This message notifies the destination device that the Cisco Unified Communications Manager gateway is non-ISDN and that the destination device should play in-band ringback. This problem usually associates with Cisco Unified Communications Managers that connect to PBXs through digital gateways.
MCDN Channel Number Extension Bit Set to Zero	To set the channel number extension bit to zero, check the check box. To set the extension bit to 1, uncheck the check box. This setting only applies to the DMS-100 protocol
Send Calling Name in Facility IE	Check the check box to send the calling name in the Facility IE field. By default, the Cisco Unified Communications Manager leaves the check box unchecked. Set this feature for a private network that has a PRI interface that is enabled for ISDN calling name delivery. When this check box is checked, the calling party name gets sent in the Facility IE of the SETUP or FACILITY message, so the name can display on the called party device. Set this feature for PRI trunks in a private network only. Do not set this feature for PRI trunks that are connected to the PSTN. **Note** This field applies to the NI2 protocol only.
Interface Identifier Present	Check the check box to indicate that an interface identifier is present. By default, the Cisco Unified Communications Manager leaves the check box unchecked. This setting only applies to the DMS-100 protocol for digital access gateways in the Channel Identification information element (IE) of the SETUP, CALL PROCEEDING, ALERTING, and CONNECT messages.
Interface Identifier Value	Enter the value that was obtained from the PBX provider. This field applies to only the DMS-100 protocol. Valid values range from 0 through 255.

Field	Description
Connected Line ID Presentation (QSIG Inbound Call)	Choose whether you want the Cisco Unified Communications Manager to allow or block the connected party phone number from displaying on an inbound caller phone. This field applies only to gateways that are using QSIG protocol. The gateway applies this setting for incoming calls only. Choose Default if you do not want to change the connected line ID presentation. Choose Allowed if you want Cisco Unified Communications Manager to send "Connected Line ID Allowed" to enable the connected party number to display for the calling party. Choose Restricted if you want Cisco Unified Communications Manager to send "Connected Line ID Restricted" to block the connected party number from displaying for the calling party. If a call that originates from an IP phone on Cisco Unified Communications Manager encounters a device, such as a trunk, gateway, or route pattern, that has the Connected Line ID Presentation set to Default, the presentation value is automatically set to Allowed. For more information about this field, see the *Cisco Unified Communications Manager System Guide*.
Connected Party Settings	
Connected Party Transformation CSS	This setting is applicable only for inbound Calls. This setting allows you to transform the connected party number sent from Cisco Unified Communications Manager in another format, such as a DID or E.164 number. **Note** You can configure a Connected Party Transformation CSS only when you select one of the following protocols that support Connected Number Information Element: • For T1 PRI : ◦ PRI DMS - 100 ◦ PRI DMS - 250 ◦ PRI ISO QSIG T1 • For E1 PRI : ◦ PRI ISO QSIG E1 For other protocol types, Connected Party Transformation CSS is grayed out. Using this setting, Cisco Unified Communications Manager includes transformed number in Connected Number Information Element (IE) of CONNECT message for basic call. For PRI DMS - 100 and DMS - 250 protocols , Cisco Unified Communications Manager includes transformed number in Connected Number Information Element (IE) of NOTIFY message for inbound calls after redirection. Make sure that the Connected Party Transformation CSS that you choose contains the connected party transformation pattern that you want to assign to this device. **Note** If you configure the Connected Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Connected Party Transformation CSS in a non-null partition that is not used for routing.

Field	Description
Use Device Pool Connected Party Transformation CSS	To use the Connected 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 Connected Party Transformation CSS that you configured for this device in the Trunk Configuration window.
UUIE Configuration	
Passing Precedence Level Through UUIE	Check this check box to enable passing MLPP information through the PRI 4ESS UUIE field. The system uses this box for interworking with DRSN switch. The system makes this check box available only if the PRI Protocol Type value of PRI 4ESS is specified for this gateway. The default value specifies unchecked.
Security Access Level	Enter the value for the security access level. Valid values include 00 through 99. The system makes this field available only if the Passing Precedence Level Through UUIE check box is checked. The default value specifies 2.
Incoming Calling Party Settings	
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.

Field	Description
National Number	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 16 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, you cannot configure the Strip Digits field. 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. • Strip Digits—Enter the number of digits, up to the number 24, 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—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 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. 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. **Tip** For more information on configuring these settings, see the *Cisco Unified Communications Manager Features and Services Guide*.

Field	Description
International Number	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 16 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, you cannot configure the Strip Digits field. 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. • Strip Digits—Enter the number of digits, up to the number 24, 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— 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 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. 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. **Tip** For more information on configuring these settings, see the *Cisco Unified Communications Manager Features and Services Guide*.

Field	Description
Subscriber Number	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 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). **Tip** If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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. • Strip Digits—Enter the number of digits, up to the number 24, 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 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. 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. **Tip** For more information on configuring these settings, see the *Cisco Unified Communications Manager Features and Services Guide*.

Field	Description
Unknown Number	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 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). **Note** If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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. • Strip Digits—Enter the number of digits, up to the number 24, 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—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 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. 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. **Tip** For more information on configuring these settings, see the *Cisco Unified Communications Manager Features and Services Guide*.
Incoming Called Party Settings	
Clear Prefix Settings	To delete all prefixes for all called party number types, click Clear Prefix Settings.
Default Prefix Settings	To enter the default value for all prefix fields at the same time, click Default Prefix Settings.

Field	Description
National Number	Configure the following settings to transform incoming called party numbers that use National for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called party numbers that use National for the Called Party Number Type. You can enter up to 16 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, you cannot configure the Strip Digits field. 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 does not apply any prefix or strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, 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 called party number of National type before it applies the prefixes. • Use Device Pool CSS—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 the device. • Calling Search Space—This setting allows you to transform the called party number of National called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

Field	Description
International Number	Configure the following settings to transform incoming called party numbers that use International for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called party numbers that use International for the Called Party Numbering Type. You can enter up to 16 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, you cannot configure the Strip Digits field. 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 does not apply any prefix or strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, 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 called party number of International type before it applies the prefixes. • Use Device Pool CSS— 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 the device. • Calling Search Space—This setting allows you to transform the called party number of International called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

Field	Description
Unknown Number	Configure the following settings to transform incoming called party numbers that use Unknown for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called numbers that use Unknown for the Called Party Numbering Type. You can enter up to 16 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, you cannot configure the Strip Digits field. 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 does not apply any prefix or strip digit functionality. **Tip** To configure the Strip Digits field, 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 called party number of Unknown type before it applies the prefixes. • Use Device Pool CSS—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 the device. • Calling Search Space—This setting allows you to transform the called party number of Unknown called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

Field	Description
Subscriber Number	Configure the following settings to transform incoming called party numbers that use Subscriber for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called numbers that use Subscriber for the Called Party Numbering Type. You can enter up to 16 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, you cannot configure the Strip Digits field. 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 does not apply any prefix or strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, 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 called 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 transform the called party number of Subscriber called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.
Product-Specific Configuration	
Model-specific configuration fields that the gateway manufacturer defines	The gateway manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the "?" information icon to the right of the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, see the documentation for the specific gateway that you are configuring or contact the manufacturer.
Geolocation Configuration	

Field	Description
Geolocation	From the drop-down list box, choose a geolocation. You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation. You can also choose a geolocation that has been configured with the **System** > **Geolocation Configuration** menu option. For an explanation of geolocations, including configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocations, see the *Cisco Unified Communications Manager Features and Services Guide*.
Geolocation Filter	From the drop-down list box, choose a geolocation filter. If you leave the <None> setting, no geolocation filter gets applied for this device. You can also choose a geolocation filter that has been configured with the **System** > **Geolocation Filter** menu option. For an explanation of geolocation filters, including configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocation filters, see the *Cisco Unified Communications Manager Features and Services Guide*.

Related Topics

Location Setup , on page 127
Service Parameter Setup , on page 151
About Calling Search Space Setup , on page 273
Gateway Setup , on page 465

Digital Access T1 Port Settings

The following table provides detailed descriptions for Digital Access T1 port configuration settings.

Table 88: Digital Access T1 Port Configuration Settings

Field	Description
MAC Address (non-IOS gateway)	Enter MAC address of the gateway. The MAC address uniquely identifies the hardware device. You must enter a 12-hexadecimal character value.

Field	Description
Domain Name	For MGCP gateways, this display-only field contains a string that Cisco Unified Communications Manager generates that uniquely identifies the MGCP digital interface. For example S1/DS1-0@VG200-2 S1 indicates slot 1, DS1-0 designates the digital interface, and @VG200-2 designates the MGCP domain name.
Note Enter either a MAC address or a domain name, whichever applies.	
Description	Enter a description that clarifies the purpose of the device. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
Device Pool	From the drop-down list box, choose the appropriate device pool. The device pool specifies a collection of properties for this device including Communications Manager Group, Date/Time Group, Region, and Calling Search Space for auto-registration of devices.
Common Device Configuration	From the drop-down list box, choose the common device configuration that you want to use for this gateway. The common device configuration determines softkey template, MOH, and MLPP settings.
Call Classification	This parameter determines whether an incoming call that is using this gateway is considered off the network (OffNet) or on the network (OnNet). When the Call Classification field is configured as Use System Default, the setting of the Cisco Unified Communications Manager clusterwide service parameter, Call Classification, determines whether the gateway is OnNet or OffNet. This field provides an OnNet or OffNet alerting tone when the call is OnNet or OffNet, respectively.
Media Resource Group List	This list provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from among the available media resources according to the priority order that is defined in a Media Resource List.
Packet Capture Mode (for Cisco IOS MGCP gateways only)	Configure this field only when you need to troubleshoot encrypted signaling information for the Cisco IOS MGCP gateway. Configuring packet capturing may cause call-processing interruptions. For more information on this field, see the *Cisco Unified Communications Manager Security Guide*.
Packet Capture Duration (for Cisco IOS MGCP gateways only)	Configure this field only when you need to troubleshoot encrypted signaling information for the Cisco IOS MGCP gateway. Configuring packet capturing may cause call-processing interruptions. For more information on this field, see the *Cisco Unified Communications Manager Security Guide*.

Field	Description
Calling Search Space	From the drop-down list box, choose the appropriate calling search space. A calling search space designates a collection of route partitions that are searched to determine how a collected (originating) number should be routed. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more 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, then find and choose a calling search space name. **Note** To set the maximum list box items, choose **System** > **Enterprise Parameters** and choose CCMAdmin Parameters.
AAR Calling Search Space	Choose the appropriate calling search space for the device 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.
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 box, choose the appropriate location for this device. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this device consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the **System** > **Location** menu option. For more details about locations, see the Location Setup , on page 127. For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*.
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.
MLPP Domain	From the drop-down list box, choose an MLPP domain to associate with this device. If you leave the value <None>, this device inherits its MLPP domain from the value that was set for the device pool of the device. If the device pool does not have an MLPP Domain setting, this device inherits its MLPP Domain from the value that was set for the MLPP Domain Identifier enterprise parameter.

Field	Description
MLPP Indication	Some devices do not make this setting available. If available, this setting specifies whether a device that plays precedence tones will use the capability when it places an MLPP precedence call. From the drop-down list box, choose a setting to assign to this device from the following options: • Default—This device inherits its MLPP indication setting from its device pool. • Off—This device does not handle nor process indication of an MLPP precedence call. • On—This device does handle and process indication of an MLPP precedence call. **Note** Do not configure a device with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful.
MLPP Preemption	Some devices do not make this setting available. If available, this 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 to assign to this device from the following options: • Default—This device inherits its MLPP preemption setting from its device pool. • Disabled—This device does not allow preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. • Forceful—This device allows preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. **Note** Do not configure a device with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful.

Field	Description
Enable G. Clear Codec	Check this box to enable G. Clear Codec support for MGCP T1 PRI gateways and SIP trunks. When you enable G. Clear Codec, echo cancellation and zero suppression for outbound calls get disabled. **Note** Fast Start and Media Termination Point Required options in Cisco Unified Communications Manager Administration do not work. To enable G. Clear Code support on SIP trunks between clusters, you must configure the SIP Clear Channel Data Route Class Label and SIP Route Class Naming Authority service parameters. If you have low bandwidth codec regions, you must enable the G. Clear Bandwidth Override service parameter. The following functionality does not support the G. Clear Codec: • T1 and E1 CAS • H.323 Intercluster Trunks • SCCP devices • RSVP • Frame aligning individual DS-0 circuits
Handle DTMF Precedence Signals	Check this box to enable this gateway to interpret special DTMF signals as MLPP precedence levels.
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
Load Information	Enter the appropriate firmware load information for the gateway. The values that you enter here override the default values for this gateway.
Port Selection Order	Choose the order in which channels or ports are allocated for outbound calls from first (lowest number port) to last (highest number port) or from last to first. Valid entries include Top Down (first to last) or Bottom Up (last to first). If you are not sure which port order to use, choose Top Down.
Digit Sending	Choose one of the following digit-sending types for out-dialing: • DTMF—Dual-tone multifrequency. Normal touchtone dialing • MF—Multifrequency • PULSE—Pulse (rotary) dialing

Field	Description
Network Locale	From the drop-down list box, choose the locale that is associated with the gateway. The network locale identifies a set of detailed information to support the hardware in a specific location. The network locale contains a definition of the tones and cadences that the device uses in a specific geographic area. **Note** 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. If the device is associated with a network locale that it does not support in the firmware, the device will fail to come up.
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified Communications Manager inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values: • Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates. • Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified Communications Manager places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVPAgent). If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the *Cisco Unified Communications Manager System Guide* for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified Communications Manager first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified Communications Manager first tries to find a transcoder that is also designated as a TRP. See the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.

Field	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.
V150 (subset)	Check this box to enable V.150 (subset) modem relay support on the gateways. IP-STEs currently use this feature to support end-to-end secure calls to an ISDN-STE. (Applies only to T1 PRI and T1 CAS) **Note** This setting supports both V.150 and V.150.1 MER (Minimal Essential Requirements) modem relay functionality. The default value specifies unchecked.
Product-Specific Configuration	
Model-specific configuration fields that the gateway manufacturer defines	The gateway manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the "?" information icon to the right of the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, see the documentation for the specific gateway that you are configuring or contact the manufacturer.
Geolocation Configuration	
Geolocation	From the drop-down list box, choose a geolocation. You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation. You can also choose a geolocation that has been configured with the **System** > **Geolocation Configuration** menu option. For an explanation of geolocations, including configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocations, see the *Cisco Unified Communications Manager Features and Services Guide*.

Field	Description
Geolocation Filter	From the drop-down list box, choose a geolocation filter. If you leave the <None> setting, no geolocation filter gets applied for this device. You can also choose a geolocation filter that has been configured with the **System** > **Geolocation Filter** menu option. For an explanation of geolocation filters, including configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocation filters, see the *Cisco Unified Communications Manager Features and Services Guide*.

Related Topics

About Calling Search Space Setup , on page 273
Gateway Setup , on page 465

BRI Port Settings

The following table provides detailed descriptions for BRI port configuration settings.

Table 89: BRI Port Configuration Settings

Field	Description
Device Information	
End-Point Name (MGCP gateways)	For MGCP gateways, this display-only field contains a string that Cisco Unified Communications Manager generates that uniquely identifies the MGCP endpoint. For example BRI/S1/SU0/P0@SC3640.cisco.com S1 indicates slot 1, SU0 indicates subunit 0, P0 indicates port 0, and @SC3640.cisco.com designates the MGCP domain name.
Description	Enter a description that clarifies the purpose of the device. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
Device Pool	From the drop-down list box, choose the appropriate device pool. For this device, the device pool specifies a collection of properties that includes Communications Manager Group, Date and Time Group, Region, and Calling Search Space for auto-registration of devices.
Common Device Configuration	From the drop-down list box, choose the common device configuration you want to use for this gateway. The common device configuration determines softkey template, MOH, and MLPP settings.

Field	Description
Call Classification	This parameter determines whether an incoming call that is using this gateway is considered off the network (OffNet) or on the network (OnNet). When the Call Classification field is configured as Use System Default, the setting of the Cisco Unified Communications Manager clusterwide service parameter, Call Classification, determines whether the gateway is OnNet or OffNet. This field provides an OnNet or OffNet alerting tone when the call is OnNet or OffNet, respectively.
Network Locale	From the drop-down list box, choose the locale that is associated with the gateway. The network locale identifies a set of detailed information to support the hardware in a specific location. The network locale contains a definition of the tones and cadences that devises use in a specific geographic area.
Packet Capture Mode (for Cisco IOS MGCP gateways only)	Configure this field only when you need to troubleshoot encrypted signaling information for the Cisco IOS MGCP gateway. Configuring packet capturing may cause call-processing interruptions. For more information on this field, see the *Cisco Unified Communications Manager Security Guide*.
Packet Capture Duration (for Cisco IOS MGCP gateways only)	Configure this field only when you need to troubleshoot encrypted signaling information for the Cisco IOS MGCP gateway. Configuring packet capturing may cause call-processing interruptions. For more information on this field, see the *Cisco Unified Communications Manager Security Guide*.
Media Resource Group List	This list provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from among the available media resources according to the priority order that a Media Resource List defines.
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 box, choose the appropriate location for this device. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this device consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the **System** > **Location** menu option. For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*.

Field	Description
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.
Interface Information	
BRI Protocol	Choose the communications protocol for the span. BRI-NET3
Protocol Side	Choose the appropriate protocol side. This setting specifies whether the gateway connects to a Central Office/Network device or to a User device. **Note** BRI supports only the User side.
Channel Selection Order	Choose the order in which channels or ports are enabled from first (lowest number port) to last (highest number port) or from last to first. Valid entries include TOP_DOWN (first to last) or BOTTOM_UP (last to first). If you are not sure which port order to use, choose TOP_DOWN.
PCM Type	Specify the digital encoding format. Choose one of the following formats: • a-law: Use for Europe and other countries, except North America, Hong Kong, Taiwan, and Japan. • mu-law: Use for North America, Hong Kong, Taiwan, and Japan.
Delay for First Restart (1/8 sec ticks)	Enter the rate at which the spans are brought in service. The delay occurs when many BRI spans are enabled on a system and the Inhibit Restarts at BRI Initialization check box is unchecked. For example, set the first five cards to 0 and set the next five cards to 16. (Wait 2 seconds before bringing them in service.)
Delay Between Restarts (1/8 sec ticks)	Enter the time between restarts. The delay occurs when a BRI RESTART gets sent if the Inhibit Restarts check box is unchecked.
Inhibit Restarts at BRI Initialization	A RESTART message confirms the status of the ports on a BRI span. If RESTART messages are not sent, Cisco Unified Communications Manager assumes that the ports are in service. When the data link successfully connects with another BRI data link, it sends a RESTART message when this check box is unchecked.
Enable Status Poll	Check the check box to view the B-channel status in the debug window.
Unattended Port	Check this check box to indicate an unattended port on this device.

Field	Description
Enable G.Clear	Check this box to enable G. Clear Codec support for MGCP BRI gateways and SIP trunks. When you enable G. Clear Codec, echo cancellation and zero suppression for outbound calls get disabled. **Note** Fast Start and Media Termination Point Required options in Cisco Unified Communications Manager Administration do not work. To enable G. Clear Code support on SIP trunks between clusters, you must configure the SIP Clear Channel Data Route Class Label and SIP Route Class Naming Authority service parameters. If you have low bandwidth codec regions, you must enable the G. Clear Bandwidth Override service parameter. The following functionality does not support the G. Clear Codec: • T1 and E1 CAS • H.323 Intercluster Trunks • SCCP devices • RSVP • Frame aligning individual DS-0 circuits
Establish Datalink on First Call	Cisco Unified Communications Manager establishes the data link to the gateway when the gateway registers with Cisco Unified Communications Manager. When you configure the gateway and switch to negotiate the TEI (terminal endpoint identifier) on the first call, you can check the check box to establish the data link on the first call. **Note** Default leaves the check box unchecked.
Call Routing Information - Inbound Calls	

Significant Digits	Choose the number of significant digits to collect, from 0 to 32 or All. Cisco Unified Communications Manager counts significant digits from the right (last digit) of the number called. If you choose All, the Cisco Unified Communications Manager does not truncate the inbound number.
	`EXAMPLEDigits received are 123456.`
	`Significant digits setting is 4.`
	`Digits translated are 3456.`
	Use for the processing of incoming calls and to indicate the number of digits, starting from the last digit of the called number, that are used to route calls that are coming into the BRI span. See Prefix DN.

Calling Search Space	Choose the appropriate calling search space. A calling search space designates a collection of route partitions that are searched to determine how a collected (originating) number should be routed.

Field	Description
AAR Calling Search Space	Choose the appropriate calling search space for the device 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.
Prefix DN	Enter the prefix digits that are appended to the digits that this gateway receives on incoming calls. The Cisco Unified Communications Manager adds prefix digits after first truncating the number in accordance with the Num Digits setting. You can enter the international escape character + in this field.
Call Routing Information - Outbound Calls	
Called Party Transformation CSS	This setting allows you to localize the called party number on the device. Make sure that the Called Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device. **Note** If you configure the Called Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Called Party Transformation pattern in a non-null partition that is not used for routing.
Use Device Pool Called Party Transformation CSS	To use the Called 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 Called Party Transformation CSS that you configured in the PRI Port Gateway Configuration window.
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.
Geolocation	From the drop-down list box, choose a geolocation. You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation. You can also choose a geolocation that has been configured with the **System** > **Geolocation Configuration** menu option. For an explanation of geolocations, including configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocations, see the *Cisco Unified Communications Manager Features and Services Guide*.

Field	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 PRI Port Gateway Configuration window.
Calling Party Presentation	Choose whether you want the Cisco Unified Communications Manager to transmit or block caller ID. Choose Default if you do not want to change calling party presentation. Choose Allowed if you want Cisco Unified Communications Manager to send caller ID. Choose Restricted if you do not want Cisco Unified Communications Manager to send caller ID.
Calling Party Selection	Any outbound call on a gateway can send directory number information. Choose which directory number is sent: • Originator—Send the directory number of the calling device. • First Redirect Number—Send the directory number of the redirecting device. • Last Redirect Number—Send the directory number of the last device to redirect the call. • First Redirecting Party (External)—Send the directory number of the first redirecting device with the external phone mask applied. • Last Redirecting Party (External)—Send the directory number of the last redirecting device with the external phone mask applied.
Called party IE number type unknown	Choose the format for the number type in called party directory numbers. Cisco Unified Communications Manager sets the called 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 called directory number to be encoded to a non-national numbering plan type. Choose one of the following options: • Communications Manager—The Cisco Unified Communications Manager sets the directory number type. • International—Use when you are dialing outside the dialing plan for your country. • National—Use when you are dialing within the dialing plan for your country. • Unknown—The dialing plan is unknown. • Subscriber—Use when you are dialing a subscriber by using a shortened subscriber number.

Field	Description
Calling party IE number type unknown	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: • Communications Manager—The Cisco Unified Communications Manager sets the directory number type. • International—Use when you are dialing outside the dialing plan for your country. • National—Use when you are dialing within the dialing plan for your country. • Unknown—The dialing plan is unknown. • Subscriber—Use when you are dialing a subscriber by using a shortened subscriber number.
Called Numbering Plan	Choose the format for the numbering plan in called party directory numbers. Cisco Unified Communications Manager sets the called DN numbering plan. 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 PBXs by using routing as a non-national type number. Choose one of the following options: • Communications Manager—The Cisco Unified Communications Manager sets the Numbering Plan in the directory number. • ISDN—Use when you are dialing outside the dialing plan for your country. • National Standard—Use when you are dialing within the dialing plan for your country. • Private—Use when you are dialing within a private network. • Unknown—The dialing plan is unknown. • Subscriber—Use when you are dialing a subscriber by using a shortened subscriber number.

Field	Description
Calling Numbering Plan	Choose the format for the numbering plan in calling party directory numbers. Cisco Unified Communications Manager sets the calling DN numbering plan. 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 PBXs by using routing as a non-national type number. Choose one of the following options: • Communications Manager—The Cisco Unified Communications Manager sets the Numbering Plan in the directory number. • ISDN—Use when you are dialing outside the dialing plan for your country. • National Standard—Use when you are dialing within the dialing plan for your country. • Private—Use when you are dialing within a private network. • Unknown—The dialing plan is unknown. • Subscriber—Use when you are dialing a subscriber by using a shortened subscriber number.
Number of digits to strip	Choose the number of digits to strip on outbound calls, from 0 to 32. For example, when 8889725551234 is dialed, and the number of digits to strip is 3, Cisco Unified Communications Manager strips 888 from the outbound number.
Caller ID DN	Enter the pattern that you want to use for caller ID, from 0 to 24 digits. For example, in North America • 555XXXX = Variable caller ID, where X equals an extension number. The CO appends the number with the area code if you do not specify it. • 5555000 = Fixed caller ID, where you want the Corporate number to be sent instead of the exact extension from which the call is placed. The CO appends the number with the area code if you do not specify it. You can also enter the international escape character +.
Incoming Calling Party Settings	
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.

Field	Description
National Number	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 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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. • Strip Digits—Enter the number of digits, up to the number 24, 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—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 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. 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. **Tip** For more information on configuring these settings, see topics related to location configuration in the *Cisco Unified Communications Manager Features and Services Guide*.

Field	Description
International Number	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 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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. • Strip Digits—Enter the number of digits, up to the number 24, 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— 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 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. 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. **Tip** For more information on configuring these settings, see topics related to location configuration in the *Cisco Unified Communications Manager Features and Services Guide*.

Field	Description
Subscriber Number	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 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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. • Strip Digits—Enter the number of digits, up to the number 24, 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 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. 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. **Tip** For more information on configuring these settings, see topics related to location configuration in the *Cisco Unified Communications Manager Features and Services Guide*.

Field	Description
Unknown Number	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 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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. • Strip Digits—Enter the number of digits, up to the number 24, 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—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 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. 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. **Tip** For more information on configuring these settings, see topics related to configuring the incoming calling party settings for a device pool, gateway, or trunk in the *Cisco Unified Communications Manager Features and Services Guide*.
Incoming Called Party Settings	
Clear Prefix Settings	To delete all prefixes for all called party number types, click Clear Prefix Settings.
Default Prefix Settings	To enter the default value for all prefix fields at the same time, click Default Prefix Settings.

Field	Description
National Number	Configure the following settings to transform incoming called party numbers that use National for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called party numbers that use National for the Called Party Numbering Type. You can enter up to 16 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, you cannot configure the Strip Digits field. 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 called party prefix, which supports both the prefix and strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, 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 called party number of National type before it applies the prefixes. • Use Device Pool CSS— 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 the device. • Calling Search Space—This setting allows you to transform the called party number of National called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

Field	Description
International Number	Configure the following settings to transform incoming called party numbers that use International for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called party numbers that use International for the Called Party Numbering Type. You can enter up to 16 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, you cannot configure the Strip Digits field. 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 called party prefix, which supports both the prefix and strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, 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 called party number of International type before it applies the prefixes. • Use Device Pool CSS—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 the device. • Calling Search Space—This setting allows you to transform the called party number of International called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

Field	Description
Unknown Number	Configure the following settings to transform incoming called party numbers that use Unknown for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called numbers that use Unknown for the Called Party Numbering Type. You can enter up to 16 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, you cannot configure the Strip Digits field. 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 called party prefix, which supports both the prefix and strip digit functionality. **Tip** To configure the Strip Digits field, 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 called party number of Unknown type before it applies the prefixes. • Use Device Pool CSS—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 the device. • Calling Search Space—This setting allows you to transform the called party number of Unknown called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

Field	Description
Subscriber Number	Configure the following settings to transform incoming called party numbers that use Subscriber for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called numbers that use Subscriber for the Called Party Numbering Type. You can enter up to 16 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, you cannot configure the Strip Digits field. 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 called party prefix, which supports both the prefix and strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, 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 called 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 transform the called party number of Subscriber called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.
BRI Protocol Type Specific Information	
Redirecting Number IE Delivery— Outbound	Check this check box to indicate the first redirecting number and the redirecting reason of the call when the call is forwarded. (The UUIE part of the outgoing SETUP message from the Cisco Unified Communications Manager includes the Redirecting Number IE.) Uncheck the check box to exclude the first redirecting number and the redirecting reason. You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box. **Note** Default leaves the check box checked.

Field	Description
Redirecting Party Transformation CSS	This setting allows you to transform the redirecting party number on the device to another format such as DID or E164 format. Cisco Unified Communications Manager includes the transformed number in the Redirecting Number Information Element of MGCP setup message sent out of Cisco Unified Communications Manager. Make sure that the Redirecting Party Transformation CSS that you choose contains either the calling or called party transformation pattern that you want to assign to this MGCP gateway. **Note** If you configure the Redirecting Party Transformation CSS as None and also uncheck the Use Device Pool Redirecting Party CSS check box, the transformation does not match and does not get applied. Ensure that you configure the Redirecting Party Transformation CSS in a non-null partition that is not used for routing.
Use Device Pool Redirecting Party Transformation CSS	To use the Redirecting 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 Redirecting Party Transformation CSS that you configured in the MGCP Gateway Configuration window.
Redirecting Number IE Delivery— Inbound	Check this check box to accept the Redirecting Number IE in the incoming SETUP message to the Cisco Unified Communications Manager. (The UUIE part of the SETUP message includes the Redirecting Number IE.) Uncheck the check box to exclude the Redirecting Number IE. You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box. **Note** Default leaves the check box checked.
Setup non-ISDN Progress Indicator IE Enable	Default leaves this setting disabled (unchecked). Enable this setting only if users are not receiving ringback tones on outbound calls. When this setting is enabled, the Cisco Unified Communications Manager sends Q.931 Setup messages out digital (that is, non-H.323) gateways with the Progress Indicator field set to non-ISDN. This message notifies the destination device that the Cisco Unified Communications Manager gateway is non-ISDN and that the destination device should play in-band ringback. This problem usually associates with Cisco Unified Communications Managers that connect to PBXs through digital gateways.
Product-Specific Configuration	

Field	Description
Model-specific configuration fields that are defined by the gateway manufacturer	The model-specific fields under product-specific configuration define the gateway manufacturer. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the "?" information icon to the right of the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, see the documentation for the specific gateway that you are configuring or contact the manufacturer.

Related Topics

Location Setup , on page 127
Gateway Setup , on page 465

POTS Port Settings

The following table describes the POTS port configuration settings.

Table 90: POTS Port Configuration Settings

Field	Description
Port Selection	
Port Type	For POTS ports, this field displays POTS.
Beginning Port Number Ending Port Number	Choose whether you want to add and configure all available ports, a single port, or a range of ports by setting values for the Beginning Port Number and Ending Port Number fields: • To specify a range of ports, choose appropriate values for Beginning Port Number and Ending Port Number. • To create a single port, choose the same number in the Beginning Port Number and Ending Port Number fields. • To add all available ports, choose All Ports for both the Beginning Port Number and Ending Port Number fields.
Port Details	
Port Direction	Choose the direction of calls that pass through this port: • Inbound—Use for incoming calls only. • Outbound—Use for outgoing calls. • Bothways—Use for inbound and outbound calls (default).

Field	Description
Audio Signal Adjustment into IP Network	This field specifies the gain or loss that is applied to the received audio signal relative to the port application type. **Note** Improper gain setting may cause audio echo. Use caution when you are adjusting this setting.
Audio Signal Adjustment from IP Network	This field specifies the gain or loss that is applied to the transmitted audio signal relative to the port application type. **Note** Improper gain setting may cause audio echo. Use caution when you are adjusting this setting.
Prefix DN	Enter the prefix digits that are appended to the digits that this gateway receives on incoming calls. The Cisco Unified Communications Manager adds prefix digits after it truncates the number in accordance with the Num Digits setting. You can enter the international escape character +.
Num Digits	Enter the number of significant digits to collect, from 0 to 32. Cisco Unified Communications Manager counts significant digits from the right (last digit) of the number that is called. Use this field for the processing of incoming calls and to indicate the number of digits starting from the last digit of the called number that are used to route calls that are coming into the PRI span. See Prefix DN.
Expected Digits	Enter the number of digits that are expected on the inbound side of the trunk. For this rarely used field, leave zero as the default value if you are unsure.
Call Restart Timer (1000-5000 ms)	Call Restart Timer (1000-5000 ms); ms indicates time in milliseconds.
Offhook Validation Timer (100-1000 ms)	Offhook Validation Timer (100-1000 ms); ms indicates time in milliseconds.
Onhook Validation Timer (100-1000 ms)	Onhook Validation Timer (100-1000 ms); ms indicates time in milliseconds.
Hookflash Timer (100-1500 ms)	Hookflash Timer (100-1500 ms); ms indicates time in milliseconds.
Unattended Port	Check this check box to indicate an unattended port on this device.
Product-Specific Configuration	

Field	Description
Model-specific configuration fields that the gateway manufacturer defines	The gateway manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the "?" information icon to the right of the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, see the documentation for the specific gateway that you are configuring or contact the manufacturer.

Related Topics

Gateway Setup , on page 465

Loop-Start Port Settings

The following table describes the loop-start port configuration settings.

Table 91: Loop-Start Port Configuration Settings

Field	Description
Port Type	From the Port Type drop-down list box, choose Loop Start.
Beginning Port Number Ending Port Number	Choose whether you want to add and configure all available ports, a single port, or a range of ports by setting values for the Port Number and End Port Number fields: • To specify a range of ports, choose appropriate values for Beginning Port Number and Ending Port Number. • To create a single port, choose the same number in the Beginning Port Number and Ending Port Number fields. • To add all available ports, choose All Ports for both the Beginning Port Number and Ending Port Number fields.
Port Direction	Choose the direction of calls that pass through this port: • Inbound—Use for incoming calls only. • Outbound—Use for outgoing calls. • Both Ways—Use for inbound and outbound calls.
Attendant DN	Enter the directory number to which you want incoming calls routed; for example, zero or a directory number for an attendant.
Unattended Port	Check this check box to indicate an unattended port on this device.

Field	Description
Product-Specific Configurations	
Model-specific configuration fields that the gateway manufacturer defines	The gateway manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the "?" information icon to the right of the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, see the documentation for the specific gateway that you are configuring or contact the manufacturer.

Related Topics

Gateway Setup , on page 465

Ground-Start Port Settings

The following table describes the ground-start port configuration settings.

Table 92: Ground-Start Port Configuration Settings

Field	Description
Port Type	From the Port Type drop-down list box, choose Ground Start.
Beginning Port Number Ending Port Number	Choose whether you want to add and configure all available ports, a single port, or a range of ports by setting values for the Beginning Port Number and Ending Port Number fields: • To specify a range of ports, choose appropriate values for Beginning Port Number and Ending Port Number. • To create a single port, choose the same number in the Beginning Port Number and Ending Port Number fields. • To add all available ports, choose All Ports for both the Beginning Port Number and Ending Port Number fields.
Port Direction	Choose the direction of calls that pass through this port: • Inbound—Use for incoming calls only. • Outbound—Use for outgoing calls. • Both Ways—Use for inbound and outbound calls.
Attendant DN	Enter the number to which you want incoming calls to be routed; for example, zero or a directory number for an attendant.

Field	Description
Unattended Port	Check this check box to indicate an unattended port on this device.
Product-Specific Configuration	
Model-specific configuration fields that the gateway manufacturer defines	The gateway manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the "?" information icon to the right of the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, see the documentation for the specific gateway that you are configuring or contact the manufacturer.

Related Topics

Gateway Setup , on page 465

E and M Port Settings

E & M (Ear and Mouth) ports allow connection for PBX trunk lines (tie lines). E & M designates a signaling technique for two-wire, four-wire, and six-wire telephone and trunk interfaces.

The following table describes the E & M port configuration settings.

Table 93: E and M Port Configuration Settings

Field	Description
Port Type	From the Port Type drop-down list box, choose EANDM.
Beginning Port Number Ending Port Number	Choose whether you want to add and configure all available ports, a single port, or a range of ports by setting values for the Beginning Port Number and Ending Port Number fields: • To specify a range of ports, choose appropriate values for Beginning Port Number and Ending Port Number. • To create a single port, choose the same number in the Beginning Port Number and Ending Port Number fields. • To add all available ports, choose All Ports for both the Beginning Port Number and Ending Port Number fields.
Port Details	

Field	Description
Port Direction	Choose the direction of calls that pass through this port: • Inbound—Use for incoming calls only. • Outbound—Use for outgoing calls. • Both Ways—Use for inbound and outbound calls.
Calling Party Selection	Any outbound call on a gateway can send directory number information. Choose which directory number is sent: • Originator—Send the directory number of the calling device. • First Redirect Number—Send the directory number of the redirecting device. • Last Redirect Number—Send the directory number of the last device to redirect the call. • First Redirect Number (External)—Send the directory number of the first redirecting device with the external phone mask applied. • Last Redirect Number (External)—Send the directory number of the last redirecting device with the external phone mask applied.
Caller ID Type	Choose the caller ID type: • ANI—Choose this type to use the Asynchronous Network Interface (ANI) caller ID type. • DNIS—Choose this type to use the Dialed Number Identification Service (DNIS) caller ID type.
Caller ID DN	Enter the pattern that you want to use for calling line ID, from 0 to 24 digits. For example, in North America • 555XXXX = Variable calling line ID, where X equals an extension number. The CO appends the number with the area code if you do not specify it. • 5555000 = Fixed calling line ID, where you want the Corporate number to be sent instead of the exact extension from which the call is placed. The CO appends the number with the area code if you do not specify it. You can also enter the international escape character +.
Prefix DN	Enter the prefix digits that are appended to the called party number on incoming calls. The Cisco Unified Communications Manager adds prefix digits after first truncating the number in accordance with the Num Digits setting. You can enter the international escape character +.

Field	Description
Num Digits	Choose the number of significant digits to collect, from 0 to 32. Cisco Unified Communications Manager counts significant digits from the right (last digit) of the number that is called. Use this field if you check the Sig Digits check box. Use this field for the processing of incoming calls and to indicate the number of digits starting from the last digit of the called number that are used to route calls that are coming into the PRI span. See Prefix DN and Sig Digits.
Expected Digits	Enter the number of digits that are expected on the inbound side of the trunk. If you are unsure, leave zero as the default value for this rarely used field.
Product-Specific Configuration	
Model-specific configuration fields that the gateway manufacturer defines	The gateway manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the "?" information icon to the right of the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, see the documentation for the specific gateway that you are configuring or contact the manufacturer.

Related Topics

Gateway Setup , on page 465

Add Gateway to Cisco Unified Communications Manager

To enable Cisco Unified Communications Manager to manage IP telephony gateways in your network, you must first add each gateway to the Cisco Unified Communications Manager configuration database. The procedures, windows, and configuration settings for adding a gateway vary according to the gateway model that you are adding.

The following procedure describes how to add a new gateway in Cisco Unified Communications Manager.

Procedure

Step 1 To display the Find and List Gateways window, choose **Device** > **Gateway**.

Step 2 Click the Add New button. The Add a New Gateway window displays.

Step 3 From the Gateway Type drop-down list box, choose the gateway type that you want to add. The Device Protocol field may automatically get populated depending on gateway type that you choose.

Step 4 Click Next.

Step 5 In Table 94: Gateways, on page 564, click the specific procedure for the gateway type that you are configuring. After you are in the correct procedure, start with the step where you enter the appropriate settings for that particular gateway type.

Gateway Addition Associated Procedures

The following table lists the procedure to add a gateway for each type of gateway that is supported.

Table 94: Gateways

Type of Gateway	Procedure to Add
Cisco Voice Gateway 200 (VG200) VG224 Gateway Cisco IOS 269X, 26XX, 362X, 364X, 366X, 3725, 3745 Gateways Cisco 2801, 2811, 2821, 2851, 3825, 3845 Gateways Cisco Catalyst 4000 Access Gateway Module Cisco Catalyst 4224 Voice Gateway Switch Communication Media Module Cisco IAD2400	Use the procedure to add a Cisco IOS MGCP gateway.
Cisco IOS 269X, 3725, 3745 Gateways	Use the procedure to add a Cisco IOS SCCP gateway.
Cisco Catalyst 6000 E1 VoIP Gateway Cisco Catalyst 6000 T1 VoIP Gateway	Use the procedure to add a Non-IOS MGCP gateway.
Other Cisco IOS Gateway that is configured in H.323 mode	Use the procedure to add a Cisco IOS H.323 gateway.
Cisco Catalyst 6000 24 Port FXS Gateway	Use the procedure to add an analog access gateway and ports.
Cisco VG248 Gateway	Use the procedure to add a Cisco VG248 analog phone gateway.

Related Topics

Add Cisco IOS MGCP Gateway , on page 565
Add Cisco IOS SCCP Gateway , on page 571
Add Non-IOS MGCP Gateway , on page 572
Add Cisco IOS H.323 Gateway , on page 573
Add Analog Access Gateway and Ports , on page 574
Add Cisco VG248 Analog Phone Gateway , on page 574

Add Cisco IOS MGCP Gateway

Use the following procedure to add and configure a Cisco IOS MGCP gateway to Cisco Unified Communications Manager. The following Cisco IOS gateways support MGCP:

- CiscoVG200 Voice Gateway
- VG224 Gateway
- Cisco IOS 362x, 364x, 366x Gateways
- Cisco IOS 3725 and 3745 Gateways
- Cisco IOS 26xx and 269x Gateways
- Cisco 2801, 2811, 2821, 2851, 3825, 3845 Gateways
- Cisco Catalyst 4000 Access Gateway Module
- Cisco Catalyst 4224 Voice Gateway Switch
- Communication Media Module
- Cisco IAD2400 gateways

Note Like other IOS MGCP gateways, MRP/ASI gateways may work with a Cisco Unified Communications Manager group that contains three Cisco Unified Communications Managers. ASI/MRP gateways testing occurs, however, with only one backup Cisco Unified Communications Manager.

Before You Begin

Before configuring a Cisco IOS MGCP gateway for use with Cisco Unified Communications Manager, you must configure the gateway by using the Cisco IOS command-line interface (CLI). For procedures and commands that are required to perform this configuration, see the configuration documentation that is supplied with the gateway.

Procedure

Step 1 To display the Find and List Gateways window, choose **Device** > **Gateway**.

Step 2 Click the Add New button. The Add a New Gateway window displays.

Step 3 From the Gateway Type drop-down list box, choose one of the following MGCP gateways:

a) Cisco VG200
b) VG224
c) Cisco 362X, 364X, 366X
d) Cisco 3725 and 3745
e) Cisco 26XX and 269X
f) Cisco 2801, 2811, 2821, 2851, 3825, 3845
g) Cisco Catalyst 4000 Access Gateway Module
h) Cisco Catalyst 4224 Voice Gateway Switch
i) Communication Media Module
j) Cisco IAD2400

Note The Cisco Catalyst 6000 gateways also support MGCP but are configured differently.

Cisco IOS MGCP gateways support different device protocols for interfacing to the PSTN or other non-IP devices, depending on the gateway model and the type of installed network modules and voice interface cards (VICs). A subsequent web window provides configuration for these interfaces.

Step 4 Click Next.

Step 5 If a Protocol drop-down list box displays, choose MGCP and click Next. Otherwise, skip to Step 6, on page 566.

Step 6 The appropriate Gateway Configuration window displays.
Enter the appropriate settings and choose the type of network modules that are installed in each slot, as described in the Table 81: MGCP Gateway Configuration Settings , on page 467, including any product-specific configuration settings.

Step 7 Click Save.
The Gateway Configuration window updates and displays drop-down list boxes with options for configuring the type of voice interface cards (VICs) in each subunit of each network module.

The available choices depend on the type of network modules that are configured in the Gateway Configuration window.

Step 8 From the drop-down list boxes, choose the type of VICs that are installed in each subunit and click Save.
The window updates to add links for configuring endpoint information and ports for the chosen type of VICs.

Step 9 Click an endpoint identifier (for example, 1/0/0) to configure device protocol information and add ports for the installed types of VICs.
See the related topics for links to the detailed instructions.

Step 10 To reset the gateway and apply the changes, click Reset.

Step 11 Continue configuring endpoint information and ports as needed.

Step 12 After you finish configuring the endpoint and adding ports, you need to add the MGCP gateway device to a route group/route list or assign a route pattern to the gateway, so calls can be routed to the gateway.

Note You need to add the MGCP gateway to a route pattern only for outbound calling.

Related Topics

Add FXS Ports to MGCP Gateway , on page 567
Add FXO Ports To MGCP Gateway , on page 568
Add Digital Access T1 Ports to MGCP Gateway , on page 569
Add Digital Access PRI Device to MGCP Gateway , on page 570
Add BRI Port to MGCP Gateway , on page 570
Add Non-IOS MGCP Gateway , on page 572

Add Ports to MGCP Gateway

The device protocols and port types that can be configured on MGCP gateways vary by the type of installed voice interface cards.

Related Topics

Add FXS Ports to MGCP Gateway , on page 567
Add FXO Ports To MGCP Gateway , on page 568
Add Digital Access T1 Ports to MGCP Gateway , on page 569
Add Digital Access PRI Device to MGCP Gateway , on page 570
Add BRI Port to MGCP Gateway , on page 570

Add FXS Ports to MGCP Gateway

You can use Foreign Exchange Station (FXS) ports to connect to any POTS device. Use this procedure to configure FXS ports on an MGCP gateway.

Before You Begin

You must add an MGCP gateway before configuring ports.

Procedure

Step 1 To display the Find and List Gateways window, choose **Device** > **Gateway** or skip to Step 4, on page 567 if you have already located the MGCP gateway to which you want to add FXS ports.

Step 2 Enter the appropriate search criteria to locate the MGCP gateway to which you want to add FXS ports.

Step 3 Click the name of the desired gateway to display its MGCP configuration settings and endpoint identifiers.

Step 4 From the Gateway Configuration window, click the endpoint identifier for the FXS VIC that you want to configure.
The window refreshes and displays the Gateway Configuration window.

Step 5 Enter the appropriate Gateway Information and Port Information settings. See the following for details about these fields:

- FXS/FXO Port Settings , on page 500
- POTS Port Settings , on page 557

Step 6 Click Save.

Note After you insert a POTS port, the window refreshes and displays the POTS port information at the bottom of the window. An Add a new DN link displays below the new port.

Step 7 Click Add a new DN to add directory numbers to the POTS port or, if you configured another type of port, go to Step 9, on page 568.

Step 8 To return to the main MGCP gateway configuration window for the gateway to which you just added the ports, choose Back to MGCP Configuration in the Related Links drop-down list box and click Go.

Step 9 To reset the gateway and apply the changes, click Reset.

Step 10 Repeat Step 4, on page 567 through Step 8, on page 568 to add additional FXS ports.

Related Topics

About Directory Number Setup , on page 289
Gateway Setup , on page 465

Add FXO Ports To MGCP Gateway

You can use Foreign Exchange Office (FXO) ports for connecting to a central office or PBX. Use this procedure to add and configure FXO ports for loop start or ground start on an MGCP gateway.

Note Cisco Unified Communications Manager assumes all loop-start trunks lack positive disconnect supervision. Configure trunks with positive disconnect supervision as ground start, so active calls can be maintained during a Cisco Unified Communications Manager server failover.

Before You Begin

You must add an MGCP gateway before configuring ports.

Procedure

Step 1 To display the Find and List Gateways window, choose **Device** > **Gateway** or skip to Step 4, on page 568 if you have already located the MGCP gateway to which you want to add FXO ports.

Step 2 Enter the appropriate search criteria to locate the MGCP gateway to which you want to add FXO ports and click Find. The search results window displays.

Step 3 Click the name of the desired gateway to display its MGCP configuration settings and endpoint identifiers.

Step 4 From the MGCP Configuration window, click the endpoint identifiers of the FXO port that you want to configure.

Step 5 From the Port Type drop-down list box, choose either Ground Start or Loop Start.

Note You must choose the same port type for both endpoint identifiers of the VIC-2FXO port. If you choose different port types, a message displays.

Step 6 Enter the appropriate Gateway Configuration and Port Information settings. See the following for details about these fields:

a) FXS/FXO Port Settings , on page 500

b) Loop-Start Port Settings , on page 559

c) Ground-Start Port Settings , on page 560

Step 7 Click Save.

Step 8 To return to the main MGCP gateway configuration window for the gateway to which you just added the ports, choose Back to MGCP Configuration in the Related Links drop-down list box and click Go.

Step 9 To reset the gateway and apply the changes, click Reset.

Step 10 To add more FXO ports, repeat Step 4, on page 568 though Step 7, on page 569.

Related Topics

Gateway Setup , on page 465

Add Digital Access T1 Ports to MGCP Gateway

Use this procedure to add Digital Access T1 (T1-CAS) ports to an MGCP gateway.

Procedure

Step 1 To display the Find and List Gateways window, choose **Device** > **Gateway** or skip to Step 4 if you have already located the MGCP gateway to which you want to add T1-CAS ports.

Step 2 To locate the MGCP gateway to which you want to add a Digital Access T1 (T1-CAS) port, enter the appropriate search criteria.

Step 3 To display its MGCP configuration settings and endpoint identifiers, click the name of the desired gateway.

Step 4 From the Gateway Configuration window, click the endpoint identifier of the Digital Access T1 (T1-CAS) port that you want to configure.
In the Device Protocol drop-down list box that displays, choose Digital Access T1 and click Next.

See the related topics for links to find the appropriate settings for the port type that you choose.

Step 5 Enter the appropriate Gateway Configuration settings.
See the Table 88: Digital Access T1 Port Configuration Settings , on page 533 for details.

Step 6 Click Save.

Step 7 To reset the gateway and apply the changes, click Reset.

Related Topics

Gateway Setup , on page 465
Port Setup , on page 500

Add Digital Access PRI Device to MGCP Gateway

Procedure

Step 1 To display the Find and List Gateways window, choose **Device** > **Gateway** or skip to Step 4, on page 567 if you have already located the MGCP gateway to which you want to add a port.

Step 2 To locate the MGCP gateway to which you want to add a T1 PRI or E1 PRI port, enter the appropriate search criteria.

Step 3 To display the configuration information for the selected gateway, click the name of the desired gateway in the list.

Step 4 From the Gateway Configuration window, click the endpoint identifier of the T1 PRI or E1 PRI port that you want to configure.

Step 5 Configure the T1 PRI or E1 PRI device protocol settings. See the Table 87: Digital Access PRI Port Configuration Settings , on page 508 for detailed field descriptions.

Step 6 Click Save.

Step 7 To reset the gateway and apply the changes, click Reset.

Related Topics

Gateway Setup , on page 465

Add BRI Port to MGCP Gateway

The device protocols and port types that you can configure on MGCP gateways vary by the type of installed voice interface cards (VICs). This section contains the procedures for adding a BRI port to an MGCP gateway.

Procedure

Step 1 To display the Find/List Gateways window, choose **Device** > **Gateway**, or if you have already located the MGCP gateway to which you want to add a port, skip to Step 4, on page 568.

Step 2 To locate the MGCP gateway to which you want to add a BRI port, enter the appropriate search criteria.

Step 3 To display the configuration information for the chosen gateway, click the name of the desired gateway in the list.

Step 4 From the MGCP Configuration window, click the endpoint identifier of the BRI port that you want to configure.

Step 5 Configure the BRI device protocol settings. See the Table 89: BRI Port Configuration Settings , on page 540 for detailed field descriptions.

Step 6 Click Save.

Step 7 To apply the changes, reset the gateway.

Related Topics

Gateway Setup , on page 465

Add Cisco IOS SCCP Gateway

Use the following procedure to add and configure a Cisco IOS SCCP gateway to Cisco Unified Communications Manager. The following Cisco IOS gateways support SCCP:

- Cisco IOS 269xGateways
- Cisco IOS 3725 and 3745 Gateways
- Cisco VG224 Gateway

Before You Begin

Configure a Cisco IOS SCCP gateway by adding the gateway first to Cisco Unified Communications Manager. Afterward, configure the gateway by using the Cisco IOS command-line interface (CLI). For procedures and commands that are required to perform this configuration, see the configuration documentation that is supplied with the gateway.

Procedure

Step 1 Choose **Device** > **Gateway**.
The Find and List Gateway window displays.

Step 2 Click Add New.
The Add a New Gateway window displays.

Step 3 From the Gateway Type drop-down list box, choose one of the following SCCP gateways:
a) Cisco IOS 269x
b) Cisco IOS 3725 and 3745

Step 4 From the Protocol drop-down list box, choose SCCP.
Cisco IOS SCCP gateways support SCCP for interfacing to the PSTN or other non-IP devices, depending on the gateway model and the type of installed network modules and voice interface cards (VICs). A subsequent web window provides configuration for the interface.

Step 5 Click Next.
The Gateway Configuration window displays for this SCCP gateway.

Step 6 Enter the appropriate settings and choose the type of network modules that are installed in each slot, as described in Table 85: Cisco IOS SCCP Gateway Configuration Settings , on page 498, including any product-specific configuration settings.

Step 7 Click Save.
The Gateway Configuration window updates and displays drop-down list boxes with options for configuring the type of voice interface cards (VICs) in each subunit of each network module.

The available choices depend on the type of network modules that are configured in the Gateway Configuration window.

Step 8 From the drop-down list boxes, choose the type of VICs that are installed in each subunit and click Save.
The window updates to add links for configuring endpoint information and ports for the chosen type of VICs.

Step 9 Click an endpoint identifier (for example, 1/0/0) to configure device protocol information, add ports for the installed types of VICs, and add FXS/BRI port to a SCCP gateway. See the related topics for details of configuring the analog phones.

Step 10 Reset the gateway to apply the changes.

Step 11 Continue configuring endpoint information and ports as needed.

Related Topics

Cisco Unified IP Phone Setup , on page 579
Set Up Speed-dial Buttons or Abbreviated Dialing , on page 625

Add Non-IOS MGCP Gateway

Use the following procedure to add the following non-IOS Cisco MGCP gateways to Cisco Unified Communications Manager:

- Cisco Catalyst 6000 E1 VoIP Gateway
- Cisco Catalyst 6000 T1 VoIP Gateway

Procedure

Step 1 To display the Find and List Gateways window, choose **Device** > **Gateway**.

Step 2 Click the Add New button.
The Add a New Gateway window displays.

Step 3 From the Gateway Type drop-down list box, choose one of the following digital gateways and click Next:

a) Cisco Catalyst 6000 E1 VoIP Gateway
b) Cisco Catalyst 6000 T1 VoIP Gateway

Step 4 From the drop-down list box, choose the appropriate device protocol for the type of interfaces that you are configuring on the gateway. The available choices vary according to gateway model:

a) Cisco Catalyst 6000 T1 VoIP Gateway—Choose either Digital Access PRI or Digital Access T1.
b) Cisco Catalyst 6000 E1 VoIP Gateway—The Digital Access PRI device protocol automatically gets chosen, and the Gateway Configuration window displays. Skip to Step 6, on page 572.

Step 5 Click Next.
The Gateway Configuration window displays.

Step 6 Enter the appropriate settings, depending on whether you are configuring a Digital Access PRI interface or a Digital Access T1 interface as described in following sections:

- Digital Access PRI Port Settings , on page 507
- Digital Access T1 Port Settings , on page 533

Step 7 Click Save.

Step 8 If you are configuring a Digital Access T1 interface on a Catalyst 6000 T1 VoIP Gateway, in the Ports pane that displays on the left side of the window, click Add a New Port link to configure ports.

Step 9 To reset the gateway and apply the changes, click Reset.

Related Topics

Gateway Setup , on page 465
Add Digital Access T1 Ports to MGCP Gateway , on page 569

Add Cisco IOS H.323 Gateway

Perform the following procedures to add a Cisco IOS H.323 Gateway to Cisco Unified Communications Manager.

Note After a gateway is registered with Cisco Unified Communications Manager, gateway registration status may display in Cisco Unified Communications Manager Administration as unknown.

Before You Begin

Before configuring a Cisco IOS H.323 gateway for use with Cisco Unified Communications Manager, you must configure the gateway by using the Cisco IOS command-line interface (CLI). Compared to MGCP gateways, H.323 gateways require more configuration on the gateway because the gateway must maintain the dial plan and route pattern. For procedures and commands that are required to perform this configuration, see the configuration documentation that is supplied with the gateway.

Procedure

Step 1 To display the Find and List Gateways window, choose **Device** > **Gateway**.

Step 2 Click the Add New button.
The Add a New Gateway window displays.

Step 3 From the Gateway Type drop-down list box, choose H.323 Gateway.

Step 4 Click Next.

Step 5 Enter the appropriate settings as described in Table 82: H.323 Gateway Configuration Settings, on page 470.

Step 6 Click Save.

Step 7 To reset the gateway and apply the changes, click Reset.

Related Topics

Gateway Setup , on page 465

Add Analog Access Gateway and Ports

Perform the procedure in this section to add and configure ports for the Cisco Catalyst 6000 24 Port FXS Gateway.

Procedure

Step 1 To display the Find and List Gateways window, choose **Device** > **Gateway**.

Step 2 Click the Add New button.
The Add a New Gateway window displays.

Step 3 From the Gateway type drop-down list box, choose Cisco Catalyst 6000 24 Port FXS Gateway.

Step 4 Click Next.
The Gateway Configuration window displays.

Step 5 Enter the appropriate settings, as described in the Table 83: Analog Access Gateway Configuration Settings , on page 492.

Step 6 Click Save.

Step 7 To add a port to this gateway, click the Add a New Port link in the Ports pane that displays on the left side of the window.
The Port Configuration window displays.

Step 8 From the drop-down list box, choose POTS as the port type and click Next.

Step 9 Enter the appropriate port configuration settings as described in the Table 90: POTS Port Configuration Settings , on page 557.

Step 10 Click Save.
If you have inserted POTS ports, the window refreshes and displays the POTS port in the list on the left side of the window. An Add DN link displays to the right of the new port.

Step 11 To add a directory numbers to a POTS port, click Add DN.

Step 12 After you finish adding POTS ports and configuring directory numbers for the POTS ports, you can return to the Gateway Configuration window. In the Related Links drop-down list box, choose Configure Device and click Go.

Step 13 To apply the changes, click Reset.

Related Topics

About Directory Number Setup , on page 289
Gateway Setup , on page 465

Add Cisco VG248 Analog Phone Gateway

The Cisco VG248 Analog Phone Gateway, a standalone, rack-mounted, 48-FXS port product, allows on-premise analog telephones, fax machines, modems, voice-messaging systems, and speakerphones to register with one Cisco Unified Communications Manager cluster.

The Cisco VG248 connects to a Cisco Unified Communications Manager by using the Skinny Client Control Protocol to allow for enhanced features.

Cisco Unified Communications Manager recognizes the Cisco VG248 as a gateway device, called a "Cisco VG248 Gateway." Additionally, Cisco Unified Communications Manager treats each of the 48 ports as an individual device, similar to a Cisco Unified IP Phone, called a "Cisco VGC Phone."

Use the following procedure to add a Cisco VG248 Gateway and to add and configure ports to the gateway.

Procedure

Step 1 To display the Find and List Gateways window, choose **Device** > **Gateway**.

Step 2 Click the Add New button.
The Add a New Gateway window displays.

Step 3 From the Gateway type drop-down list box, choose Cisco VG248 Gateway.

Step 4 Click Next.
The Gateway Configuration window displays.

Step 5 Enter the appropriate settings, as described in the Table 84: Cisco VG248 Gateway Configuration Settings , on page 497.

Step 6 From the Configured Slots, VICs and Endpoints drop-down list box, choose 48_PORTS.

Step 7 Click Save.
The ports 0 through 48 display in the Configured Slots, VICs, and Endpoints area.

Step 8 Click a port.
The Phone Configuration window displays and lists the phone model as Cisco VGCPhone. From the Gateway Configuration window, the MAC address automatically displays.

Step 9 Enter the appropriate settings. See the related topics link to configuring speed-dial buttons or abbreviated dialing for more information.

Step 10 Click Save.

Step 11 To configure a directory number for the port, click the Add a New DN link that displays in the Association Information area on the left side of the window.
The Directory Number Configuration window displays. For information about adding and configuring directory numbers, see the related topics.

Step 12 To configure more ports for the gateway, from the Related Link drop-down list box, choose the Back to Gateway link and click Go.
The Gateway Configuration window displays. To configure the phone settings and directory numbers for additional ports, repeat Step 8, on page 575 through Step 11, on page 575.

When you configure port 1, the Create all new ports like port 1 button displays at the top of the Gateway Configuration window. This button allows you to configure ports 2 through 48 with the same parameters and settings as port 1, but only if ports 2 through 48 are not configured.

Step 13 To apply the changes, click Reset.

Related Topics

About Directory Number Setup , on page 289

Gateway Setup , on page 465
Set Up Speed-dial Buttons or Abbreviated Dialing , on page 625

Gateway and Port Modification

Using Cisco Unified Communications Manager, you can synchronize, as well as update gateways and ports for all gateway types.

Related Topics

Synchronize Gateway , on page 576
Update Gateways and Ports , on page 576

Synchronize Gateway

To synchronize a gateway with the most recent configuration changes, perform the following procedure, which applies 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 **Device** > **Gateway**.
The Find and List Gateways window displays.

Step 2 Choose the search criteria to use.

Step 3 Click Find.
The window displays a list of gateways that match the search criteria.

Step 4 Check the check boxes next to the gateways that you want to synchronize. To choose all gateways 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.

Related Topics

Gateway Setup , on page 465

Update Gateways and Ports

Complete the following steps to update a gateway or reconfigure gateway ports from Cisco Unified Communications Manager.

Procedure

Step 1 Choose **Device** > **Gateway**.

The Find and List Gateways window displays.

Step 2 To locate a specific gateway, enter search criteria.

Step 3 Click Find.
A list of discovered devices displays.

Step 4 Click the Device Name of the gateway that you want to update.
The Gateway Configuration window displays.

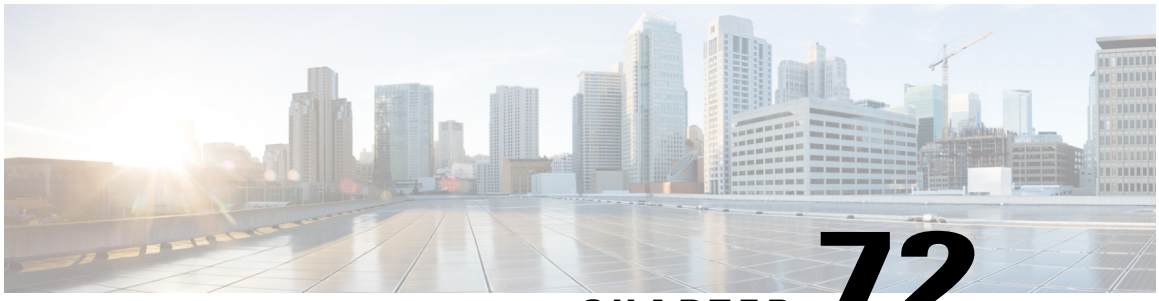
Step 5 Update the appropriate gateway or port settings as described in the related topics links.
To access gateway ports, click the icon of the gateway port or the MGCP endpoint link on the left side of the configuration window for the chosen gateway.

Step 6 Click Save.

Step 7 To apply the changes, click Reset to reset the gateway.

Related Topics

Gateway Setup , on page 465
MGCP Gateway Settings , on page 467
Analog Access Gateway Settings , on page 491
Port Setup , on page 500
FXS/FXO Port Settings , on page 500
Digital Access PRI Port Settings , on page 507
Digital Access T1 Port Settings , on page 533



CHAPTER 72

Cisco Unified IP Phone Setup

This chapter provides information about working with and configuring Cisco Unified IP Phones in Cisco Unified Communications Manager Administration.

About Cisco Unified IP Phones and Device Setup

Cisco Unified IP Phones are full-featured telephones that you can connect directly to your IP network. Use the Cisco Unified Communications Manager Administration Phone Configuration window to configure the following Cisco Unified IP Phones and devices:

- Cisco Unified IP Phone 7900 family for both SCCP and SIP
- Cisco Unified IP Phone 9951 or 9971
- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 6900 family.
- Cisco IP Video Phone 7985
- Cisco Unified IP SIP Phone 3911
- Cisco IP Phone 30 VIP and Cisco IP Phone 30 SP+
- Cisco IP Phone 12 S, Cisco IP Phone 12 SP, Cisco IP Phone 12 SP+
- H.323 clients
- Computer Telephony Integration (CTI) ports

  Be aware that CTI ports may not be associated with directory numbers (DNs) that are members of line groups and, by extension, that are members of hunt lists. If a DN is a member of a line group or hunt list, that DN cannot get associated with a CTI port that you configure with the Phone Configuration window.
- Cisco IP Communicator, Cisco Unified Personal Communicator, and Cisco Unified Mobile Communicator
- Cisco ATA 186 Analog Telephone Adaptor
- Third-party SIP Device (Basic) and (Advanced)
- IP-STE
- Cisco VG248 and VG224 ports (analog phones)

  You configure the Cisco VG248 and VG224 analog phone gateways from the Gateway Configuration window of Cisco Unified Communications Manager Administration. From this window, you configure the gateway analog phone ports (doing this takes you to the Phone Configuration window). When you want to update the VG248 and VG224 ports, use the Phone Configuration window.

See topics related to the Cisco Unified IP Phones in the *Cisco Unified Communications Manager System Guide* lists the configuration steps for Cisco Unified IP Phones that support SIP.

Related Topics

Gateway Setup , on page 465
Non-Cisco SIP Phones Setup , on page 985
Third-Party SIP Phone Setup Process , on page 985

Phone Setup

In Cisco Unified Communications Manager Administration, use the **Device** > **Phone** menu path to configure phones.

Finding Phones Tips

The Cisco VG248 and VG224 Analog Phone Gateways will not display when you search for phones. You can search for the Cisco VG248 and VG224 Analog Phone ports from the Find and List Phones window of Cisco Unified Communications Manager Administration.

Tip For methods to limit your search, see the related topics section and the *Cisco Unified Communications Manager System Guide*.

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. For phones that have an IPv4 address only or both IPv4 and IPv6 addresses, the IPv4 address displays in the window. For phones with an IPv6 address only, the IP Address displays as 0.0.0.0 in the IP Address column in the Find and List Phones window. To identify the IPv6 address for the phone, click the Device Name link in the Find and List Phones window, which causes the Phone Configuration window to display. For the IPv6 Only device, the Phone Configuration window displays an IPv4 address of 0.0.0.0, listed as IP Address, above the IPv6 address.

Phone Configuration Tips

When you add a new phone, you can choose a phone template that was created by the Bulk Administration Tool to configure automatically some of the phone configuration settings, based on the template.

For each phone device type, the Phone Configuration window displays either Device is trusted or Device is not trusted, along with a corresponding icon. The system determines whether the device is trusted, based on the device type. You cannot configure whether the device is trusted.

Note The Product-Specific Configuration section contains model-specific fields that the phone manufacturer defines. Cisco Unified Communications Manager dynamically populates the fields with default values.

To view field descriptions and help for product-specific configuration items, click the "?" question icon in the Product Specific Configuration area to display help in a popup window.

If you need more information, see the documentation for the specific phone that you are configuring or contact the manufacturer.

Select the "Override Common Settings" box for any corresponding setting in the Product Specific Configuration area that you wish to update. If you do not check this box, the corresponding parameter setting does not take effect. Parameters that you set in the Product Specific Configuration area may also appear in the Device Configuration window for various devices and in the Enterprise Phone Configuration window. If you set these same parameters in these other windows too, the setting that takes precedence is determined in the following order: 1) Device Configuration window settings, 2) Common Phone Profile window settings, 3) Enterprise Phone Configuration window settings.

Phone Reset Tips

For instructions on how to reset a phone, see the descriptions of the Reset Selected and Reset buttons.

You do not have to reset a Cisco Unified IP Phone after you add a directory number or update its settings for your changes to take effect. Cisco Unified Communications Manager automatically performs the reset; however, you can reset a Cisco Unified IP Phone at any time by using the following procedure.

Note If a call is in progress, the phone does not reset until the call completes.

You can also updating the phone with the latest configuration changes by using the least-intrusive method.

Related Topics

GUI Buttons and Icons , on page 19
Gateway Setup , on page 465
Cisco Unified IP Phone Setup , on page 579
Phone Settings, on page 583
Set Up Cisco Unified IP Phone , on page 620
Synchronize Phone , on page 625
Find Actively Logged-In Device , on page 632

Phone Deletion Preparation

Before you delete the phone, determine whether the directory number that is associated with the phone needs to be removed or deleted. To remove the directory number before deleting the phone; otherwise, the directory number remains in the Cisco Unified Communications Manager database when the phone gets deleted.

You can view the directory numbers that are assigned to the phone from the Association Information area of the Phone Configuration window. You can also choose Dependency Records from the Related Links drop-down list box in the Phone 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.

Related Topics

Remove Directory Number From Phone , on page 322
Delete Unassigned Directory Number , on page 335
Access Dependency Records , on page 982

Phone Settings

The following table describes the available settings in the Phone Configuration window.

Table 95: Phone Settings

Field	Description
Device Information	
Active Load ID	This field displays the name of the active firmware load if the Cisco Unified IP Phone has registered with Cisco Unified Communications Manager. In some cases, the Active Load ID field displays “Unknown.” For example, Cisco Unified Communications Manager Administration might display “Unknown” in the Active Load ID field for any of the following circumstances: • For SCCP phones, when the phone is a Cisco Unified IP Phone 7940 (SCCP), 7960 (SCCP), or 7985 (SCCP), because these phone models do not support the necessary version of SCCP. • For SCCP and SIP phones, when the phone is any third-party phone. • When Cisco Unified Communications Manager cannot determine the status of the phone.
Device is Active	The Device Is Active message in the Phone Configuration window in Cisco Unified Communications Manager Administration displays when a phone consumes device license units and when a phone can register with Cisco Unified CM. For a phone that uses a real MAC address, not the dummy MAC address that is created via BAT, the Device Is Active message displays, which indicates that the phone uses device license units and can register with Cisco Unified Communications Manager. For a phone that uses the dummy MAC address that is created via BAT, the Device Is Active message does not display. If you manually convert the dummy MAC address to a real MAC address in the Phone Configuration window, the Device Is Active message displays after you save the configuration; this ensures that the phone can register with Cisco Unified Communications Manager and that licensing consumes device license units for the phone.
Device Trust Mode	Select whether the device is trusted or not trusted. You can configure this setting for analog phones using SCCP, and for some third-party endpoints.

Field	Description
MAC Address	Enter the Media Access Control (MAC) address that identifies Cisco Unified IP Phones (hardware phones only). Make sure that the value comprises 12 hexadecimal characters. For information on how to access the MAC address for your phone, see the Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager that supports your phone model. Cisco VG248 Analog Phone Gateway: The MAC address for the Cisco VG248 gateway specifies the endpoint from the Gateway Configuration window of Cisco Unified Communications Manager Administration. Only one MAC address exists for the Cisco VG248 Analog Phone Gateway. All 48 ports share the same MAC address. Cisco Unified CM requires unique MAC addresses for all devices. Cisco Unified Communications Manager converts the MAC address for each device by • Dropping the first two digits of the MAC address • Shifting the MAC address two places to the left • Adding the two-digit port number to the end of the MAC address (to the right of the number) `EXAMPLEMAC Address for the Cisco VG248 is 000039A44218 the MAC address for registered port 12 in the Cisco Unified Communications Manager is0039A4421812` Cisco VG224 Analog Phone Gateway: You can configure a Cisco VG224 gateway as an MGCP gateway or an SCCP gateway. When it is configured as an SCCP gateway, it can have 24 analog phone endpoints. When it is configured this way, it functions similarly to an IOS SCCP gateway. The MAC address for each individual phone gets calculated by using a formula that considers the slot position, subunit, port, and the last 10 characters of the original MAC address.

Field	Description
Device Name	Enter a name to identify software-based telephones, H.323 clients, and CTI ports. For device names that are not based on a MAC address, as a general rule, you can enter 1 to 15 characters comprised of alphanumeric characters (a-z, A-D, 0-9). In most cases you can use dot (.), dash (-), and underscore (_) as well. **Tip** Because the rules for the device name field depend on the device type, Cisco recommends that you see the product documentation to determine which character set is valid for your device, as well as the number of characters allowed. For example, when you configure the device name for the Cisco Unified Personal Communicator, make sure that the name starts with UPC. **Note** Ensure that the device name of a Cisco Unified Mobile Communicator does not exceed 15 characters. If the device name of a Cisco Unified Mobile Communicator exceeds 15 characters, migration of this device will fail upon upgrade to a different release of Cisco Unified Communications Manager. If an existing Cisco Unified Mobile Communicator device name specifies a longer name, shorten the device name to 15 or fewer characters. Cisco Unified Mobile Communicator supports dual mode phones. The preceding limit of 15 characters also applies to Cisco Unified Mobile Communicator dual mode. When the MI for a dual mode phone is longer than 15 characters, the cellular network rejects the phone registration.
Description	Identify the purpose of the device. You can enter the user name (such as John Smith) or the phone location (such as Lobby) in this field. For Cisco VG248 gateways, begin the description with VGC<mac address>. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
Device Pool	Choose the device pool to which you want this phone assigned. The device pool defines sets of common characteristics for devices, such as region, date/time group, and softkey template.
Common Device Configuration	Choose the common device configuration to which you want this phone assigned. The common device configuration includes the attributes (services or features) that are associated with a particular user. Configure the common device in the Common Device Configuration window. To see the common device configuration settings, click the View Details link.
Phone Button Template	Choose the appropriate phone button template. The phone button template determines the configuration of buttons on a phone and identifies which feature (line, speed dial, and so on) is used for each button. Cisco Unified CM does not make this field available for H.323 clients or CTI ports.

Field	Description
Softkey Template	Choose the appropriate softkey template. The softkey template determines the configuration of the softkeys on Cisco Unified IP Phones. Leave this field blank if the common device configuration contains the assigned softkey template.
Common Phone Profile	From the drop-down list box, choose a common phone profile from the list of available common phone profiles.
Calling Search Space	From the drop-down list box, choose the appropriate calling search space (CSS). A calling search space comprises a collection of partitions that are searched to determine how a dialed number should be routed. The calling search space for the device and the calling search space for the directory number get used together. The directory number CSS takes precedence over the device CSS. For more information, see the *Cisco Unified Communications Manager System Guide*. **Note** When set to <none>, Unified CM uses the device mobility calling search space, which is configured on the device pool.
AAR Calling Search Space	Choose the appropriate calling search space for the device to use when it performs automated alternate routing (AAR). 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.
Media Resource Group List	Choose the appropriate Media Resource Group List. A Media Resource Group List comprises a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from the available media resources according to the priority order that is defined in a Media Resource Group List. If you choose <None>, Cisco Unified CM uses the Media Resource Group List that is defined in the device pool. For more information, see the *Cisco Unified Communications Manager System Guide*.
User Hold MOH Audio Source	To specify the audio source that plays when a user initiates a hold action, click the drop-down arrow and choose an audio source from the list that displays. If you do not choose an audio source, Cisco Unified CM uses the audio source that is defined in the device pool or the system default if the device pool does not specify an audio source ID. **Note** You define audio sources in the Music On Hold Audio Source Configuration window. For access, choose **Media Resources** > **Music On Hold Audio Source**.

Field	Description
Network Hold MOH Audio Source	To specify the audio source that is played when the network initiates a hold action, click the drop-down arrow and choose an audio source from the list that displays. If you do not choose an audio source, Cisco Unified CM uses the audio source that is defined in the device pool or the system default if the device pool does not specify an audio source ID. **Note** You define audio sources in the Music On Hold Audio Source Configuration window. For access, choose **Media Resources** > **Music On Hold Audio Source**.
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 box, choose the appropriate location for this Cisco Unified IP Phone. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this Cisco Unified IP Phone consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the **System** > **Location** menu option. For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*.
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. If no AAR group is specified, Cisco Unified CM uses the AAR group that is associated with Device Pool or Line.
User Locale	From the drop-down list box, choose the locale that is associated with the phone user interface. The user locale identifies a set of detailed information to support users, including language and font. Cisco Unified CM makes this field available only for phone models that support localization. **Note** If no user locale is specified, Cisco Unified CM uses the user locale that is associated with the device pool. If the users require that information be displayed (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 Manager Locale Installer documentation.

Field	Description
Network Locale	From the drop-down list box, choose the locale that is associated with the phone. The network locale contains a definition of the tones and cadences that the phone in a specific geographic area uses. Cisco Unified CM makes this field available only for phone models that support localization. **Note** If no network locale is specified, Cisco Unified CM uses the network locale that is associated with the device pool. If users require that country-specific tones be played (on the phone), verify that the locale is installed before configuring the network locale. See the *Cisco Unified Communications Manager* Locale Installer documentation.
Built In Bridge	Enable or disable the built-in conference bridge for the barge feature by using the Built In Bridge drop-down list box (choose On, Off, or Default). **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 7940 and 7960 phones when the device security mode is set to encrypted. For more configuration information, see the *Cisco Unified Communications Manager Features and Services Guide*. You can also see the *Cisco Unified Communications Manager Security Guide* for more information.
Privacy	For each phone that wants Privacy, choose On in the Privacy drop-down list box. For more configuration information, see the *Cisco Unified Communications Manager Features and Services Guide*.

Field	Description
Device Mobility Mode	From the drop-down list box, turn the device mobility feature on or off for this device or choose Default to use the default device mobility mode. Default setting uses the value for the Device Mobility Mode service parameter for the device. Click View Current Device Mobility Settings to display the current values of these device mobility parameters: • Cisco Unified Communications Manager Group • Roaming Device Pool • Location • Region • Network Locale • AAR Group • AAR Calling Search Space • Device Calling Search Space • Media Resource Group List • SRST For more configuration information, see the *Cisco Unified Communications Manager Features and Services Guide*.
Wireless LAN Profile Group	Select a wireless LAN profile group from the drop-down list box. You may also click **View Details** to display the settings for this wireless LAN profile group. **Note** You can specify the Wireless LAN Profile Group at the Device Pool level or the individual phone level. **Note** This field does not apply to all phone models.
Wi-Fi Hotspot Profile	Select a Wi-Fi Hotspot Profile from the drop-down list box. You may also click **View Details** to display the settings for this Wi-Fi Hotspot Profile. **Note** This field does not apply to all phone models.
Signaling Port	This field applies only to H.323 devices. The value designates the H.225 signaling port that this device uses. Default value specifies 1720. Valid values range from 1 to 65535.
Video Capabilities Enabled/disabled	This check box turns video capabilities on and off. **Note** This field does not apply to all phone models.

Field	Description
Owner User ID	From the drop-down list box, choose the user ID of the assigned phone user. The user ID gets recorded in the call detail record (CDR) for all calls made from this device. Assigning a user ID to the device also moves the device from "Unassigned Devices" to "Users" in the License Usage Report. **Note** Do not configure this field if you are using extension mobility. Extension mobility does not support device owners.
Mobility User ID (Dual-mode phones only)	From the drop-down list box, choose the user ID of the person to whom this dual-mode phone is assigned. **Note** The Mobility User ID configuration gets used for the Cisco Unified Mobility and Mobile Voice Access features for dual-mode phones. The Owner User ID and Mobility User ID can differ.
Phone Personalization	The Phone Personalization setting allows you to enable a Cisco Unified IP Phone, so it works with Phone Designer, a Cisco Unified Communications widget that allows a phone user to customize the wallpaper and ring tones on the phone. From the Phone Personalization drop-down list box, choose one of the following options: • Disabled-The user cannot customize the Cisco Unified IP Phone by using Phone Designer. • Enabled-The user can use Phone Designer to customize the phone. • Default-The phone uses the configuration from the Phone Personalization enterprise parameter if you choose Default in both the Phone Configuration and Common Phone Profile Configuration windows. If you choose Default in the Common Phone Profile Configuration window but not in the Phone Configuration window, the phone uses the configuration that you specify in the Phone Configuration window. You must install and configure Phone Designer, so the phone user can customize the phone. Before you install and configure Phone Designer, identify which Cisco Unified IP Phone models work with Phone Designer, as described in the Phone Designer documentation. For more information on Phone Designer, see the Phone Designer documentation at: http://www.cisco.com/en/US/docs/voice_ip_comm/cupa/phone_designer/7.1/english/install/guide/Installation_Guide.html

Field	Description
Services Provisioning	From the drop-down list box, choose how the phone will support the services: • Internal—The phone uses the phone configuration file to support the service. Choose this option or Both for Cisco-provided default services where the Service URL has not been updated; that is, the service URL indicates `Application:Cisco/<name of service>`; for example, `Application:Cisco/CorporateDirectory`. Choose Internal or Both for Cisco-signed Java MIDlets because Cisco-signed Java MIDlets are provisioned in the configuration file. • External URL—Choosing External URL indicates that the phone ignores the services in the phone configuration file and retrieves the services from a Service URL. If you configured a custom Service URL for a service, including a Cisco-provided default service, you must choose either External URL or Both; if you choose Internal in this case, the services that are associated with the custom URLs do not work on the phone. • Both—Choosing Both indicates that the phone support both the services that are defined in the configuration file and external applications that are retrieved from service URLs.
Primary Phone	Choose the physical phone that will be associated with the application, such as IP communicator or Cisco Unified Personal Communicator. When you choose a primary phone, the application consumes fewer device license units and is considered an "adjunct" license (to the primary phone). See the *Cisco Unified Communications Manager Features and Services Guide*.
Wait for Far End H.245 Terminal Capability Set	This field applies only to H.323 devices. This check box specifies that Cisco Unified CM waits to receive the far-end H.245 Terminal Capability Set before it sends its H.245 Terminal Capability Set. By default, the system checks this check box. To specify that Cisco Unified CM should initiate capabilities exchange, uncheck this check box.
Phone Load Name	Enter the custom software for the Cisco Unified IP Phone. The value that you enter overrides the default value for the current model. For more information about Cisco Unified IP Phone software and configuration, see the Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager, which is specific to the phone model and Unified CM release.

Field	Description
Single Button Barge	From the drop-down list box, enable or disable the Single Button Barge/cBarge feature for this device or choose Default to use the service parameter setting. • Off—This setting disables the Single Button Barge/cBarge feature; however, the regular Barge or cBarge features will still work. • Barge—This setting enables the Single Button Barge feature. • CBarge—This setting enables the Single Button cBarge feature. • Default—Uses the Single Button Barge/cBarge setting that is in the service parameter. For more configuration information, see the *Cisco Unified Communications Manager Features and Services Guide*.
Join Across Lines	From the drop-down list box, enable or disable the Join Across Lines feature for this device or choose Default to use the service parameter setting. • Off—This setting disables the Join Across Lines feature. • On—This setting enables the Join Across Lines feature. • Default—This setting uses the Join Across Lines setting that is in the service parameter.

Field	Description
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values: • Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates. • Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified CM 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 *Cisco Unified Communications Manager System Guide* for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified CM first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified CM first tries to find a transcoder that is also designated as a TRP. See the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.
BLF Audible Alert Setting (Phone Idle)	This setting determines the busy lamp field (BLF) audible alert setting when no current call exists on the BLF DN: • On—An audible alert sounds. • Off—No audible alert sounds. • Default—The configuration in the Service Parameters Configuration window determines the alert option.
BLF Audible Alert Setting (Phone Busy)	This setting determines the BLF audible alert setting when at least one active call exists on the BLF DN, but no call pickup alerts exist: • On—An audible alert sounds. • Off—No audible alert sounds. • Default—The configuration in the Service Parameters Configuration window determines the alert option.

Field	Description
Always Use Prime Line	From the drop-down list box, choose one of the following options: • Off—When the phone is idle and receives a call on any line, the phone user answers the call from the line on which the call is received. • On—When the phone is idle (off hook) and receives a call on any line, the primary line gets chosen for the call. Calls on other lines continue to ring, and the phone user must select those other lines to answer these calls. • Default—Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter, which supports the Cisco CallManager service.
Always Use Prime Line for Voice Message	From the drop-down list box, choose one of the following options: • On—If the phone is idle, the primary line on the phone becomes the active line for retrieving voice messages when the phone user presses the Messages button on the phone. • Off—If the phone is idle, pressing the Messages button on the phone automatically dials the voice-messaging system from the line that has a voice message. Cisco Unified CM always selects the first line that has a voice message. If no line has a voice message, the primary line gets used when the phone user presses the Messages button. • Default—Cisco Unified CM uses the configuration from the Always Use Prime Line for Voice Message service parameter, which supports the Cisco CallManager service.
Geolocation	From the drop-down list box, choose a geolocation. You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation. You can also choose a geolocation that has been configured with the **System** > **Geolocation Configuration** menu option.
Feature Control Policy	From the drop-down list box, you can choose a feature control policy that has already been configured in the Feature Control Policy configuration window (**Device** > **Device Settings** > **Feature Control Policy**).
Retry Video Call as Audio	This check box applies only to video endpoints that receive a call. If this phone receives a call that does not connect as video, the call tries to connect as an audio call. By default, the system checks this check box to specify that this device should immediately retry a video call as an audio call (if it cannot connect as a video call) prior to sending the call to call control for rerouting. If you uncheck this check box, a video call that fails to connect as video does not try to establish as an audio call. The call then fails to call control, and call control routes the call via automatic alternate routing (AAR) and/or route/hunt list.

Field	Description
Ignore Presentation Indicators (internal calls only)	Check this check box to configure call display restrictions on a call-by-call basis. When this check box is checked, Cisco Unified CM ignores any presentation restriction that is received for internal calls. 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. See the translation configuration settings Table 49: Translation Pattern Settings, on page 278 for more information about the calling line ID presentation and the connected line ID presentation parameters. For more information about call display restrictions, see the *Cisco Unified Communications Manager Features and Services Guide*.
Allow Control of Device from CTI	Check this check box to allow CTI to control and monitor this device. If the associated directory number specifies a shared line, the check box should be enabled as long as at least one associated device specifies a combination of device type and protocol that CTI supports.
Logged into Hunt Group	This check box, which gets checked by default for all phones, indicates that the phone is currently logged in to a hunt list (group). When the phone gets added to a hunt list, the administrator can log the user in or out by checking (and unchecking) this check box. Users use the softkey on the phone to log their phone in or out of the hunt list.
Remote Device	If you are experiencing delayed connect times over SCCP pipes to remote sites, check the Remote Device check box in the Phone Configuration window. Checking this check box tells Cisco Unified CM to allocate a buffer for the phone device when it registers and to bundle SCCP messages to the phone. **Tip** Because this feature consumes resources, be sure to check this check box only when you are experiencing signaling delays for phones that are running SCCP. Most users do not require this option. Cisco Unified CM sends the bundled messages to the phone when the station buffer is full, as soon as it receives a media-related message, or when the Bundle Outbound SCCP Messages timer expires. To specify a setting other than the default setting (100 msec) for the Bundle Outbound SCCP Messages timer, configure a new value in the Service Parameters Configuration window for the Cisco CallManager service. Although 100 msec specifies the recommended setting, you may enter 15 msec to 500 msec. The phone must support SCCP version 9 to use this option. The following phones do not support SCCP message optimization: Cisco Unified IP Phone 7935/7936. This feature may require a phone reset after update.

Field	Description
Protected Device	Check this check box to designate a phone as protected, which enables the phone to play a 2-second tone to notify the user when a call is encrypted and both phones are configured as protected devices. The tone plays for both parties when the call is answered. The tone does not play unless both phones are protected and the call occurs over encrypted media. Checking this check box represents only one of several configuration requirements for the secure indication tone to play. For a detailed description of the secure indication tone feature and the configuration requirements, see the *Cisco Unified Communications Manager Security Guide*. If you check this check box and the system determines that the call is not encrypted, the phone plays nonsecure indication tone to alert the user that the call is not protected.
Hotline Device	Check this check box to make this device a Hotline device. Hotline devices can only connect to other Hotline devices. 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.
Caller ID For Calls From This Phone	
Calling Party Transformation CSS for Calls from this Phone	From the drop-down list box, choose the calling search space (CSS) that contains the calling party transformation pattern that you want to apply on the calling number when this phone initiates a call. Cisco Unified CM transforms the calling party using the digit transformations configured on the matching calling party transformation pattern when this phone initiates a call. This setting allows you to transform the calling party number before Cisco Unified CM routes the call. For example, a transformation pattern can change a phone extension to an E.164 number. This setting is generally configured when a user dials using a URI instead of digits. Cisco Unified CM allows calling party transformations on various patterns when dialing using digits, this setting provides similar transformation provision even when dialing using a URI.
Use Device Pool Calling Party Transformation CSS (Caller ID for Calls from this Phone)	Check this check box to use the Calling Party Transformation CSS configured at the device pool to which this phone belongs to transform the calling party for calls initiated from this phone. At the device pool, Calling Party Transformation CSS present under Phone Settings is used to transform the calling party for calls initiated from this phone. Leave this check box unchecked to apply the Calling Party Transformation CSS setting that appears in this configuration window.
Remote Number Transformation	

Field	Description
Calling Party Transformation CSS for Remote Number	From the drop-down list box, choose the calling search space (CSS) that contains the calling party transformation pattern that you want to apply on the remote calling number for calls received on this phone. Cisco Unified CM transforms the remote calling number using the digit transformations configured on the matching calling party transformation pattern before presenting it to this device. For example, a transformation pattern can change remote number in E.164 format to a localized version. This setting can be used to transform the remote connected number for direct calls initiated from this phone. This setting can also be used to transform remote connected number post feature invocation irrespective of the direction of the call. The transformation of a remote connected number is controlled using the service parameter "Apply Transformations On Remote Number" (present under advanced section of Cisco Call Manager service). Refer to this parameter description for more details.
Use Device Pool Calling Party Transformation CSS for Remote Number (Device Mobility Related Information)	Check this check box to apply the Calling Party Transformation CSS configured at the device pool to which this phone belongs to transform the remote calling and remote connected number. At the device pool, Calling Party Transformation CSS present under Device Mobility Related Information section is used to transform remote calling and remote connected number. Leave this check box unchecked to apply the Calling Party Transformation CSS setting that appears in this configuration window for transforming the remote number.
Protocol Specific Information	
Packet Capture Mode	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. Choose one of the following options from the drop-down list box: • None—This option, which serves as the default setting, indicates that no packet capturing is occurring. After you complete packet capturing, configure this setting. • Batch Processing Mode—Cisco Unified CM writes the decrypted or nonencrypted messages to a file, and the system encrypts each file. On a daily basis, the system creates a new file with a new encryption key. Cisco Unified CM, which stores the file for seven days, also stores the keys that encrypt the file in a secure location. Cisco Unified CM stores the file in the PktCap virtual directory. A single file contains the time stamp, source IP address, source IP port, destination IP address, packet protocol, message length, and the message. The TAC debugging tool uses HTTPS, administrator username and password, and the specified day to request a single encrypted file that contains the captured packets. Likewise, the tool requests the key information to decrypt the encrypted file. For more information on packet capturing, see the *Troubleshooting Guide for Cisco Unified Communications Manager*.

Field	Description
Packet Capture Duration	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. This field specifies the maximum number of minutes that is allotted for one session of packet capturing. The default setting equals 0, although the range exists from 0 to 300 minutes. To initiate packet capturing, enter a value other than 0 in the field. After packet capturing completes, the value, 0, displays. For more information on packet capturing, see the *Cisco Unified Communications Manager Troubleshooting Guide*.
SRTP Allowed	As this check box explains, if this flag is checked, IPSec needs to be configured in the network to provide end-to-end security. Failure to do so will expose keys and other information. For more information on SRTP encryption, see the *Cisco Unified Communications Manager Security Guide*.
Presence Group	Configure this field with the Presence feature. From the drop-down list box, choose a Presence group for the end user. The selected group specifies the devices, end users, and application users that can monitor this directory number. The default value for Presence Group specifies Standard Presence group, configured with installation. Presence groups that are configured in Cisco Unified Communications Manager Administration also appear in the drop-down list box. Presence authorization works with presence groups to allow or block presence requests between groups. See the *Cisco Unified Communications Manager Features and Services Guide* for information about configuring permissions between groups and how presence works with extension mobility.
Device Security Profile	Choose the security profile to apply to the device. You must apply a security profile to all phones that are configured in Cisco Unified Communications Manager Administration. *Installing Cisco Unified Communications Manager* provides a set of predefined, nonsecure security profiles for auto-registration. To enable security features for a phone, you must configure a new security profile for the device type and protocol and apply it to the phone. If the phone does not support security, choose a nonsecure profile. To identify the settings that the profile contains, choose **System** > **Security Profile** > **Phone Security Profile**. **Note** The CAPF settings that are configured in the profile relate to the Certificate Authority Proxy Function settings that display in the Phone Configuration window. You must configure CAPF settings for certificate operations that involve manufacturer-installed certificates (MICs) or locally significant certificates (LSC). See the Cisco Unified Communications Manager Security Guide for more information about how CAPF settings that you update in the phone configuration window affect security profile CAPF settings.

Field	Description
SIP Dial Rules	If required, choose the appropriate SIP dial rule. SIP dial rules provide local dial plans for Cisco Unified IP Phones 7905, 7912, 7940, and 7960, so users do not have to press a key or wait for a timer before the call gets processed. Leave the SIP Dial Rules field set to <None> if you do not want dial rules to apply to the IP phone that is running SIP. This means that the user must use the Dial softkey or wait for the timer to expire before the call gets processed.
MTP Preferred Originating Codec	From the drop-down list box, choose the codec to use if a media termination point is required for SIP calls.
Rerouting Calling Search Space	From the drop-down list box, choose a calling search space to use for rerouting. The rerouting calling search space of the referrer gets used to find the route to the refer-to target. When the Refer fails due to the rerouting calling search space, the Refer Primitive rejects the request with the “405 Method Not Allowed” message. The redirection (3xx) primitive and transfer feature also uses the rerouting calling search space to find the redirect-to or transfer-to target.
Out-of-Dialog Refer Calling Search Space	From the drop-down list box, choose an out-of-dialog refer calling search space. Cisco Unified CM uses the out-of-dialog (OOD) Refer Authorization calling search space (CSS) to authorize the SIP out-of-dialog Refer. The administrator can restrict the use of out-of-dialog Refer by configuring the OOD CSS of the Referrer. Refer Primitive rejects the OOD Refer request with a “403 Forbidden” message.
SUBSCRIBE Calling Search Space	Supported with the Presence feature, the SUBSCRIBE calling search space determines how Cisco Unified CM routes presence requests that come from the phone. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the phone. From the drop-down list box, choose the SUBSCRIBE calling search space to use for presence requests for the phone. All calling search spaces that you configure in Cisco Unified Communications Manager Administration display in the SUBSCRIBE Calling Search Space drop-down list box. If you do not select a different calling search space for the end user from the drop-down list, the SUBSCRIBE calling search space defaults to None. To configure a SUBSCRIBE calling search space specifically for this purpose, you configure a calling search space as you do all calling search spaces.

Field	Description
Outbound Call Rollover	Use this setting for the Cisco Unified IP Phone 7931. • No Rollover—Conference and transfer will not work in this mode. If a user attempts to use either of these features, the phone status displays as "Error Pass Limit." Choose this setting only if you need to support CTI applications. • Rollover Within Same DN—Conferences and call transfers complete by using the same directory number (on different lines). For example, consider a phone that has directory number 1506 that is assigned to both Line 6 and 7. The user has an active call on Line 6 and decides to transfer the call. When the user presses the Transfer button, the call on Line 6 gets placed on hold, and a new call initiates on Line 7 to complete the transfer. • Rollover to any line—Conferences and call transfers complete by using a different directory number and line than the original call. For example, consider a phone that has directory number 1507 assigned to Line 8 and directory number 1508 assigned to Line 9. The user has an active call on Line 8 and decides to transfer the call. When the user presses the Transfer button, the call on Line 8 gets placed on hold, and a new call initiates on Line 9 to complete the transfer.
SIP Profile	Choose the default SIP profile or a specific profile that was previously created. SIP profiles provide specific SIP information for the phone such as registration and keepalive timers, media ports, and do not disturb control.
Digest User	Choose an end user that you want to associate with the phone for this setting that is used with digest authentication (SIP security). Ensure that you configured digest credentials for the user that you choose, as specified in the End User Configuration window. After you save the phone configuration and apply the configuration update to the phone, the digest credentials for the user get added to the phone configuration file. For more information on digest authentication, see the *Cisco Unified Communications Manager Security Guide*.
Media Termination Point Required	Use this field to indicate whether a media termination point is used to implement features that H.323 does not support (such as hold and transfer). Check the Media Termination Point Required check box if you want to use an MTP to implement features. Uncheck the Media Termination Point Required check box if you do not want to use an MTP to implement features. Use this check box only for H.323 clients and those H.323 devices that do not support the H.245 empty capabilities set or if you want media streaming to terminate through a single source. If you check this check box to require an MTP and this device becomes the endpoint of a video call, the call will be audio only.
Unattended Port	Check this check box to indicate an unattended port on this device.

Field	Description
Require DTMF Reception	For phones that are running SIP and SCCP, check this check box to require DTMF reception for this phone. **Note** In configuring Cisco Unified Mobility features, when using intercluster DNs as remote destinations for an IP phone via SIP trunk (either intercluster trunk [ICT] or gateway), check this check box so that DTMF digits can be received out of band, which is crucial for Enterprise Feature Access midcall features.
RFC2833 Disabled	For phones that are running SCCP, check this check box to disable RFC2833 support.
Certification Authority Proxy Function (CAPF) Information	
Certificate Operation	From the drop-down list box, choose one of the following options: • No Pending Operation—Displays when no certificate operation is occurring (default setting). • Install/Upgrade—Installs a new or upgrades an existing locally significant certificate in the phone. • Delete—Deletes the locally significant certificate that exists in the phone. • Troubleshoot—Retrieves the locally significant certificate (LSC) or the manufacture installed certificate (MIC), so you can view the certificate credentials in the CAPF trace file. If both certificate types exist in the phone, Cisco Unified CM creates two trace files, one for each certificate type. By choosing the Troubleshooting option, you can verify that an LSC or MIC exists in the phone. For more information on CAPF operations, see the *Cisco Unified Communications Manager Security Guide*.

Field	Description
Authentication Mode	This field allows you to choose the authentication method that the phone uses during the CAPF certificate operation. From the drop-down list box, choose one of the following options: • By Authentication String—Installs/upgrades, deletes, or troubleshoots a locally significant certificate only when the user enters the CAPF authentication string on the phone. • By Null String— Installs/upgrades, deletes, or troubleshoots a locally significant certificate without user intervention. This option provides no security; Cisco strongly recommends that you choose this option only for closed, secure environments. • By Existing Certificate (Precedence to LSC)—Installs/upgrades, deletes, or troubleshoots a locally significant certificate if a manufacture-installed certificate (MIC) or locally significant certificate (LSC) exists in the phone. If a LSC exists in the phone, authentication occurs via the LSC, regardless whether a MIC exists in the phone. If a MIC and LSC exist in the phone, authentication occurs via the LSC. If a LSC does not exist in the phone, but a MIC does exist, authentication occurs via the MIC. Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails. At any time, the phone uses only one certificate to authenticate to CAPF even though a MIC and LSC can exist in the phone at the same time. If the primary certificate, which takes precedence, becomes compromised for any reason, or, if you want to authenticate via the other certificate, you must update the authentication mode. • By Existing Certificate (Precedence to MIC)—Installs, upgrades, deletes, or troubleshoots a locally significant certificate if a LSC or MIC exists in the phone. If a MIC exists in the phone, authentication occurs via the MIC, regardless whether a LSC exists in the phone. If a LSC exists in the phone, but a MIC does not exist, authentication occurs via the LSC. Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails. **Note** The CAPF settings that are configured in the Phone Security Profile window interact with the CAPF parameters that are configured in the Phone Configuration window.
Authentication String	If you chose the By Authentication String option in the Authentication Mode drop-down list box, this field applies. Manually enter a string or generate a string by clicking the Generate String button. Ensure that the string contains 4 to 10 digits. To install, upgrade, delete, or troubleshoot a locally significant certificate, the phone user or administrator must enter the authentication string on the phone.

Field	Description
Key Size (Bits)	For this setting that is used for CAPF, choose the key size for the certificate from the drop-down list box. The default setting equals 1024. Other options include 512 and 2048. If you choose a higher key size than the default setting, the phones take longer to generate the entropy that is required to generate the keys. Key generation, which is set at low priority, allows the phone to function while the action occurs. Depending on the phone model, you may notice that key generation takes up to 30 or more minutes to complete. **Note** The CAPF settings that are configured in the Phone Security Profile window interact with the CAPF parameters that are configured in the Phone Configuration window.
Operation Completes by	This field, which supports the Install/Upgrade, Delete, and Troubleshoot Certificate Operation options, specifies the date and time in which you must complete the operation. The values that display apply for the publisher database server.
Certificate Operation Status	This field displays the progress of the certificate operation; for example, <operation type> pending, failed, or successful, where operating type equals the Install/Upgrade, Delete, or Troubleshoot Certificate Operation options. You cannot change the information that displays in this field.
Expansion Module Information (The following fields only display when the expansion modules are supported by the phone.)	
Module 1	Choose the appropriate expansion module or none.
Module 1 Load Name	Enter the custom software for the appropriate expansion module, if applicable. The value that you enter overrides the default value for the current model. Ensure the firmware load matches the module load.
Module 2	Choose the appropriate expansion module or none.
Module 2 Load Name	Enter the custom software for the second expansion module, if applicable. The value that you enter overrides the default value for the current model. Ensure the firmware load matches the module load.
Module 3	Choose the appropriate expansion module or none.
Module 3 Load Name	Enter the custom software for the appropriate expansion module, if applicable. The value that you enter overrides the default value for the current model. Ensure the firmware load matches the module load.
External Data Locations Information (Leave blank to use default)	

Field	Description
Information	Enter the location (URL) of the help text for the information (i) button. Leave this field blank to accept the default setting.
Directory	Enter the server from which the phone obtains directory information. Leave this field blank to accept the default setting. **Note** If you set a Secured Directory URL enterprise parameter in the Enterprise Parameters Configuration window, that value overwrites the value of this field.
Messages	Leave this field blank (not used by Cisco Unified Communications Manager).
Services	Enter the location (URL) for IP phone services.
Authentication Server	Enter the URL that the phone uses to validate requests that are made to the phone web server. If you do not provide an authentication URL, the advanced features on the Cisco Unified IP Phone that require authentication will not function. By default, this URL accesses a Cisco Unified Communications Self Care Portal window that was configured during installation. Leave this field blank to accept the default setting.
Proxy Server	Enter the host and port (for example, proxy.cisco.com:80) that are used to proxy HTTP requests for access to non-local host addresses from the phone HTTP client. The rule contains two parts for when to use the proxy server parameter: **1** The hostname contains a "." **2** The hostname specifies an IP address in any form. If you do not configure this URL, the phone attempts to connect directly to the URL. To accept the default setting, leave this field blank.
Idle	Enter the URL that displays on the Cisco Unified IP Phone display when the phone has not been used for the time that is specified in Idle Timer field. For example, you can display a logo on the LCD when the phone has not been used for 5 minutes. To accept the default setting, leave this field blank.
Idle Timer (seconds)	Enter the time (in seconds) that you want to elapse before the URL that is specified in the Idle field displays. To accept the value of the Idle URL Timer enterprise parameter, leave this field blank.

Field	Description
Secure Authentication URL	Enter the secure URL that the phone uses to validate requests that are made to the phone web server. **Note** If you do not provide a Secure Authentication URL, the device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, the device chooses the appropriate URL, based on its capabilities. By default, this URL accesses a Cisco Unified Communications Self Care Portal window that was configured during installation. Leave this field blank to accept the default setting. Maximum length: 255
Secure Directory URL	Enter the secure URL for the server from which the phone obtains directory information. This parameter specifies the URL that secured Cisco Unified IP Phones use when you press the Directory button. **Note** If you do not provide a Secure Directory URL, the device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, the device chooses the appropriate URL, based on its capabilities. Leave this field blank to accept the default setting. Maximum length: 255
Secure Idle URL	Enter the secure URL for the information that displays on the Cisco Unified IP Phone display when the phone is idle, as specified in Idle Timer field. For example, you can display a logo on the LCD when the phone has not been used for 5 minutes. **Note** If you do not provide a Secure Idle URL, the device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, the device chooses the appropriate URL, based on its capabilities. To accept the default setting, leave this field blank. Maximum length: 255
Secure Information URL	Enter the secure URL for the server location where the Cisco Unified IP Phone can find help text information. This information displays when the user presses the information (i) button or the question mark (?) button. **Note** If you do not provide a Secure Information URL, the device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, the device chooses the appropriate URL, based on its capabilities. To accept the default setting, leave this field blank. Maximum length: 255

Field	Description
Secure Messages URL	Enter the secure URL for the messages server. The Cisco Unified IP Phone contacts this URL when the user presses the Messages button. **Note** If you do not provide a Secure Messages URL, the device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, the device chooses the appropriate URL, based on its capabilities. To accept the default setting, leave this field blank. Maximum length: 255
Secure Services URL	Enter the secure URL for Cisco Unified IP Phone services. The is the location that the secure Cisco Unified IP Phone contacts when the user presses the Services button. **Note** If you do not provide a Secure Services URL, the device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, the device chooses the appropriate URL, based on its capabilities. To accept the default setting, leave this field blank. Maximum length: 255
Extension Information	
Enable Extension Mobility	Check this check box if this phone supports extension mobility.
Log Out Profile	This drop-down list box specifies the device profile that the device uses when no one is logged in to the device by using Cisco Extension Mobility. You can choose either Use Current Device Settings or one of the specific configured profiles that are listed. If you select a specific configured profile, the system retains a mapping between the device and the login profile after the user logs out. If you select Use Current Device Settings, no mapping gets retained.
Log In Time	This field remains blank until a user logs in. When a user logs in to the device by using Cisco Extension Mobility, the time at which the user logged in displays in this field.
Log Out Time	This field remains blank until a user logs in. When a user logs in to the device by using Cisco Extension Mobility, the time at which the system will log out the user displays in this field.
Configuration File Encryption Symmetric Key Information	

Field	Description
Symmetric Key	Enter a string of hexadecimal characters that you want to use for the symmetric key. Valid characters include numerals, 0-9, and upper/lower case characters, A-F (or a-f). Make sure that you enter the correct bits for the key size; otherwise, Cisco Unified CM rejects the value. Cisco Unified CM supports the following key sizes: • Cisco Unified IP Phones 7905 and 7912 (SIP only)—256 bits • Cisco Unified IP Phones 7940 and 7960 (SIP only)—128 bits Use this string for one-time use only. Every time that you update the configuration settings, you must generate a new key before you apply the configuration changes to the phone. For more information on symmetric key operations for encrypted configuration file downloads, see the *Cisco Unified Communications Manager Security Guide*.
Generate String	If you want Cisco Unified Communications Manager Administration to generate a hexadecimal string for you, click the Generate String button.
Revert to Database Value	If you want to restore the value that exists in the database, click this button. This button proves useful if you enter an error in the Symmetric Key field before you save the configuration.
H.323 Information	
Outgoing Caller ID Pattern	For outgoing calls to the H.323 Client, enter the pattern, from 0 to 24 digits, that you want to use for caller ID.
Calling Party Selection	Choose the directory number that is sent on an outbound call to the H.323 Client. The following options specify which directory number is sent: • Originator—Send the directory number of the calling device. • First Redirect Number—Send the directory number of the redirecting device. • Last Redirect Number—Send the directory number of the last device to redirect the call. • First Redirect Number (External)—Send the external directory number of the redirecting device. • Last Redirect Number (External)—Send the external directory number of the last device to redirect the call.
Calling Party Presentation	Choose whether the Cisco Unified CM transmits or blocks caller ID. If you want Cisco Unified CM to send caller ID, choose Allowed. If you do not want Cisco Unified CM to send caller ID, choose Restricted. Default specifies that caller ID does not get sent.

Field	Description
Display IE Delivery	This check box enables delivery of the display information element (IE) in SETUP and CONNECT messages for the calling and called party name delivery service. The default setting checks this check box.
Redirecting Number IE Delivery Outbound	Check this check box to indicate the first redirecting number and the redirecting reason of the call when the call is forwarded. (The UUIE part of the outgoing SETUP message from the Cisco Unified CM includes the Redirecting Number IE.) Uncheck the check box to exclude the first redirecting number and the redirecting reason from the outgoing SETUP message. You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box. **Note** The default setting leaves this check box unchecked.
Redirecting Number IE Delivery Inbound	Check this check box to accept the Redirecting Number IE in the incoming SETUP message to the Cisco Unified CM. (The UUIE part of the SETUP message includes the Redirecting Number IE.) Uncheck the check box to exclude the Redirecting Number IE in the incoming SETUP message to the Cisco Unified CM. You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box. **Note** Default leaves the check box unchecked.
Gatekeeper Information	
Gatekeeper Name	This field specifies the name of the gatekeeper that controls the H.323 client. Ensure the gatekeeper is configured in Cisco Unified CM before an H.323 client is allowed to specify the gatekeeper in its configuration. Default specifies empty.
E.164	Always use a unique E.164 number. Do not use null value.
Technology Prefix	This field specifies a number ending with the # sign that describes the capability of an endpoint in a zone. This field has no impact if via Zone configuration can be used. Default specifies 1#*. Do not use null value.
Zone	This field specifies the zone name of the zone that the gatekeeper manages. Do not use the following values: same zone name for the H.323 client and trunk; null.
Associated Mobility Identity	

Field	Description
(mobility identity)	If a mobility identity has already been configured for this device, this area displays the Name and Destination Number of the mobility identity. You can click either value to display the Mobility Identity Information in the Remote Destination Configuration window. **Note** This field displays only after a Cisco Unified Mobile Communicator device has been added. The Cisco Unified Mobile Communicator must be enabled for a mobile phone.
Add New Mobility Identity	If no mobility identity has been defined for this device, click this link to add a mobility identity. The Remote Destination Configuration window displays, which allows you to add a new mobility identity to associate with this device. **Note** This field displays only after a Cisco Unified Mobile Communicator device has been added.
Associated Remote Destinations	
(remote destination)	If a remote destination has already been configured for this device, this area displays the Name and Destination Number of the remote destination(s). You can click the values to display the Remote Destination Information in the Remote Destination Configuration window.
Add a New Remote Destination	Click this link to add a remote destination to associate with this device. The Remote Destination Configuration window displays, which allows you to add a new remote destination to associate with this device.
Route calls to all remote destinations when client is not connected	Determines whether calls should be routed to all remote destinations when the active remote destination is not set. Check this check box to receive calls during network connection outage or to use a third-party voicemail system. **Note** This field appears only on a CTI remote device type.
MLPP Information	
MLPP Domain	Choose an MLPP domain from the drop-down list box for the MLPP domain that is associated with this device. If you leave the None value, this device inherits its MLPP domain from the value that was set in the common device configuration. If the common device configuration does not have an MLPP domain setting, this device inherits its MLPP domain from the value that was set for the MLPP Domain Identifier enterprise parameter.

Field	Description
MLPP Indication	If available, this setting specifies whether a device that can play precedence tones will use the capability when it places an MLPP precedence call. From the drop-down list box, choose a setting to assign to this device from the following options: • Default—This device inherits its MLPP indication setting from the common device configuration. • Off—This device does not handle nor process indication of an MLPP precedence call. • On—This device does handle and process indication of an MLPP precedence call. **Note** Do not configure a device with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful. Turning on MLPP Indication (at the enterprise parameter or device level) disables normal Ring Setting behavior for the lines on a device, unless MLPP Indication is turned off (overridden) for the device.
MLPP Preemption	Be aware that this setting is not available on all devices. If available, this setting specifies whether a device that can preempt calls in progress will use the capability when it places an MLPP precedence call. From the drop-down list box, choose a setting to assign to this device from the following options: • Default—This device inherits its MLPP preemption setting from the common device configuration. • Disabled—This device does not allow preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. • Forceful—This device allows preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. **Note** Do not configure a device with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful.
Confidential Access Level	Select the appropriate CAL value from the drop-down list box.
Confidential Access Mode	From the drop-down list box, select one of the following options to set the CAL mode: • Fixed—CAL value has higher precedence over call completion. • Variable—Call completion has higher precedence over CAL level.

Field	Description
Do Not Disturb (DND)	
Do Not Disturb	Check this check box to enable Do Not Disturb on the phone.
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 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 gets 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.
Secure Shell Information	

Field	Description
Secure Shell User	Enter a user ID for the secure shell user. You can enter any alphanumeric or special characters up to 50 characters. Invalid characters include", %, &, <, >, and \. This field displays when the phone device that you are configuring supports SSH access. Cisco Technical Assistance Center (TAC) uses secure shell for troubleshooting and debugging. Contact TAC for further assistance. See the *Cisco Unified Communications Manager Security Guide* for this release for information about how to configure encrypted phone configuration files to ensure that Cisco Unified CM does not send SSH credentials to the phone in the clear.
Secure Shell Password	Enter the password for a secure shell user. You can enter any alphanumeric or special characters up to 200 characters. Invalid characters include", %, &, <, >, and \. Contact TAC for further assistance. See the *Cisco Unified Communications Manager Security Guide* for this release for information about how to configure encrypted phone configuration files to ensure that Cisco Unified CM does not send SSH passwords to the phone in the clear.
Association Information	
Modify Button Items	After you add a phone, the Association Information area displays on the left side of the Phone Configuration window. Click this button to manage button associations for this phone. A dialog box warns that any unsaved changes to the phone may be lost. If you have saved any changes that you made to the phone, click OK to continue. The Reorder Phone Button Configuration window displays for this phone.
Line [1] - Add a new DN Line [2] - Add a new DN	After you add a phone, the Association Information area displays on the left side of the Phone Configuration window. Click these links to add a directory number(s) that associates with this phone. When you click one of the links, the Directory Number Configuration window displays.
Add a new SD	After you add a phone, the Association Information area displays on the left side of the Phone Configuration window. Click this link to add speed-dial settings for this phone. When you click the link, the Speed Dial and Abbreviated Dial Configuration window displays for this phone.
Add a new SURL	After you add a phone, the Association Information area displays on the left side of the Phone Configuration window. Click this link to configure service URL buttons for this phone. When you click the link, the Configure Service URL Buttons window displays for this phone.

Field	Description
Add a new BLF SD	After you add a phone, the Association Information area displays on the left side of the Phone Configuration window. Click this link to configure busy lamp field/speed dial settings for this phone. When you click the link, the Busy Lamp Field Directed Call Park Configuration window displays for this phone.
Add a new BLF Directed Call Park	After you add a phone, the Association Information area displays on the left side of the Phone Configuration window. Click this link to configure busy lamp field/directed call park settings for this phone. When you click the link, the Busy Lamp Field Directed Call Park Configuration window displays for this phone. For more information on configuring BLF/Directed Call Park buttons, see the *Cisco Unified Communications Manager Features and Services Guide*.
Product-Specific Configuration Layout	
Model-specific configuration fields that the device manufacturer defines	To view field descriptions and help for product-specific configuration items, click the "?" information icon in the Product Specific Configuration area to display help in a popup dialog box. If you need more information, see the documentation for the specific device that you are configuring or contact the manufacturer. Select the "Override Common Settings" box for any corresponding setting in the Product Specific Configuration area that you wish to update. If you do not check this box, the corresponding parameter setting does not take effect. Parameters that you set in the Product Specific Configuration area may also appear in the Device Configuration window for various devices and in the Enterprise Phone Configuration window. If you set these same parameters in these other windows too, the setting that takes precedence is determined in the following order: 1) Device Configuration window settings, 2) Common Phone Profile window settings, 3) Enterprise Phone Configuration window settings.

Related Topics

Location Setup , on page 127
Calling Search Space Setup , on page 273
About Translation Pattern Setup , on page 277
About Directory Number Setup , on page 289
Display Calling Search Space , on page 320
Gateway Setup , on page 465
BLF Speed Dial Setup , on page 620
Synchronize Phone , on page 625
Set Up Speed-dial Buttons or Abbreviated Dialing , on page 625
Service URL Button Setup, on page 629
Modify Custom Phone Button Template Button Items , on page 630

Device Defaults Setup , on page 701

Phone Settings Migration

You can migrate existing phone settings to a different phone.

Related Topics

Migrate Existing Phone Settings to Another Phone , on page 623
Phone Migration Settings , on page 624

Speed-Dial and Abbreviated-Dial Setup

The following table describes the speed-dial button configuration settings. The Speed Dial and Abbreviated Dial Configuration window contains the following sections: speed-dial settings on the phone and abbreviated-dial settings that are not associated with a button. The descriptions in the table apply to both sections.

The system provides a total of 199 speed-dial and abbreviated-dial settings.

Speed Dial Settings

Configure these settings for the physical buttons on the phone.

Abbreviated Dial Settings

Configure these settings for the speed-dial numbers that you access with abbreviated dialing. When the user configures up to199 speed-dial entries, part of the speed-dial entries can get assigned to the speed-dial buttons on the IP phone; the remaining speed-dial entries get used for abbreviated dialing. When a user starts dialing digits, the AbbrDial softkey displays on the phone, and the user can access any speed-dial entry by entering the appropriate index (code) for abbreviated dialing.

Pause in Speed Dial Feature Specific Settings

In Cisco Unified Communication Manager, the user can configure Forced Authorization Code (FAC), Client Matter Code (CMC), and post-connect Dual Tone Multifrequency (DTMF) digits as a part of a speed dial number. The Unified CM recognizes the destination address digits, FAC, CMC, and post-connect DTMF digits that are configured as a part of a speed dial number.

The Unified CM uses the following:

1. Destination address digits to route the call
2. FAC digits to authorize the user before routing the call to a particular gateway or a trunk
3. CMC digits for billing before routing the call to a particular gateway or a trunk

The Unified CM sends out post-connect DTMF digits with appropriate pause duration after the call is connected and a media connection is established.

Note Even if the media connection is established before a call is connected, the DTMF digits are sent only after the call is connected.

There are two methods to configure this feature:

- Method I : Using a comma as a pause and also as a delimiter
- Method II : Entering destination address digits, FAC, CMC, and DTMF digits as a continuous string without using any delimiter

Method I: Using comma as a pause and also as a delimiter

1 Using comma as a pause
The users can configure the special character comma (,) within speed dial, which acts as a pause duration of 2 seconds for sending post-connect DTMF digits. The Unified CM pauses for the appropriate duration corresponding to the number of commas entered before sending out DTMF digits to the remote side of the call.

Example 1: Reading a Voicemail message

Without the Pause in Speed dial feature, the user must perform the following to read a voicemail message:

1. Click message button on the phone or 8000 [Voicemail pilot number] to reach the Cisco Unity Server.
2. Enter 91941420# [PIN] after announcement of 2 seconds after the call is connected.
3. Enter option 3 to read the latest message after a pause of around 6 seconds (while the operator reads the options) after the PIN is verified.

With Pause in Speed dial feature, the user can configure speed dial as

8000,91941420#,,,3 and press the speed dial key and read the latest message received. Here, the Unified CM waits for 2 seconds after the call is connected, then sends out the PIN [91941420#] to the Cisco Unity Server and again waits for 6 seconds before sending out the option [3] to the Cisco Unity Server.

2 Using comma as a delimiter
A comma can be used as a delimiter in the following cases:

- To separate the FAC from the destination address digits
- To separate destination address digits and CMC (if FAC is not enabled)
- To separate the FAC and CMC

This enables Unified CM to recognize the destination address digits, FAC, CMC, and DTMF digits when user has configured the following:

1. Overlapping dial patterns [Example: 9.XXXX and 9.XXXXX are overlapping Route patterns]
2. Variable length dial patterns [Example: 8.!]
3. Overlapping FAC and CMC [Example of overlapping FAC: 8787, 87879]

Example 2: Connecting to IVR application over a gateway

If the user wants to reach out to an IVR application over a gateway, to the user must enter FAC and CMC digits to reach the gateway and then send out IVR responses after the call is connected. The manual dialing works as follows:

1. Enter called number: 91886543
2. Enter Forced Authorization Code: 8787
3. Enter Client Matter Code: 5656
4. IVR response 4 seconds after the call is connected: 987989#

Using the Pause in Speed Dial feature, a user can configure speed dial as follows to achieve the same result:

91886543,8787,5656,,987989#

In this example, the Unified CM uses 8787 as FAC, 5656 as CMC before the call is routed to a gateway and sends out IVR response [987989#] 4 seconds after the call is connected.

Note Ensure the FAC always precedes the CMC when you configure a speed dial that includes FAC and CMC.

Note Ensure to use only a single comma as a delimiter. If more than one comma is configured, the digits after multiple commas are considered as DTMF digits and users are prompted to enter the FAC or CMC manually.

Handling incorrect FAC or CMC when comma is used as a delimiter

Whenever comma is used as a delimiter and FAC or CMC is configured as a part of speed dial is incorrect or unauthorized to make a particular call then the Unified CM disconnects the call with the following error message on the phone where speed dial is invoked:

Error: Invalid Code in SpeedDial

Method II: Entering main address, FAC, CMC, and DTMF digits as a continuous string without using any delimiter

With this method, speed dial is configured as a continuous string of digits and Unified CM identifies following components from the digit string:

1. Destination address digits
2. FAC
3. CMC
4. DTMF digits [DTMF digits are sent immediately after the call is connected]

This method allows the user to configure the Pause in Speed Dial feature on Cisco Unified Personal Communicator endpoints which do not have the speed dial option.

Example 3: Connecting to IVR application, which prompts users to enter responses immediately after call is connected

If the user wants to reach an IVR application and is required to enter FAC and CMC digits to reach to a gateway and then send out IVR response after call is connected, the manual dialing works as follows:

1. Enter called number: 91886543 [Using Route Pattern 9.XXXXXXX]
2. Enter Forced Authorization Code: 8787
3. Enter Client Matter Code: 5656
4. IVR response immediately after the call is connected: 987989#

Using the Pause in Speed Dial feature, a user can configure speed dial as follows to achieve the same result:

9188654387875656987989#

Handling incorrect FAC or CMC when comma is not used as a delimiter

Whenever a comma is not used as a delimiter and FAC or CMC is configured as a part of speed dial is incorrect or unauthorized to make a particular call then the Unified CM switches to manual dialing mode from the point of failure.

Example: If FAC entered is incorrect (even if CMC entered is correct), Unified CM switches to manual dialing mode and displays the following error message at the phone:

Auth code failed: Enter manually

After receiving this error message, the user must dial out FAC, CMC, and DTMF digits manually.

If FAC entered is correct and validated but CMC entered is incorrect, Unified CM switches to manual dialing mode and displays the following error message at the phone:

CM code failed: Enter manually

After receiving this error message, the user must dial CMC and DTMF digits manually.

The following table describes the comparison between using a comma and not using a comma as a delimiter.

Table 96: Comparison Between Two Methods

Method I : Using comma as a delimiter and also as a pause	Method II : Not using comma as a delimiter
Can be configured when the customer has • Overlapping route patterns • Variable length dial patterns • Overlapping FAC and CMC	Only preferred for calls made using fixed length route patterns. This method may not work when overlapping route patterns and overlapping FAC and CMC are configured.
DTMF digits can be sent after appropriate pause duration.	DTMF digits are always sent immediately after the call is connected.
Call is disconnected when invalid FAC or CMC is entered.	For FAC, CMC failure cases, Unified CM switches to manual dialing mode and user gets one more chance to enter correct code.
Can be used even when FAC and CMC are not required to make calls; that is, can be used for sending only DTMF digits.	Can be used only for the calls made over route patterns where at least one out of FAC and CMC is enabled. This method cannot be used for sending only DTMF digits.

Note Unified CM ensures FAC, CMC, and DTMF digits are not displayed in the phone placed calls history for the calls made using speed dial with the codes configured.

After a call is successful, when the user presses the Redial softkey or dials out from the placed calls history, to the user must dial out FAC, CMC, and DTMF digits manually.

When the Unified CM sends a group of DTMF digits (configured as a part of speed dial) after a pause or after the call is connected, there is a possibility that the Unified CM may out-pulse these DTMF digits quickly for remote application or remote gateway to process.

To prevent this, Unified CM pauses for the duration specified in service parameter "Pause In Speed Dial InterDigit Interval." In the previous example DTMF digits are: **987989#**

Unified CM sends out the first DTMF digit, that is, 9, and waits for the duration specified in this service parameter before sending out the next digit, that is, 8. Similarly, it follows the same pattern before sending out each digit.

The following table describes the Speed-dial and abbreviated-dial configuration settings.

Table 97: Speed-Dial and Abbreviated-Dial Configuration Settings

Field	Description
(number from 1 to 199 in the left column)	This column identifies the speed-dial button on the phone or on the Cisco Unified IP Phone Expansion Module (for example, 1, 2, 3, or 4) or the abbreviated-dial index for abbreviated dial.
Number	Enter the number that you want the system to dial when the user presses the speed-dial button. You can enter digits 0 through 9, *, #, and +, which is the international escape character. For a Pause in Speed Dial, you can enter comma (,) which can act as a delimiter as well as other pause before sending DTMF digits.
Label	Enter the text that you want to display for the speed-dial button or abbreviated-dial number. **Note** If you are configuring a Pause in Speed Dial, you must add a label so that FAC, CMC, and DTMF digits are not displayed on the phone screen. Cisco Unified Communications Manager does not make this field available for the Cisco Unified IP Phone 7910.

The following table describes the SIP Phone models and support information.

Phone Model Support

Table 98: SIP Phone Models and Support Information

Phone Model	Support	Description
Cisco Unified IP Phones 8961, 9951, 9971 using SIP	Fully Supported	• Placed calls history of a phone does not show FAC, CMC, and post-connect DTMF digits for the calls that are placed using the speed dial. • DTMF digits are sent by both out of band and RFC2833 method. In both the cases, users can hear the tone that indicates the DTMF digit is sent.

Phone Model	Support	Description
Cisco Unified Personal Communicator Clients	Supported using only method II [See Method II section]	• DTMF digits can be sent by both out of band and RFC2833 method.

The following table describes the SCCP Phone models and support information.

Table 99: SCCP Phone Models and Support Information

Phone Model	Support	Description
Cisco Unified IP Phones 7906, 7911, 7931, 7941, 7961, 7942, 7962, 7945,7965, 7970, 7971, 7975 using SCCP	Fully Supported	• Placed calls history of a phone does not show FAC, CMC, and post-connect DTMF digits for the calls placed using the speed dial. • DTMF digits can be sent by both out of band and RFC2833 method. In both the cases, users can hear the tone that indicates the DTMF digit is sent.
Other SCCP Phone Models	Partially Supported	• Placed calls history of a phone does not show FAC, CMC, and post-connect DTMF digits for calls that are placed using speed dial. • DTMF digit can be sent only by out of band method and no tone is played to indicate the digit is sent.

CME and SRST Limitations

When a phone is in the CME (configured as SRST) or SRST mode, for the speed dial calls where a comma is used as a pause duration or as a delimiter, the phone sends only the digits before the first comma as the destination address digits to the CME or SRST router. Hence, the call proceeds in the manual dialing mode, provided the appropriate dial peer is configured on the router, and users are required to dial out FAC and DTMF digits manually.

For the speed dials where FAC , CMC, and DTMF digits are entered as a continuous string , the phone sends the entire set of digits to CME or SRST router and calls may fail because the CME and SRST router does not

have capability to recognize the destination address digits , FAC, and DTMF digits from the digit string received.

Related Topics

Cisco Unified IP Phone Setup , on page 579

BLF Speed Dial Setup

When you configure 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 with a BLF/SpeedDial button on the device of the watcher.

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

For information on configuring BLF/SpeedDial buttons, see the *Cisco Unified Communications Manager Features and Services Guide*.

BLF Directed Call Park Setup

Directed Call Park allows a user to transfer a parked 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.

For information on configuring BLF/Directed Call Park buttons, see the *Cisco Unified Communications Manager Features and Services Guide*.

Set Up Cisco Unified IP Phone

You can automatically add phones to the Cisco Unified Communications Manager database by using auto-registration or manually add phones by using the Phone Configuration windows.

By enabling auto-registration, you can automatically add a Cisco Unified IP Phone to the Cisco Unified Communications Manager database when you connect the phone to your IP telephony network. During auto-registration, Cisco Unified Communications Manager assigns the next available sequential directory number to the phone. In many cases, you might not want to use auto-registration; for example, if you want to assign a specific directory number to a phone.

Note Cisco recommends using auto-registration in small configurations or testing labs only.

If you configure the clusterwide security mode to mixed mode, Cisco Unified Communications Manager disables auto-registration.

If you do not use auto-registration, you must manually add phones to the Cisco Unified Communications Manager database.

After you add a Cisco Unified IP Phone to Cisco Unified Communications Manager Administration, the RIS Data Collector service displays the device name, registration status, and the IP address of the Cisco Unified Communications Manager to which the phone is registered in the Phone Configuration window.

Before a Cisco Unified IP Phone can be used, you must use this procedure to add the phone to Cisco Unified Communications Manager. You can also use this procedure to configure third-party phones that are running SIP, H.323 clients, CTI ports, the Cisco ATA 186 Telephone Adaptor, or the Cisco IP Communicator. H.323 clients can comprise Microsoft NetMeeting clients. CTI ports designate virtual devices that Cisco Unified Communications Manager applications such as Cisco SoftPhone and Cisco Unified Communications Manager Auto-Attendant use.

When you add a new phone, you can choose a phone template that was created by the Bulk Administration Tool to configure automatically some of the phone configuration settings, based on the template.

Phone templates must exist on the server before you can select a phone template. For more information about Bulk Administration Tool phone templates, see the *Cisco Unified Communications Manager Bulk Administration Guide*.

Note Add the Cisco VG248 and VG224 Phone Ports from the Gateway Configuration window of Cisco Unified Communications Manager Administration.

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 an IPv4 URL for the web server on the phone. For phones that use an IPv6 address only, you cannot click the IPv6 address because the web server on the phone only supports IPv4.

Timesaver If you plan on using nonstandard phone button and softkey templates, configure the templates before you add the phones.

Procedure

Step 1 Choose**Device** > **Phone**.
The Find and List Phones window displays.

Step 2 Perform one of the followings tasks:

Note You can display the MAC address of a phone.

a) To copy an existing phone, locate the appropriate phone in the Find and List Phones window, click the Copy button next to the phone that you want to copy, and continue with Step 5, on page 622.

b) To copy an existing phone and copy the directory numbers, speed dials, busy lamp field/speed dials, and service URLs that are associated with the phone, locate the appropriate phone in the Find and List Phones window, click the Super Copy button next to the phone that you want to copy, and continue with Step 5, on page 622.

Note The lines that get copied become shared lines between the original phone and the new phone.

c) To add a new phone, click the Add New button and continue with Step 3, on page 622.

d) To update an existing phone, locate the appropriate phone and continue with Step 5, on page 622.

Step 3 Perform one of the following tasks when you choose the phone model:

a) From the Phone Type drop-down list box, select the appropriate phone type or device and click Next. After you choose a phone type, you cannot modify it.

b) Select the Phone Template radio button, select the appropriate phone template from the drop-down list box, and click Next. (Only phone templates that were created in the Bulk Administration Tool display in the drop-down list box.)

Step 4 If the Select the device protocol drop-down list box displays, choose the appropriate protocol of the device and click Next. Otherwise, continue with Step 5, on page 622.
The Phone Configuration window displays.

Step 5 Enter the appropriate settings as described in Table 95: Phone Settings, on page 583.
Only the settings that are appropriate to the chosen phone type display in the window.

Step 6 Click Save.
If you are adding a phone, a message displays that states that the phone has been added to the database. To add a directory number to this phone, click one of the line links, such as Line [1] - Add a new DN, in the Association Information pane that displays on the left side of the window. Continue to configure the directory number settings.

If you are updating a phone, a message displays that states that you must click the Apply Config button for your changes to take effect and synchronize the phone.

What to Do Next

You can continue to configure the following on the phone:

- speed-dial buttons
- services
- service URL buttons
- busy lamp field/speed-dial settings

Related Topics

About Directory Number Setup , on page 289
Gateway Setup , on page 465
Cisco Unified IP Phone Setup , on page 579
BLF Speed Dial Setup , on page 620
Synchronize Phone , on page 625
Set Up Speed-dial Buttons or Abbreviated Dialing , on page 625
Set Up IP Phone Services , on page 626
Display Phone MAC Address , on page 635
About Phone Button Template Setup , on page 721
Create Nonstandard Softkey Templates , on page 726
Add IP Phone Services to Phone Buttons , on page 743

Migrate Existing Phone Settings to Another Phone

The Phone Migration window in Cisco Unified Communications Manager Administration allows you to migrate feature, user, and line configuration for a phone to a different phone. You can migrate data to a different phone model or to the same phone model that runs a different protocol. For example, you can migrate data from a Cisco Unified IP Phone 7965 to a Cisco Unified IP Phone 7975, or you can migrate data from a phone model that runs SCCP, for example, the Cisco Unified IP Phone 7965 (SCCP) and move it to the same phone model that runs SIP, for example, the Cisco Unified IP Phone 7965 (SIP).

Tip Phone migration allows you to port existing phone configuration to a new phone without the need to add a phone, lines, speed dials, and so on.

Before you migrate existing phone configuration to a different phone, see the topics related to phone migration for information to review before you migrate the settings and migration procedures.

Before You Begin

Before you can migrate phone configuration to a new phone, consider the following information:

- If the phone models do not support the same functionality, be aware that you may lose functionality on the new phone after the migration occurs. Before you save the migration configuration in the Phone Migration window, Cisco Unified Communications Manager Administration displays a warning that you may lose feature functionality.
- Some phone models do not support phone migration; for example, CTI port, H.323 client, Cisco Unified Mobile Communicator, Cisco IP Softphone, and so on.
- Before you can migrate the phone configuration, you must create a phone template in BAT for the phone model and protocol to which you want to migrate. For example, if you want to migrate the configuration for a Cisco Unified IP Phone 7965 to a Cisco Unified IP Phone 7975, you create the phone template for the Cisco Unified IP Phone 7975.
  If the Phone Configuration window does not display a field for the original phone, but the field is required for the new phone, the new phone uses the value from the phone template for the required field.
- The new phone uses the same existing database record as the original phone, so migrating the phone configuration to the new phone removes the configuration for the original phone from Cisco Unified Communications Manager Administration/the Cisco Unified Communications Manager database; that is, you cannot view or access the configuration for the original phone after the migration.
  Migrating to a phone that uses fewer speed dials or lines does not remove the speed dials or lines for the original phone from Cisco Unified Communications Manager Administration/the Cisco Unified Communications Manager database, although some speed dials/lines do not display on the new phone. After you migrate the configuration, you can see all speed dials and lines for the original phone in the Phone Configuration window for the new phone.
- Before you migrate the phone configuration to a new phone, ensure that the phones are unplugged from the network. After you perform the migration tasks, you can plug the new phone into the network and register the device.
- Before you migrate the phone configuration to a new phone, ensure that you have enough device license units for the new phone.

Tip If you want to migrate the configuration for multiple phones, use the Bulk Administration Tool; for information on how to perform this task, see the Cisco Unified Communications Manager Bulk Administration Guide.

Procedure

Step 1 Make sure that you created a phone template in BAT for the phone model and protocol to which you want to migrate the data. In Cisco Unified Communications Manager Administration, choose **Bulk Administration** > **Phones** > **Phone Template**.

Step 2 In the Find and List Phones window (**Device** > **Phone**), find the phone configuration that you want to migrate.

Step 3 After you display the Phone Configuration window for the phone configuration that you want to migrate, choose Migrate Phone from the Related Links drop-down list box.

Step 4 Enter the migration configuration settings, as described in Table 100: Phone Migration Configuration Settings , on page 624.

Step 5 Click Save.

Step 6 If a warning displays that the new phone may lose feature functionality, click OK.

Related Topics

Phone Migration Settings , on page 624

Phone Migration Settings

The following table lists configuration settings for phone migration.

Table 100: Phone Migration Configuration Settings

Field	Description
Phone Template	From the drop-down list box, choose the phone template for the phone model to which you want to migrate the phone configuration. Only the phone templates that you configured in the Phone Template window in Bulk Administration display (**Bulk Administration** > **Phones** > **Phone Template**).
MAC Address	This field support hardware phones only. Enter the Media Access Control (MAC) address for the new Cisco Unified IP Phone to which you are migrating the configuration. Make sure that the value comprises 12 hexadecimal characters. For information on how to access the MAC address for your phone, see the Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager that supports your phone model.

Field	Description
Description	If you want to do so, enter a description for the new phone. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).

Related Topics

Cisco Unified IP Phone Setup , on page 579

Synchronize Phone

To synchronize a phone with the most recent configuration changes, perform the following procedure, which applies 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 **Device** > **Phone**.
The Find and List Phones window displays.

Step 2 Choose the search criteria to use.

Step 3 Click **Find**.
The window displays a list of phones that match the search criteria.

Step 4 Check the check boxes next to the phones that you want to synchronize. To choose all phones 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**.

Related Topics

Cisco Unified IP Phone Setup , on page 579

Set Up Speed-dial Buttons or Abbreviated Dialing

You use Cisco Unified Communications Manager Administration to configure speed-dial buttons for phones if you want to provide speed-dial buttons for users or if you are configuring phones that do not have a specific user who is assigned to them. Users use Cisco Unified Communications Self Care Portal to change the speed-dial buttons on their phones.

Table 97: Speed-Dial and Abbreviated-Dial Configuration Settings , on page 618 describes the speed-dial button and abbreviated dialing configuration settings. The Speed Dial and Abbreviated Dial Configuration window contains the following sections: speed-dial settings on the phone and abbreviated-dial settings that

are not associated with a button. The descriptions in Table 97: Speed-Dial and Abbreviated-Dial Configuration Settings , on page 618 apply to both sections.

The system provides a total of 199 speed-dial and abbreviated-dial settings.

- Speed Dial Settings

  Configure these settings for the physical buttons on the phone.

- Abbreviated Dial Settings

  Configure these settings for the speed-dial numbers that you access with abbreviated dialing. When the user configures up to 199 speed-dial entries, part of the speed-dial entries can get assigned to the speed-dial buttons on the IP phone; the remaining speed-dial entries get used for abbreviated dialing. When a user starts dialing digits, the AbbrDial softkey displays on the phone, and the user can access any speed-dial entry by entering the appropriate index (code) for abbreviated dialing.

Note Not all Cisco Unified IP Phones support abbreviated dialing. See the phone user guide for information.

Procedure

Step 1 From the Phone Configuration window, choose Add/Update Speed Dials from the Related Links drop-down list box at the top of the window and click Go.
The Speed Dial and Abbreviated Dial Configuration window displays for this phone.

Note To display the Phone Configuration window, choose **Device** > **Phone**. Enter your search criteria and click Find. Choose the phone for which you want to configure speed-dial buttons.

Step 2 Enter the appropriate settings as described in Table 97: Speed-Dial and Abbreviated-Dial Configuration Settings , on page 618.

Note For a Pause in Speed Dial, you can enter comma (,) which can act as a delimiter as well as other pause before sending DTMF digits.

Step 3 To apply the changes, click Save.

Step 4 To close the window, click Close.

Related Topics

Cisco Unified IP Phone Setup , on page 579

Set Up IP Phone Services

From certain phones, such as Cisco Unified IP Phone 7970, 7960, and 7940, users can access services, such as weather, stock quotes, or other services that are available to them. Using Cisco Unified Communications Manager Administration, you can set up the available services for phones. For some services, users can use the Cisco Unified Communications Self Care Portal menu to modify the services. For information about the Cisco Unified Communications Self Care Portal, see the Cisco Unified IP Phone User Guide that is specific to your phone model.

Related Topics

Subscribe to Service , on page 627
Update Service , on page 628
Unsubscribe From Service , on page 628
IP Phone Services Setup , on page 733

Subscribe to Service

You (or an end user) cannot subscribe to services that are marked as enterprise subscriptions. (The enterprise subscription column displays in the Find and List IP Phone Services window. If true displays in the column, you (or an end user) cannot subscribe to the service. In a service is marked as an enterprise subscription, the service automatically displays on the phone, unless you disable the service in the Phone Services Configuration window.

To subscribe to new services for a phone, perform the following steps.

Before You Begin

If you need to do so, add the phone services to Cisco Unified Communications Manager.

Procedure

Step 1 Choose **Device** > **Phone**.
The Find and List Phones window displays.

Step 2 To locate a specific phone, enter search criteria and click Find.
A list of phones that match the search criteria displays.

Step 3 Choose the phone to which you want to add a service.
The Phone Configuration window displays.

Step 4 On the upper, right side of the window, choose Subscribe/Unsubscribe Services from the Related Links drop-down list box and click Go.
The Subscribed IP phone services window displays for this phone.

Step 5 From the Select a Service drop-down list box, choose the service that you want to add to the phone.

Step 6 Click Next.
The window displays with the service that you chose. If you want to choose a different service, click Back and repeat Step 5, on page 627.

Step 7 If the service has required parameters, enter that information into the field that is provided.

Step 8 Click Subscribe.
The service displays in the Subscribed Services list.

Step 9 If you want to subscribe to additional services, click the Subscribe a New Service link in the Subscribed Services area. Repeat Step 5, on page 627 through Step 8, on page 627.

Related Topics

Cisco Unified IP Phone Setup , on page 579

About IP Phone Service Setup , on page 733

Update Service

Perform the following steps to update a service. You can update the service name and service parameter values, if necessary.

Procedure

Step 1 Choose **Device** > **Phone**.
The Find and List Phones window displays.

Step 2 To locate a specific phone, enter search criteria and click Find.
A list of phones that match the search criteria displays.

Step 3 Choose the phone for which you want to update a service.
The Phone Configuration window displays.

Step 4 On the upper, right side of the window, choose Subscribe/Unsubscribe Services from the Related Links drop-down list box and click Go.

Step 5 From the Subscribed Services list, choose a service.

Step 6 Update the appropriate parameter and click Save.

Related Topics

Cisco Unified IP Phone Setup , on page 579

Unsubscribe From Service

To unsubscribe from a service, perform the following steps.

Procedure

Step 1 Choose **Device** > **Phone**.
The Find and List Phones window displays.

Step 2 Enter search criteria to locate a specific phone and click Find.
A list of phones that match the search criteria displays.

Step 3 Choose the phone from which you want to delete a service.
The Phone Configuration window displays.

Step 4 On the upper, right side of the window, choose Subscribe/Unsubscribe Services from the Related Links drop-down list box and click Go.

Step 5 From the Subscribed Services list, choose a service.

Step 6 Click Unsubscribe.
A warning message verifies that you want to unsubscribe from the service.

Step 7 To unsubscribe, click OK or click Cancel to restore your previous settings.

Related Topics

Cisco Unified IP Phone Setup , on page 579

Service URL Button Setup

From some Cisco Unified IP Phone models, users can access information services, such as weather, stock quotes, or other services that are available to them. Using Cisco Unified Communications Manager Administration, you can configure services to be available on a phone button (speed dial button) and then configure that button for the phone. See the Cisco Unified IP Phone User Guide that is specific for your phone model.

Tip When you configure a service, you specify whether you want the service to display under the Messages, Directory, or Services button. If your phone model has a Messages, Directory, or Services button/option, the service can display under any of these buttons in addition to the phone button for speed dials (service URL button). If a service is marked as an enterprise subscription, you cannot add the service to a service URL button.

Related Topics

IP Phone Services Setup , on page 733

Add Service URL Button

To configure the service URL buttons for a phone, perform the following steps.

Before You Begin

Before you begin, perform the following configurations:

- Add the services to Cisco Unified Communications Manager.
- Configure the service URL button on the phone button template.
- Subscribe to the service.

Procedure

Step 1 Choose **Device** > **Phone**.
The Find and List Phones window displays.

Step 2 To locate a specific phone, enter search criteria and click Find.
A list of phones that match the search criteria displays.

Step 3 Choose the phone to which you want to add a service URL button.
The Phone Configuration window displays.

Step 4 In the Association Information area on the left side of the Phone Configuration window, click the Add a new SURL link.
The Configure Service URL Buttons window displays for this phone.

Step 5 From the Button Service drop-down list box, choose the service that you want to add to or update for the phone.

Step 6 You can change the value in the Label field.

Step 7 To add the service to or update for the phone button, click Save.

Step 8 If more buttons and services are available, you can assign additional services to additional buttons by repeating Add Service URL Button , on page 629 through Add Service URL Button , on page 629.

Step 9 To close this window and return to the Phone Configuration window, click Close.

Related Topics

Cisco Unified IP Phone Setup , on page 579
Set Up IP Phone Services , on page 626
About Phone Button Template Setup , on page 721
About IP Phone Service Setup , on page 733

Copy Phone Record to Remote Destination Profile

You can copy information from a phone record to a new remote destination profile, which is used for Cisco Unified Mobility and Mobile Voice Access. See the *Cisco Unified Communications Manager Features and Services Guide* for instructions on configuring remote destination profiles.

Procedure

Step 1 From the Phone Configuration window, choose Copy to Remote Destination Profile from the Related Links drop-down list box at the top of the window and click Go.
The Remote Destination Profile Configuration window displays for this phone.

Step 2 Enter the appropriate settings as described in the topics related to Cisco Unified Mobility in the *Cisco Unified Communications Manager Features and Services Guide*.

Step 3 To apply the changes, click Save.

Step 4 To close the window, click Close.

Related Topics

Cisco Unified IP Phone Setup , on page 579

Modify Custom Phone Button Template Button Items

When you configure a phone and associate it with a custom, nonstandard phone button template, you can modify the phone button items in the associated phone button template. When you do so, you create a new

phone button template that is customized for this particular phone. The new phone button template displays in the list of phone button templates with a name of the format “SEP999999999999-Individual Template”, where 999999999999 specifies the MAC address of the phone.

Note You cannot perform this procedure if the phone is associated with a standard phone button template. You must first associate this phone with a custom, nonstandard phone template.

To modify the button items of a custom, nonstandard phone button template, perform the following steps.

Procedure

Step 1 Choose **Device** > **Phone**.
The **Find and List Phones** window displays.

Step 2 Enter search criteria and click **Find** to locate a specific phone.
A list of phones that match the search criteria displays.

Step 3 Choose the phone for which you want to modify the phone button items.
The **Phone Configuration** window displays.

Step 4 Click **Modify Button Items** in the **Association Information** area on the left side of the window.
A popup window warns you that unsaved changes (to the phone) may be lost. If you have made changes to the phone configuration, click **Cancel** and save those changes before proceeding.

Step 5 Click **OK** to continue.
The **Reorder Phone Button Configuration** window displays. This window comprises the following panes:

Associated Items

This pane displays a list of the items that are assigned to the phone buttons in this phone button template. The system assigns the first item in the list to button 1, the second item to button 2, and so forth.

Unassigned Associated Items

This pane displays a list of the items that are not assigned to phone buttons in this phone button template.

Dissociate These Items

This pane displays a list of the items that cannot presently be assigned to a phone button.

Step 6 Select an item in the **Associated Items** pane and click the up or down arrows to change the order of the associated items.

Step 7 Select an item in either the **Associated Items** or **Unassigned Associated Items** panes and click the left or right arrows to move the item to the other pane.

Step 8 Select an item in the **Associated Items** or **Unassigned Associated Items** panes and click the up or down arrows to move that item to the **Dissociate These Items** pane or vice versa.

Step 9 Click **Save** after you have finished moving items among the panes and all items are in the desired order.

Step 10 Click **Close** to close the **Reorder Phone Button Configuration** window.

Related Topics

Cisco Unified IP Phone Setup , on page 579

Find Actively Logged-In Device

The Cisco Extension Mobility and Cisco Extension Mobility Cross Cluster features keep a record of the devices to which users are actively logged in. For the Cisco Extension Mobility feature, the actively logged-in device report tracks the local phones that are actively logged in by local users; for the Cisco Extension Mobility Cross Cluster feature, the actively logged-in device report tracks the local phones that are actively logged in by remote users.

Cisco Unified Communications Manager provides a specific search window for searching for devices to which users are logged in. Follow these steps to search for a specific device or to list all devices for which users are actively logged in.

Procedure

Step 1 Choose **Device** > **Phone**.
The Find and List Phones window displays. Records from an active (prior) query may also display in the window.

Step 2 Select the Actively Logged In Device Report from the Related Links drop-down list box in the upper, right corner of the Find and List Phones window and click Go. The Find and List Actively Logged In Devices window displays.

Step 3 To find all actively logged-in device records in the database, ensure the dialog box is empty; go to Step 4, on page 632.
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 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.

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.

Related Topics

Cisco Unified IP Phone Setup , on page 579

Find Remotely Logged-In Device

The Cisco Extension Mobility Cross Cluster feature keeps a record of the devices to which users are logged in remotely. The Remotely Logged In Device report tracks the phones that other clusters own but that are actively logged in by local users who are using the EMCC feature.

Cisco Unified Communications Manager provides a specific search window for searching for devices to which users are logged in remotely. Follow these steps to search for a specific device or to list all devices for which users are logged in remotely.

Procedure

Step 1 Choose **Device** > **Phone**.
The Find and List Phones window displays. Records from an active (prior) query may also display in the window.

Step 2 Select Remotely Logged In Device from the Related Links drop-down list box in the upper, right corner of the Find and List Phones window and click Go. The Find and List Remotely Logged In Devices window displays.

Step 3 To find all remotely logged-in device records in the database, ensure the dialog box is empty; go to Find Actively Logged-In Device , on page 632.
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 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.

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.

Related Topics

Cisco Unified IP Phone Setup , on page 579

Remote Lock

In Unified Communications Manager, some phones can be locked remotely. When a remote lock is performed on a phone, the phone cannot be used until it is unlocked.

If a phone supports the Remote Lock feature, a **Lock** button appears in the top right hand corner.

To remotely lock a phone, perform the following steps.

Procedure

Step 1 Choose **Device** > **Phone**.
The **Find and List Phones** window displays.

Step 2 Enter search criteria and click **Find** to locate a specific phone.
A list of phones that match the search criteria displays.

Step 3 Choose the phone for which you want to perform a remote lock.
The **Phone Configuration** window displays.

Step 4 Click **Lock**.
If the phone is not registered, a popup window displays to inform you that the phone will be locked the next time it is registered. Click **Lock**. A **Device Lock/Wipe Status** section appears, with information about the most recent request, whether it is pending, and the most recent acknowledgement.

Remote Wipe

In Unified Communications Manager, some phones can be wiped remotely. When a remote wipe is performed on a phone, the operation resets the phone to its factory settings. Everything previously stored on the phone is wiped out.

If a phone supports the Remote Wipe feature, a **Wipe** button appears in the top right hand corner.

Caution This operation cannot be undone. You should only perform this operation when you are sure you want to reset the phone to its factory settings.

To remotely wipe a phone, perform the following steps.

Procedure

Step 1 Choose **Device** > **Phone**.
The **Find and List Phones** window displays.

Step 2 Enter search criteria and click **Find** to locate a specific phone.
A list of phones that match the search criteria displays.

Step 3 Choose the phone for which you want to perform a remote wipe.
The **Phone Configuration** window displays.

Step 4 Click **Wipe**.
If the phone is not registered, a popup window displays to inform you that the phone will be wiped the next time it is registered. Click **Wipe**. A **Device Lock/Wipe Status** section appears, with information about the most recent request, whether it is pending, and the most recent acknowledgment.

Phone Lock/Wipe Report

Unified Communications Manager provides a specific search window for searching for devices which have been remotely locked and/or remotely wiped. Follow these steps to search for a specific device or to list all devices which have been remotely locked and/or remotely wiped.

Procedure

Step 1 Choose **Device** > **Phone**.
The Find and List Phones window displays. Records from an active (prior) query may also display in the window.

Step 2 Select the Phone Lock/Wipe Report from the Related Links drop-down list box in the upper, right corner of the Find and List Phones window and click Go. The Find and List Lock and Wipe Devices window displays.

Step 3 To find all remotely locked or remotely wiped device records in the database, ensure that the text box is empty; go to Step 4.
To filter or search records

a) From the first drop-down list box, select the device operation type(s) to search.
b) From the second drop-down list box, select a search parameter.
c) From the third drop-down list box, select a search pattern.
d) 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 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.

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.

Display Phone MAC Address

The Media Access Control (MAC) address comprises a unique, 12-character, hexadecimal number that identifies a Cisco Unified IP Phone or other hardware device. Locate the number on a label on the bottom of the phone (for example, 000B6A409C405 for Cisco Unified IP Phone 7900 family of phones or SS-00-0B-64-09-C4-05 for Cisco IP Phone SP 12+ and 30 VIP). Cisco Unified Communications Manager makes the MAC address a required field for Cisco Unified IP Phone device configuration. When you enter the MAC address in Cisco Unified Communications Manager fields, do not use spaces or dashes and do not include the “SS” that may precede the MAC address on the label.

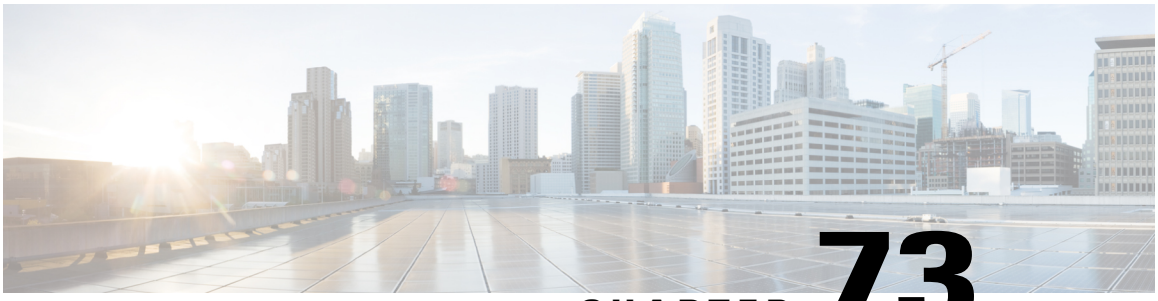
For more information on displaying the MAC Address or additional configuration settings on Cisco Unified IP Phones, see the Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager

that supports the phone model. To display the MAC address for the Cisco IP Phone 12 Series and Cisco IP Phone 30 Series phones or the Cisco VG248 Gateway, perform the following tasks:

- Cisco IP Phone 12 (SP +) Series and 30 Series (VIP)—Press ** to display the MAC address on the second line of the LCD display.
- Cisco VG248 phone ports—The MAC address specifies the endpoint from the Gateway Configuration window of Cisco Unified Communications Manager Administration.
- Cisco VG224 phone ports—You can configure a Cisco VG224 gateway as an MGCP gateway or an SCCP gateway. When it is configured as an SCCP gateway, it can have 24 analog phone endpoints. When it is configured this way, it functions similarly to an IOS SCCP gateway. The MAC address for each individual phone gets calculated by using a formula that considers the slot position, subunit, port, and the last 10 characters of the original MAC address.
- Cisco IP Communicator—Get the MAC address from the network interface of the client PC on which you want to install the Cisco IP Communicator application.

Related Topics

Gateway Setup , on page 465



CHAPTER 73

Trunk Setup

This chapter provides information about Cisco Unified Communications Manager trunk configuration.

About Trunk Setup

Use a trunk device to configure a logical route to a gatekeeper (that is, the wholesale network or an intercluster trunk with gatekeeper control), to an intercluster trunk without a gatekeeper, or to a SIP network. Choose from the following available trunk types:

- H.225 trunk (gatekeeper controlled)
- Intercluster trunk (gatekeeper controlled)
- Intercluster trunk (non-gatekeeper controlled)
- SIP trunk

Tip Configure SIP Trunk Security Profiles and SIP Profiles before you configure a SIP Trunk. For more information, see the *Cisco Unified Communications Manager Security Guide*.

Tip Resetting a trunk drops any calls in progress that are using that trunk. Restarting a gateway tries to preserve the calls in progress that are using that gateway, if possible. Other devices wait until calls complete before restarting or resetting. Resetting/restarting an H.323 or SIP device does not physically reset/restart the hardware; it only reinitializes the configuration that is loaded by Cisco Unified Communications Manager.

For SIP trunks, Restart and Reset behave the same way, so all active calls will disconnect when either choice is pressed. Trunks do not have to undergo a Restart or Reset when Packet Capture is enabled or disabled.

Related Topics

SIP Trunk Security Profile Setup , on page 167
About SIP Profile Setup , on page 745

H.225 and Intercluster Trunks Settings

The following table describes the trunk settings for gatekeeper-controlled H.225 trunks, gatekeeper-controlled intercluster trunks, and non-gatekeeper-controlled intercluster trunks.

Table 101: H.225 and Intercluster Trunks Settings

Field	Description
Device Information	
Device Name	Enter a unique identifier for the trunk.
Description	Enter a descriptive name for the trunk. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
Device Pool	Choose the appropriate device pool for the trunk. For trunks, device pools specify a list of Cisco Unified Communications Managers that the trunk uses to distribute the call load dynamically. **Note** Calls that are initiated from a phone that is registered to a Cisco Unified Communications Manager that does not belong to the device pool of the trunk use different Cisco Unified Communications Managers of this device pool for different outgoing calls. Selection of nodes occurs in a random order.A call that is initiated from a phone that is registered to a Cisco Unified Communications Manager that does belong to the device pool of the trunk uses the same Cisco Unified Communications Manager node for outgoing calls if the Cisco Unified Communications Manager is up and running.

Field	Description
Common Device Configuration	Choose the common device configuration to which you want this trunk assigned. The common device configuration includes the attributes (services or features) that are associated with a particular user. Common device configurations are configured in the Common Device Configuration window.
Call Classification	This parameter determines whether an incoming call through this trunk is considered off the network (OffNet) or on the network (OnNet). When the Call Classification field is configured as Use System Default, the setting of the Cisco Unified Communications Manager clusterwide service parameter, Call Classification, determines whether the trunk is OnNet or OffNet. This field provides an OnNet or OffNet alerting tone when the call is OnNet or OffNet, respectively. The alerting tones are provided by Cisco Unified Communications Manager Annunciators. Use this parameter in conjunction with the settings on the Route Pattern Configuration window to classify an outgoing call as OnNet or OffNet.
Media Resource Group List	This list provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from among the available media resources according to the priority order that a Media Resource Group List defines.
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 box, choose the appropriate location for this trunk. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this trunk consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the ***System Location*** menu option. For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*. The location also associates with the RSVP policy with regard to other locations. The configuration allows RSVP to be enabled and disabled based upon location pairs.

Field	Description
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.
Tunneled Protocol	This drop-down list box displays for H.225 trunks, gatekeeper-controlled trunks, and non-gatekeeper-controlled trunks. Choose the QSIG option if you want to use trunks to transport (tunnel) non-H.323 protocol information in H.323 signaling messages from Cisco Unified Communications Manager to other Annex M.1-compliant H.323 PINXs. QSIG tunneling supports the following features: Call Completion, Call Diversion, Call Transfer, Identification Services, and Message Waiting Indication.
QSIG Variant	To display the options in the QSIG Variant drop-down list box, choose QSIG from the Tunneled Protocol drop-down list box. This parameter specifies the protocol profile that is sent in outbound QSIG facility information elements. From the drop-down list box, choose one of the following options: • No Changes— Default. Keep this parameter set to the default value unless a Cisco support engineer instructs otherwise. • Not Selected • ECMA—Choose for ECMA PBXs that use Protocol Profile 0x91. • ISO—Choose for PBXs that use Protocol Profile 0x9F. For more information, see the following information: • Be aware that the QSIG Variant can also be defined as a clusterwide parameter. • For information on QSIG support with Cisco Unified Communications Manager, see the *Cisco Unified Communications Manager System Guide*.

Field	Description
ASN.1 ROSE OID Encoding	To display the options in the ASN.1 ROSE OID Encoding drop-down list box, choose QSIG from the Tunneled Protocol drop-down list box. This parameter specifies how to encode the Invoke Object ID (OID) for remote operations service element (ROSE) operations. From the drop-down list box, choose one of the following options: • No Changes—Default. Keep this parameter set to the default value unless a Cisco support engineer instructs otherwise. • Not Selected • Use Global Value ECMA—If you chose the ECMA option from the QSIG Variant drop-down list box, choose this option. • Use Global Value ISO—If you chose the ISO option from the QSIG Variant drop-down list box, choose this option. • Use Local Value For more information, see the following information: • Be aware that ASN.1 ROSE OID Encoding can also be defined as a clusterwide parameter. • For information on QSIG support with Cisco Unified Communications Manager, see the *Cisco Unified Communications Manager System Guide*.

Field	Description
Packet Capture Mode	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. Choose one of the following options from the drop-down list box: • None—This option, which serves as the default setting, indicates that no packet capturing is occurring. After you complete packet capturing, configure this setting. • Batch Processing Mode—Cisco Unified Communications Manager writes the decrypted or nonencrypted messages to a file, and the system encrypts each file. On a daily basis, the system creates a new file with a new encryption key. Cisco Unified Communications Manager, which stores the file for seven days, also stores the keys that encrypt the file in a secure location. Cisco Unified Communications Manager stores the file in the PktCap virtual directory. A single file contains the time stamp, source IP address, source IP port, destination IP address, packet protocol, message length, and the message. The IREC tool uses HTTPS, administrator username and password, and the specified day to request a single encrypted file that contains the captured packets. Likewise, the tool requests the key information to decrypt the encrypted file. **Tip** You do not have to reset the trunk after enabling/disabling Packet Capturing. For more information on capturing packets, see the *Troubleshooting Guide for Cisco Unified Communications Manager*.
Packet Capture Duration	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. This field specifies the maximum number of minutes that is allotted for one session of packet capturing. The default setting equals 0, although the range exists from 0 to 300 minutes. To initiate packet capturing, enter a value other than 0 in the field. After packet capturing completes, the value, 0, displays. For more information on capturing packets, see the *Cisco Unified Communications Manager Troubleshooting Guide*.

Field	Description
Media Termination Point Required	This check box is used to indicate whether a media termination point (MTP) is used to implement features that H.323 does not support (such as hold and transfer). Check the Media Termination Point Required check box if you want to use a media termination point to implement features. Uncheck the Media Termination Point Required check box if you do not want to use a media termination point to implement features. Use this check box only for H.323 clients and those H.323 devices that do not support the H.245 Empty Capabilities Set or if you want media streaming to terminate through a single source. If you check this check box to require an MTP and one or both parties are a video endpoint, the call operates as audio only.
Retry Video Call as Audio	This check box applies only to video endpoints that receive a call. For trunks, this check box pertains to calls that are received from Cisco Unified Communications Manager but not to calls that are received from the wide-area network (WAN). By default, the system checks this check box to specify that this device should immediately retry a video call as an audio call (if it cannot connect as a video call) prior to sending the call to call control for rerouting. If you uncheck this check box, a video call that fails to connect as video does not try to establish as an audio call. The call then fails to call control, and call control routes the call via Automatic Alternate Routing (AAR) and/or route/hunt list.
Wait for Far-End H.245 Terminal Capability Set	This field applies only to H.323 devices. This check box specifies that Cisco Unified Communications Manager waits to receive the far-end H.245 Terminal Capability Set before it sends its H.245 Terminal Capability Set. By default, the system checks this check box. To specify that Cisco Unified Communications Manager should initiate capabilities exchange, uncheck this check box.
Path Replacement Support	If you choose the QSIG option from the Tunneled Protocol drop-down list box, this check box displays for H.225 trunks, gatekeeper-controlled trunks, and non-gatekeeper-controlled trunks. This setting works with QSIG tunneling (Annex M.1) to ensure that non-H.323 information gets sent on the leg of the call that uses path replacement. **Note** The default setting leaves the check box unchecked. When you choose the QSIG Tunneled Protocol option, the system automatically checks the check box.

Field	Description
Transmit UTF-8 for Calling Party Name	This device uses the user locale setting of the SIP trunks to determine whether to send unicode and whether to translate received Unicode information. For the sending device, if you check this check box and the user locale setting in the device pool at the device matches the terminating phone user locale, the device sends unicode. If the user locale settings do not match, the device sends ASCII. The receiving device translates incoming unicode characters based on the user locale setting of the sending device pool of the device. If the user locale setting matches the terminating phone user locale, the phone displays the characters. **Note** The phone may display garbled characters if the two ends of the trunk configure user locales that do not belong to the same language group.
Unattended Port	Check this check box if calls can be redirected, transferred and forwarded to an unattended port, such as a voice mail port. The default value for this check box leaves it unchecked.
SRTP Allowed	Check the SRTP Allowed check box if you want Cisco Unified Communications Manager to allow secure and nonsecure calls over the trunk. If you do not check this check box, Cisco Unified Communications Manager prevents SRTP negotiation with the trunk and uses RTP. **Caution** If you check this check box, Cisco strongly recommends that you configure IPSec, so you do not expose keys and other security-related information during call negotiations. If you do not configure IPSec correctly, consider signaling between Cisco Unified Communications Manager and the gateway as nonsecure. For more information on encryption for trunks, see the *Cisco Unified Communications Manager Security Guide*.
H.235 Pass Through Allowed	This feature allows Cisco Unified Communications Manager to transparently pass through the shared secret (Diffie-Hellman key) and other H.235 data between two H.235 endpoints, so the two endpoints can establish a secure media channel. To allow H.235 pass through, check the check box.

Field	Description
Enable SAF	Check this check box if you want to enable this intercluster (non-gatekeeper controlled) trunk for SAF. When a trunk is enabled for SAF, the trunk can support the call control discovery feature. SAF-enabled trunks that are assigned to the CCD advertising service in the Advertising Service window handle inbound calls from remote call-control entities that use the SAF network. (**Call Routing** > **Call Control Discovery** > **Advertising Service**) SAF-enabled trunks that are assigned to the CCD requesting service handle outgoing calls to learned patterns. (**Call Routing** > **Call Control Discovery** > **Requesting Service**) For more information on the call control discovery feature, see the *Cisco Unified Communications Manager Features and Services Guide*.
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified Communications Manager inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values: • Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates. • Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified Communications Manager places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVPAgent). If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the *Cisco Unified Communications Manager System Guide* for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified Communications Manager first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified Communications Manager first tries to find a transcoder that is also designated as a TRP. See the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.

Field	Description
PSTN Access	If you use the Cisco Intercompany Media Engine feature, check this check box to indicate that calls made through this trunk might reach the PSTN. Check this check box even if all calls through this trunk device do not reach the PSTN. For example, check this check box for tandem trunks or an H.323 gatekeeper routed trunk if calls might go to the PSTN. When checked, this check box causes the system to create upload voice call records (VCRs) to validate calls made through this trunk device. By default, this check box remains checked. For more information on Cisco Intercompany Media Engine, see the *Cisco Intercompany Media Engine Installation and Configuration Guide*.
Intercompany Media Engine (IME)	
E.164 Transformation Profile	Check this check box if you want to use the Cisco Intercompany Media Engine and calls might reach the PSTN. For more information, see the *Cisco Intercompany Media Engine Installation and Configuration Guide*. From the drop-down list box, choose the appropriate E.164 transformation that you created on the Intercompany Media Services E.164 Transformation Configuration window (**Advanced Features** > **Intercompany Media Services** > **E.164 Transformation**). For more information on Cisco Intercompany Media Engine, see the *Cisco Intercompany Media Engine Installation and Configuration Guide*.
Incoming Calling Party Settings	
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.

Field	Description
National Number	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 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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. • Strip Digits—Enter the number of digits, up to the number 24, 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—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 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. 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. **Tip** For more information on configuring these settings, see the *Cisco Unified Communications Manager Features and Services Guide*.

Field	Description
International Number	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 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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. • Strip Digits—Enter the number of digits, up to the number 24, 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— 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 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. 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. **Tip** For more information on configuring these settings, see the *Cisco Unified Communications Manager Features and Services Guide*.

Field	Description
Subscriber Number	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 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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. • Strip Digits—Enter the number of digits, up to the number 24, 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 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. 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. **Tip** For more information on configuring these settings, see the *Cisco Unified Communications Manager Features and Services Guide*.

Field	Description
Unknown Number	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 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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. • Strip Digits—Enter the number of digits, up to the number 24, 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—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 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. 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. **Tip** For more information on configuring these settings, see the *Cisco Unified Communications Manager Features and Services Guide*.
Incoming Called Party Settings The H.323 protocol does not support the international escape character +. To ensure the correct prefixes, including the +, get applied to inbound calls over H.323 trunks, configure the incoming called party settings; that is, configuring the incoming called party settings ensures that when an inbound call comes from a H.323 trunk, Cisco Unified Communications Manager transforms the called party number back to the value that was originally sent over the trunk.	
Clear Prefix Settings	To delete all prefixes for all called party number types, click Clear Prefix Settings.

Field	Description
Default Prefix Settings	To enter the default value for all prefix fields at the same time, click Default Prefix Settings.
National Number	Configure the following settings to transform incoming called party numbers that use National for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called party numbers that use National for the Called Party Numbering Type. You can enter up to 16 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, you cannot configure the Strip Digits field. 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 called party prefix, which supports both the prefix and strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, 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 called party number of National type before it applies the prefixes. • Use Device Pool CSS— 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 the device. • Calling Search Space—This setting allows you to transform the called party number of National called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

Field	Description
International Number	Configure the following settings to transform incoming called party numbers that use International for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called party numbers that use International for the Called Party Numbering Type. You can enter up to 16 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, you cannot configure the Strip Digits field. 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 called party prefix, which supports both the prefix and strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, 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 called party number of International type before it applies the prefixes. • Use Device Pool CSS—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 the device. • Calling Search Space—This setting allows you to transform the called party number of International called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

Field	Description
Unknown Number	Configure the following settings to transform incoming called party numbers that use Unknown for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called numbers that use Unknown for the Called Party Numbering Type. You can enter up to 16 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, you cannot configure the Strip Digits field. 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 called party prefix, which supports both the prefix and strip digit functionality. **Tip** To configure the Strip Digits field, 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 called party number of Unknown type before it applies the prefixes. • Use Device Pool CSS—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 the device. • Calling Search Space—This setting allows you to transform the called party number of Unknown called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

Field	Description
Subscriber Number	Configure the following settings to transform incoming called party numbers that use Subscriber for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called numbers that use Subscriber for the Called Party Numbering Type. You can enter up to 16 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, you cannot configure the Strip Digits field. 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 called party prefix, which supports both the prefix and strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, 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 called 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 transform the called party number of Subscriber called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.
Multilevel Precedence and Preemption (MLPP) Information	
MLPP Domain	From the drop-down list box, choose an MLPP domain to associate with this device. If you leave this field blank, this device inherits its MLPP domain from the value that was set for the device pool. If the device pool does not have an MLPP Domain setting, this device inherits its MLPP Domain from the value that was set for the MLPP Domain Identifier enterprise parameter.

Field	Description
MLPP Indication	If available, this setting specifies whether a device that is capable of playing precedence tones will use the capability when it places an MLPP precedence call. From the drop-down list box, choose a setting to assign to this device from the following options: • Default—This device inherits its MLPP indication setting from its device pool. • Off—This device does not handle nor process indication of an MLPP precedence call. • On—This device does handle and process indication of an MLPP precedence call. **Note** Do not configure a device with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful.
Call Routing Information	
Inbound Calls	
Significant Digits	Significant digits represent the number of final digits that are retained on inbound calls. Use for the processing of incoming calls and to indicate the number of digits that are used to route calls that are coming in to the H.323 device. Choose the number of significant digits to collect, from 0 to 32. Cisco Unified Communications Manager counts significant digits from the right (last digit) of the number that is called.
Calling Search Space	From the drop-down list box, select the appropriate calling search space for the trunk. The calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number. You can configure the number of items that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more 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. **Note** To set the maximum list box items, choose **System** > **Enterprise Parameters** and choose CCMAdmin Parameters.
AAR Calling Search Space	Choose the appropriate calling search space for the device to use when performing automated alternate routing (AAR). 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.

Field	Description
Prefix DN	Enter the prefix digits that are appended to the called party number on incoming calls. Cisco Unified Communications Manager adds prefix digits after first truncating the number in accordance with the Significant Digits setting. You can enter the international escape character +.
Redirecting Number IE Delivery - Inbound	Check this check box to accept the Redirecting Number IE in the incoming SETUP message to the Cisco Unified Communications Manager. (The UUIE part of the SETUP message includes the Redirecting Number IE.) Uncheck the check box to exclude the Redirecting Number IE. You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box. **Note** Default leaves the check box checked. You cannot check this check box if you choose the QSIG option from the Tunneled Protocol drop-down list box.
Enable Inbound FastStart	Check this check box to enable the H.323 FastStart call connections on incoming calls. By default, the check box remains unchecked for the H.323 gateway. For intercluster calls, you must check the Enable Inbound FastStart check box on Cisco Unified Communications Manager servers in other clusters for the outbound FastStart feature to work.
Connected Party Settings	
Connected Party Transformation CSS	This setting is applicable only for inbound Calls. This setting allows you to transform the connected party number that Cisco Unified Communications Manager sends in another format, such as a DID or E.164 number. This setting is applicable while sending connected number for basic call as well as sending connected number after inbound call is redirected. Cisco Unified Communications Manager includes the transformed number in the Connected Number Information Element (IE) of CONNECT and NOTIFY messages. Make sure that the Connected Party Transformation CSS that you choose contains the connected party transformation pattern that you want to assign to this device. **Note** If you configure the Connected Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Connected Party Transformation CSS in a non-null partition that is not used for routing.

Field	Description
Use Device Pool Connected Party Transformation CSS	To use the Connected 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 Connected Party Transformation CSS that you configured for this device in the Trunk Configuration window.
Outbound Calls	
Called Party Transformation CSS	This setting allows you to send transformed called party number in SETUP message for outgoing calls. Make sure that the Called Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device. **Note** If you configure the Called Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Called Party Transformation pattern in a non-null partition that is not used for routing.
Use Device Pool Called Party Transformation CSS	To use the Called 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 Called Party Transformation CSS that you configured for this device in the Trunk Configuration window.
Calling Party Transformation CSS	This setting allows you to send transformed calling party number in SETUP message for outgoing calls. Also when redirection occurs for outbound calls, this CSS will be used to transform the connected number sent from Cisco Unified Communications Manager side in outgoing NOTIFY messages. 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** 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.
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 Trunk Configuration window.

Field	Description
Calling Party Selection	Choose the directory number that is sent on an outbound call on a gateway. The following options specify which directory number is sent: • Originator—Send the directory number of the calling device. • First Redirect Number—Send the directory number of the redirecting device. • Last Redirect Number—Send the directory number of the last device to redirect the call. • First Redirect Number (External)—Send the external directory number of the redirecting device. • Last Redirect Number (External)—Send the external directory number of the last device to redirect the call.
Calling Line ID Presentation	Cisco Unified Communications Manager uses calling line ID presentation (CLIP) as a supplementary service to control the display of the calling party number on the called party phone display screen. Choose Default if you do not want to change the presentation setting. Choose Allowed if you want calling number information to display. Choose Restricted if you do not want the calling number information to display.
Called Party IE Number Type Unknown	Choose the format for the type of number in called party directory numbers. Cisco Unified Communications Manager sets the called 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 called directory number to be encoded to a non-national numbering plan type. Choose one of the following options: • Cisco Unified Communications Manager—Cisco Unified Communications Manager sets the directory number type. • Unknown—This option indicates that 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.

Field	Description
Calling Party IE Number Type Unknown	Choose the format for the type of number 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 Unified Communications Manager—Cisco Unified Communications Manager sets the directory number type. • Unknown—This option indicates that 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. **Tip** 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 Cisco Unified Communications Manager, which is the default, your configuration for this field overwrites the Calling Party Number Type setting for the outgoing call through a particular gateway.

Field	Description
Called Numbering Plan	Choose the format for the numbering plan in called party directory numbers. Cisco Unified Communications Manager sets the called DN numbering plan. 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 called numbering plan to be encoded to a non-national numbering plan. Choose one of the following options: • Cisco Unified Communications Manager—Cisco Unified Communications Manager sets the Numbering Plan in the directory number. • ISDN—Use when you are dialing outside the dialing plan for your country. • National Standard—Use when you are dialing within the dialing plan for your country. • Private—Use when you are dialing within a private network. • Unknown—This option indicates that the dialing plan is unknown.
Calling Numbering Plan	Choose the format for the numbering plan in calling party directory numbers. Cisco Unified Communications Manager sets the calling DN numbering plan. 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 numbering plan to be encoded to a non-national numbering plan. Choose one of the following options: • Cisco Unified Communications Manager—Cisco Unified Communications Manager sets the Numbering Plan in the directory number. • ISDN—Use when you are dialing outside the dialing plan for your country. • National Standard—Use when you are dialing within the dialing plan for your country. • Private—Use when you are dialing within a private network. • Unknown—This option indicates that the dialing plan is unknown.

Field	Description
Caller ID DN	Enter the pattern, from 0 to 24 digits, that you want to use to format the caller ID on outbound calls from the trunk. For example, in North America • 555XXXX = Variable Caller ID, where X represents an extension number. The Central Office (CO) appends the number with the area code if you do not specify it. • 5555000 = Fixed Caller ID. Use this form when you want the Corporate number to be sent instead of the exact extension from which the call is placed. The CO appends the number with the area code if you do not specify it. You can enter the international escape character +.
Display IE Delivery	Check this check box to enable delivery of the display information element (IE) in SETUP and CONNECT messages for the calling and called party name delivery service. **Note** The default setting leaves this check box checked. You cannot check this check box if you choose the QSIG option from the Tunneled Protocol drop-down list box.
Redirecting Number IE Delivery - Outbound	Check this check box to indicate the first redirecting number and the redirecting reason of the call when the call is forwarded. (The UUIE part of the outgoing SETUP message from the Cisco Unified Communications Manager includes the Redirecting Number IE.) Uncheck the check box to exclude the first Redirecting Number and the redirecting reason. You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box. **Note** The default setting leaves this check box checked. You cannot check this check box if you choose the QSIG option from the Tunneled Protocol drop-down list box.
Enable Outbound FastStart	Check this check box to enable the H.323 FastStart feature on outgoing calls. By default, the check box remains unchecked for the H.323 gateway or trunk. When you check the Enable Outbound FastStart check box, you must set the Media Termination Point Required, Media Resource Group Lists, and Codec for Outbound FastStart.

Field	Description
Codec For Outbound FastStart	Choose the codec for use with the H.323 device for an outbound FastStart call: • G711 mu-law 64K (default) • G711 a-law 64K • G723 • G729 • G729AnnexA • G729AnnexB • G729AnnexA-AnnexB When you check the Enable Outbound FastStart check box, you must choose the codec for supporting outbound FastStart calls.
Gatekeeper Information (for gatekeeper-controlled H.225 trunks and intercluster trunks)	
Gatekeeper Name	Choose the gatekeeper that controls this trunk. **Note** For a gatekeeper-controlled trunk to register correctly with a gatekeeper through use of H.323 dynamic addressing, you must set the Send Product ID and Version ID service parameter to True. (The default value specifies False.) To do so, choose System > Service Parameters and find the Send Product ID and Version ID service parameter for the Cisco CallManager service in the Clusterwide Parameters (Device - H323) portion of the Service Parameter Configuration window.
Terminal Type	Use the Terminal Type field to designate the type for all devices that this trunk controls. Always set this field to Gateway for normal trunk call admission control.

Field	Description
Technology Prefix	Use this optional field to eliminate the need for entering the IP address of every Cisco Unified Communications Manager when configuring the gw-type-prefix on the gatekeeper: • If you leave this field blank (the default setting), you must specify the IP address of each Cisco Unified Communications Manager that can register with the gatekeeper when you enter the gw-type-prefix command on the gatekeeper. • When you use this field, make sure that the value that you enter exactly matches the type-prefix value that is specified with the gw-type-prefix command on the gatekeeper. For example, if you leave this field blank and you have two Cisco Unified Communications Managers with IP addresses of 10.1.1.2 and 11.1.1.3, enter the following gw-type-prefix command on the gatekeeper: gw-type-prefix 1#* default-technology gw ip 10.1.1.2 gw ip 11.1.1.3 If you enter 1#* in this field, enter the following gw-type-prefix command on the gatekeeper: gw-type-prefix 1#* default-technology
Zone	Use this optional field to request a specific zone on the gatekeeper with which Cisco Unified Communications Manager will register. The zone specifies the total bandwidth that is available for calls between this zone and another zone: • If you do not enter a value in this field, the zone subnet command on the gatekeeper determines the zone with which Cisco Unified Communications Manager registers. Cisco recommends the default setting for most configurations. • If you want Cisco Unified Communications Manager to register with a specific zone on the gatekeeper, enter the value in this field that exactly matches the zone name that is configured on the gatekeeper with the zone command. Specifying a zone name in this field eliminates the need for a zone subnet command for each Cisco Unified Communications Manager that is registered with the gatekeeper. See the command reference documentation for your gatekeeper for more information.
Remote Cisco Unified Communications Manager Information (for non-gatekeeper-controlled intercluster trunks)	
Server 1 IP Address/Host Name	Enter the IP address or host name of the first remote Cisco Unified Communications Manager that this trunk accesses.

Field	Description
Server 2 IP Address/Host Name	Enter the IP address or host name of the second remote Cisco Unified Communications Manager that this trunk accesses. **Note** If this non-gatekeeper-controlled intercluster trunk accesses the device pool of a remote non-gatekeeper-controlled intercluster trunk and that device pool has a second Cisco Unified Communications Manager node, you must enter the second remote Cisco Unified Communications Manager IP address/host name in this field.
Server 3 IP Address/Host Name	Enter the IP address or host name of the third remote Cisco Unified Communications Manager that this trunk accesses. **Note** If this non-gatekeeper-controlled intercluster trunk accesses the device pool of a remote non-gatekeeper-controlled intercluster trunk and that device pool has a third Cisco Unified Communications Manager node, you must enter the third remote Cisco Unified Communications Manager IP address/host name in this field.
UUIE Configuration	
Passing Precedence Level Through UUIE	Check this check box to enable passing MLPP information through the PRI 4ESS UUIE field. The system uses this box for interworking with DRSN switch. The system makes this check box available only if the PRI Protocol Type value of PRI 4ESS is specified for this trunk. The default value specifies unchecked.
Security Access Level	Enter the value for the security access level. Valid values include 00 through 99. The system makes this field available only if the Passing Precedence Level Through UUIE check box is checked. The default value specifies 2.
Geolocation Configuration	
Geolocation	From the drop-down list box, choose a geolocation. You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation. You can also choose a geolocation that has been configured with the **System** > **Geolocation Configuration** menu option. For an explanation of geolocations, including configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocations, see the *Cisco Unified Communications Manager Features and Services Guide*.

Field	Description
Geolocation Filter	From the drop-down list box, choose a geolocation filter. If you leave the <None> setting, no geolocation filter gets applied for this device. You can also choose a geolocation filter that has been configured with the **System** > **Geolocation Filter** menu option. For an explanation of geolocation filters, including configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocation filters, see the *Cisco Unified Communications Manager Features and Services Guide*.
Send Geolocation Information	Check this box to send geolocation information for this device. For an overview and details of how logical partitioning uses geolocation information, see the Cisco Unified Communications Manager Features and Services Guide.

Related Topics

Location Setup , on page 127
Service Parameter Setup , on page 151
About Calling Search Space Setup , on page 273

SIP Trunk Settings

The following table describes the settings for SIP trunks.

Table 102: SIP Trunk Settings

Field	Description
Trunk Service Type	Choose one of the following options from the Trunk Service Type drop-down list box: • None—Choose this option if the trunk will not be used for call control discovery, Extension Mobility Cross Cluster, or Cisco Intercompany Media Engine. • Call Control Discovery—Choosing this option enables the trunk to support call control discovery. If you assign this trunk to the CCD advertising service in the Advertising Service window, the trunk handles inbound calls from remote call-control entities that use the SAF network. If you assign this trunk to the CCD requesting service in the Requesting Service window, the trunk handles outgoing calls to learned patterns. For more information on the call control discovery feature, see the *Cisco Unified Communications Manager Features and Services Guide*. • Extension Mobility Cross Cluster—Choose this option to enable the trunk to support the Extension Mobility Cross Cluster (EMCC) feature. Choosing this option causes the following settings to remain blank or unchecked and become unavailable for configuration, thus retaining their default values: Media Termination Point Required, Unattended Port, Destination Address, Destination Address IPv6, and Destination Address is an SRV. For more information about the EMCC feature, see the *Cisco Unified Communications Manager Features and Services Guide*. • Cisco Intercompany Media Engine—Ensure that the Cisco IME server is installed and available before you configure this field. **Tip** After you choose Call Control Discovery, Extension Mobility Cross Cluster, or Cisco Intercompany Media Engine for the trunk service type and click Next, you cannot change the trunk to a different type.
Device Information	
Device Name	Enter a unique identifier for the trunk. Enter a unique identifier for the trunk. The device name can include up to 50 alphanumeric characters: A-Z, a-z, numbers, hyphens (-) and underscores (_) only.
Description	Enter a descriptive name for the trunk. The description can include up to 114 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).

Field	Description
Device Pool	Choose the appropriate device pool for the trunk. For trunks, device pools specify a list of Cisco Unified Communications Managers that the trunk uses to distribute the call load dynamically. **Note** Calls that are initiated from a phone that is registered to a Cisco Unified Communications Manager that does not belong to the device pool of the trunk use different Cisco Unified Communications Managers of this device pool for different outgoing calls. Selection of Cisco Unified Communications Manager nodes occurs in a random order. A call that is initiated from a phone that is registered to a Cisco Unified Communications Manager that does belong to the device pool of the trunk uses the same Cisco Unified Communications Manager node for outgoing calls if the Cisco Unified Communications Manager is up and running. The default value for Device Pool specifies Not Selected.
Common Device Configuration	Choose the common device configuration to which you want this trunk assigned. The common device configuration includes the attributes (services or features) that are associated with a particular user. Common device configurations are configured in the Common Device Configuration window.
Call Classification	This parameter determines whether an incoming call through this trunk is considered off the network (OffNet) or on the network (OnNet). The default value for Call Classification is Use System Default. When the Call Classification field is configured as Use System Default, the setting of the Cisco Unified Communications Manager clusterwide service parameter, Call Classification, determines whether the trunk is OnNet or OffNet. This field provides an OnNet or OffNet alerting tone when the call is OnNet or OffNet, respectively. Use this parameter in conjunction with the settings on the Route Pattern Configuration window to classify an outgoing call as OnNet or OffNet.
Media Resource Group List	This list provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from among the available media resources according to the priority order that a Media Resource Group List defines. The default value for Media Resource Group List specifies None.

Field	Description
Location	Use locations to implement call admission control (CAC) in a centralized call-processing system. CAC enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location. From the drop-down list box, choose the appropriate location for this trunk. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this trunk consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the **System** > **Location** menu option. For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*. The location also associates with the RSVP policy with regard to other locations. The configuration allows RSVP to be enabled and disabled based upon location pairs.
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted. The default value for AAR Group specifies None.

Tunneled Protocol	Select the QSIG option if you want to use SIP trunks or SIP gateways to transport (tunnel) QSIG messages from Cisco Unified Communications Manager to other PINXs. QSIG tunneling supports the following features: Call Back, Call Completion, Call Diversion, Call Transfer, Identification Services, Path Replacement, and Message Waiting Indication (MWI).
	
	Note Remote-Party-ID (RPID) headers coming in from the SIP gateway can interfere with QSIG content and cause unexpected behavior with Call Back capabilities. To prevent interference with the QSIG content, turn off the RPID headers on the SIP gateway.
	To turn off RPID headers on the SIP gateway, apply a SIP profile to the voIP dial peer on the gateway, as shown in the following example:
	`voice class sip-profiles 1000request ANY sip-header Remote-Party_ID remove`
	`response ANY sip-header Remote-Party-ID remove`
	
	`dial-peer voice 124 voip`
	`destination-pattern 3...`
	`signaling forward unconditional`
	`session protocol sipv2`
	`session target ipv4:<ip address>`
	`voice-class sip profiles 1000`

Field	Description
QSIG Variant	To display the options in the QSIG Variant drop-down list box, select QSIG from the Tunneled Protocol drop-down list box. This parameter specifies the protocol profile that is sent in outbound QSIG facility information elements. From the drop-down list box, select one of the following options: • No Changes—Default. Keep this parameter set to the default value unless a Cisco support engineer instructs otherwise. • Not Selected • ECMA—Select for ECMA PBX systems that use Protocol Profile 0x91. • ISO—Select for PBX systems that use Protocol Profile 0x9F. For more information, see the following information: • Be aware that the QSIG Variant can also be defined as a clusterwide parameter. • For information on QSIG support with Cisco Unified Communications Manager, see the *Cisco Unified Communications Manager System Guide*.
ASN.1 ROSE OID Encoding	To display the options in the ASN.1 ROSE OID Encoding drop-down list box, choose QSIG from the Tunneled Protocol drop-down list box. This parameter specifies how to encode the Invoke Object ID (OID) for remote operations service element (ROSE) operations. From the drop-down list box, select one of the following options: • No Changes—Default. Keep this parameter set to the default value unless a Cisco support engineer instructs otherwise. • Not Selected • Use Global Value ECMA—If you selected the ECMA option from the QSIG Variant drop-down list box, select this option. • Use Global Value ISO—If you selected the ISO option from the QSIG Variant drop-down list box, select this option. • Use Local Value For more information, see the following information: • Be aware that ASN.1 ROSE OID Encoding can also be defined as a clusterwide parameter. • For information on QSIG support with Cisco Unified Communications Manager, see the Cisco Unified Communications Manager System Guide.

Field	Description
Packet Capture Mode	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. Choose one of the following options from the drop-down list box: • None—This option, which serves as the default setting, indicates that no packet capturing is occurring. After you complete packet capturing, configure this setting. • Batch Processing Mode—Cisco Unified Communications Manager writes the decrypted or nonencrypted messages to a file, and the system encrypts each file. On a daily basis, the system creates a new file with a new encryption key. Cisco Unified Communications Manager, which stores the file for seven days, also stores the keys that encrypt the file in a secure location. Cisco Unified Communications Manager stores the file in the PktCap virtual directory. A single file contains the time stamp, source IP address, source IP port, destination IP address, packet protocol, message length, and the message. The TAC debugging tool uses HTTPS, administrator username and password, and the specified day to request a single encrypted file that contains the captured packets. Likewise, the tool requests the key information to decrypt the encrypted file. Before you contact TAC, you must capture the SRTP packets by using a sniffer trace between the affected devices. For more information on capturing packets, see the *Troubleshooting Guide for Cisco Unified Communications Manager*.
Packet Capture Duration	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. This field specifies the maximum number of minutes that is allotted for one session of packet capturing. The default setting equals 0, although the range exists from 0 to 300 minutes. To initiate packet capturing, enter a value other than 0 in the field. After packet capturing completes, the value, 0, displays. For more information on capturing packets, see the *Cisco Unified Communications Manager Troubleshooting Guide*.

Field	Description
Media Termination Point Required	You can configure Cisco Unified Communications Manager SIP trunks to always use an MTP. Check this check box to provide media channel information in the outgoing INVITE request. When this check box is checked, all media channels must terminate and reoriginate on the MTP device. If you uncheck the check box, the Cisco Unified Communications Manager can decide whether calls are to go through the MTP device or be connected directly between the endpoints. **Note** If check box remains unchecked (default case), Cisco Unified Communications Manager will attempt to dynamically allocate an MTP if the DTMF methods for the call legs are not compatible. For example, existing phones that run SCCP support only out-of-band DTMF, and existing phones that run SIP support RFC2833. Because the DTMF methods are not identical, the Cisco Unified Communications Manager dynamically allocates an MTP. If, however, a new phone that runs SCCP, which supports RFC2833 and out-of-band, calls an existing phone that runs SIP, Cisco Unified Communications Manager does not allocate an MTP because both phones support RFC2833. So, by having the same type of DTMF method supported on each phone, no need exists for MTP.
Retry Video Call as Audio	This check box pertains to outgoing SIP trunk calls and does not impact incoming calls. By default, the system checks this check box to specify that this device should immediately retry a video call as an audio call (if it cannot connect as a video call) prior to sending the call to call control for rerouting. If you uncheck this check box, a video call that fails to connect as video does not try to establish as an audio call. The call then fails to call control, and call control routes the call via Automatic Alternate Routing (AAR) and/or route/hunt list.
Path Replacement Support	This check box displays when you select QSIG from the Tunneled Protocol drop-down list box. This setting works with QSIG tunneling to ensure that non-SIP information gets sent on the leg of the call that uses path replacement. **Note** The default setting leaves the check box unchecked. When you select the QSIG Tunneled Protocol option, the system automatically checks the check box. Alternatively, if the Tunneled Protocol option is set to None, the Path Replacement Support check box displays as grayed out and is not available.

Field	Description
Transmit UTF-8 for Calling Party Name	This device uses the user locale setting of the device pool to determine whether to send unicode and whether to translate received Unicode information. For the sending device, if you check this check box and the user locale setting in the device pool matches the terminating phone user locale, the device sends unicode. If the user locale settings do not match, the device sends ASCII. The receiving device translates incoming unicode characters based on the user locale setting of the sending device pool. If the user locale setting matches the terminating phone user locale, the phone displays the characters. **Note** The phone may display malformed characters if the two ends of the trunk configure user locales that do not belong to the same language group. The default value for Transmit UTF-8 for Calling Party Name leaves the check box unchecked.
Transmit UTF-8 Names in QSIG APDU	This device uses the user locale setting of the device pool to determine whether to send unicode and whether to translate received Unicode information. For the sending device, if you check this check box and the user locale setting in the device pool matches the terminating phone user locale, the device sends unicode and encodes in UTF-8 format. If the user locale settings do not match, the device sends ASCII and encodes in UTF-8 format. If the configuration parameter is not set and the user locale setting in the device pool matches the terminating phone user locale, the device sends unicode (if the name uses 8-bit format) and encodes in ISO8859-1 format. The default value for Transmit UTF-8 Names in QSIG APDU leaves the check box unchecked.
Unattended Port	Check this check box if calls can be redirected and transferred to an unattended port, such as a voice mail port. The default value for this check box leaves it unchecked.

Field	Description
SRTP Allowed	Check this check box if you want Cisco Unified Communications Manager to allow secure and nonsecure media calls over the trunk. Checking this check box enables Secure Real-Time Protocol (SRTP) SIP Trunk connections and also allows the SIP trunk to fall back to Real-Time Protocol (RTP) if the endpoints do not support SRTP. If you do not check this check box, Cisco Unified Communications Manager prevents SRTP negotiation with the trunk and uses RTP negotiation instead. The default value for this check box leaves it unchecked. **Caution** If you check this check box, Cisco strongly recommends that you use an encrypted TLS profile, so that keys and other security-related information do not get exposed during call negotiations. If you use a non-secure profile, SRTP will still work but the keys will get exposed in signaling and traces. In that case, you must ensure the security of the network between Cisco Unified Communications Manager and the destination side of the trunk. For more information on encryption for trunks, see the *Cisco Unified Communications Manager Security Guide*.
Consider Traffic on This Trunk Secure	This field provides an extension to the existing security configuration on the SIP trunk, which enables a SIP trunk call leg to be considered secure if SRTP is negotiated, independent of the signaling transport. Choose one of the following values: • When using both sRTP and TLS—Default • When using sRTP Only—Displays when you check the SRTP Allowed check box For more information on security and trunks, see the *Cisco Unified Communications Manager Security Guide*.
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.

Field	Description
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified Communications Manager inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values: • Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates. • Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified Communications Manager places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVPAgent). If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the *Cisco Unified Communications Manager System Guide* for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified Communications Manager first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified Communications Manager first tries to find a transcoder that is also designated as a TRP. See the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.
PSTN Access	If you use the Cisco Intercompany Media Engine feature, check this check box to indicate that calls made through this trunk might reach the PSTN. Check this check box even if all calls through this trunk device do not reach the PSTN. For example, check this check box for tandem trunks or an H.323 gatekeeper routed trunk if calls might go to the PSTN. When checked, this check box causes the system to create upload voice call records (VCRs) to validate calls made through this trunk device. By default, this check box remains checked. For more information on Cisco Intercompany Media Engine, see the Cisco Intercompany Media Engine Installation and Configuration Guide.

Field	Description
Run On All Active Unified CM Nodes	To enable the trunk to run on every node, check this check box.
Intercompany Media Engine (IME)	
E.164 Transformation Profile	Check this check box if you want to use the Cisco Intercompany Media Engine and calls might reach the PSTN. For more information, see the Cisco Intercompany Media Engine Installation and Configuration Guide. From the drop-down list box, choose the appropriate E.164 transformation that you created on the Intercompany Media Services E.164 Transformation Configuration window (**Advanced Features** > **Intercompany Media Services** > **E.164 Transformation**). For more information on Cisco Intercompany Media Engine, see the Cisco Intercompany Media Engine Installation and Configuration Guide.
Multilevel Precedence and Preemption (MLPP) Information	
MLPP Domain	From the drop-down list, choose an MLPP domain to associate with this device. If you leave this field blank, this device inherits its MLPP domain from the value that is set for the device pool. If the device pool does not have an MLPP Domain setting, this device inherits its MLPP Domain from the value that is set for the MLPP Domain Identifier enterprise parameter. The default value for MLPP Domain specifies None.
Confidential Access Level	Select the appropriate CAL value from the drop-down list box.
Confidential Access Mode	From the drop-down list box, select one of the following options to set the CAL mode: • Fixed—CAL value has higher precedence over call completion. • Variable—Call completion has higher precedence over CAL level.
Call Routing Information	

Field	Description
Remote-Party-ID	Use this check box to allow or disallow the SIP trunk to send the Remote-Party-ID (RPID) header in outgoing SIP messages from Cisco Unified Communications Manager to the remote destination. If you check this box, the SIP trunk always sends the RPID header. If you do not check this box, the SIP trunk does not send the RPID header. **Note** Be aware that Calling Name Presentation, Connected Line ID, and Connected Name Presentation are not available when QSIG tunneling is enabled. Outgoing SIP Trunk Calls The configured values of the Calling Line ID Presentation and Calling Name Presentation provide the basis for the construction of the Privacy field of the RPID header. Each of these two options can have the values of Default, Allowed, or Restricted. If either option is set to Default, the corresponding information (Calling Line ID Presentation and/or Calling Name Presentation) in the RPID header comes from the Call Control layer (which is based on call-by-call configuration) within Cisco Unified Communications Manager. If either option is set to Allowed or Restricted, the corresponding information in the RPID header comes from the SIP trunk configuration window. Incoming SIP Trunk Calls The configured values of the Connected Line ID Presentation and Connected Name Presentation provide the basis for the construction of the Privacy field of the RPID header. Each of these two options can have the values of Default, Allowed, or Restricted. Be aware that the Connected Line ID Presentation and Connected Name Presentation options are relevant for 180/200 messages that the SIP trunk sends in response to INVITE messages that Cisco Unified Communications Manager receives. If either option is set to Default, the corresponding information (Connected Line ID Presentation and/or Connected Name Presentation) in the RPID header comes from the Call Control layer (which is based on call-by-call configuration) within Cisco Unified Communications Manager. If either option is set to Allowed or Restricted, the corresponding information in the RPID header comes from the SIP trunk configuration window. **Note** The Remote-party ID and Asserted Identity options represent independent mechanisms for communication of display-identity information.

Field	Description
Asserted Identity	

Field	Description
	Use this check box to allow or disallow the SIP trunk to send the Asserted-Type and SIP Privacy headers in SIP messages. If you check this check box, the SIP trunk always sends the Asserted-Type header; whether the SIP trunk sends the SIP Privacy header depends on the SIP Privacy configuration. If the check box is not selected, the SIP trunk does not include any Asserted-Type or SIP Privacy headers in its SIP messages. For more information, see the descriptions of Asserted-Type and SIP Privacy in this table. Outgoing SIP Trunk Calls—P Headers The decision of which Asserted Identity (either P-Asserted-Identity or P-Preferred-Identity) header gets sent depends on the configured value of the Asserted-Type option. A non-default value for Asserted-Type overrides values that come from Cisco Unified Communications Manager Call Control. If the Asserted-Type option is set to Default, the value of Screening Identification that the SIP trunk receives from Cisco Unified Communications Manager Call Control dictates the type of Asserted-Identity. Outgoing SIP Trunk Calls—SIP Privacy Header The SIP Privacy header gets used only when you check the Asserted Identity check box and when the SIP trunk sends either a PAI or PPI header. (Otherwise the SIP Privacy header neither gets sent nor processed in incoming SIP messages). The value of the SIP Privacy headers depends on the configured value of the SIP Privacy option. A non-default value for SIP Privacy overrides values that come from Cisco Unified Communications Manager Call Control. If the SIP Privacy option is set to Default, the Calling Line ID Presentation and Calling Name Presentation that the SIP trunk receives from Cisco Unified Communications Manager Call Control determines the SIP Privacy header. Incoming SIP Trunk Calls—P Headers The decision of which Asserted Identity (either P-Asserted-Identity or P-Preferred-Identity) header gets sent depends on the configured value of the Asserted-Type option. A non-default value for Asserted-Type overrides values that come from Cisco Unified Communications Manager Call Control. If the Asserted-Type option is set to Default, the value of Screening Identification that the SIP trunk receives from Cisco Unified Communications Manager Call Control dictates the type of Asserted-Identity. Incoming SIP Trunk Calls—SIP Privacy Header The SIP Privacy header gets used only when you check the Asserted Identity check box and when the SIP trunk sends either a PAI or PPI

Field	Description
	header. (Otherwise the SIP Privacy header neither gets sent nor processed in incoming SIP messages.) The value of the SIP Privacy headers depends on the configured value of the SIP Privacy option. A non-default value for SIP Privacy overrides values that come from Cisco Unified Communications Manager Call Control. If the SIP Privacy option is set to Default, the Connected Line ID Presentation and Connected Name Presentation that the SIP trunk receives from Cisco Unified Communications Manager Call Control determine the SIP Privacy header. **Note** The Remote-party ID and Asserted Identity options represent independent mechanisms for communication of display-identity information.
Asserted-Type	From the drop-down list, choose one of the following values to specify the type of Asserted Identity header that SIP trunk messages should include: • Default—This option represents the default value; Screening indication information that the SIP trunk receives from Cisco Unified Communications Manager Call Control determines the type of header that the SIP trunk sends. • PAI—The Privacy-Asserted Identity (PAI) header gets sent in outgoing SIP trunk messages; this value overrides the Screening indication value that comes from Cisco Unified Communications Manager. • PPI—The Privacy Preferred Identity (PPI) header gets sent in outgoing SIP trunk messages; this value overrides the Screening indication value that comes from Cisco Unified Communications Manager. **Note** These headers get sent only if the Asserted Identity check box is checked.

Field	Description
SIP Privacy	From the drop-down list, choose one of the following values to specify the type of SIP privacy header for SIP trunk messages to include: • Default—This option represents the default value; Name/Number Presentation values that the SIP trunk receives from the Cisco Unified Communications Manager Call Control compose the SIP Privacy header. For example, if Name/Number presentation specifies Restricted, the SIP trunk sends the SIP Privacy header; however, if Name/Number presentation specifies Allowed, the SIP trunk does not send the Privacy header. • None—The SIP trunk includes the Privacy:none header and implies Presentation allowed; this value overrides the Presentation information that comes from Cisco Unified Communications Manager. • ID—The SIP trunk includes the Privacy:id header and implies Presentation restricted for both name and number; this value overrides the Presentation information that comes from Cisco Unified Communications Manager. • ID Critical—The SIP trunk includes the Privacy:id;critical header and implies Presentation restricted for both name and number. The label critical implies that privacy services that are requested for this message are critical, and, if the network cannot provide these privacy services, this request should get rejected. This value overrides the Presentation information that comes from Cisco Unified Communications Manager. **Note** These headers get sent only if the Asserted Identity check box is checked.
Inbound Calls	
Significant Digits	Significant digits represent the number of final digits that are retained on inbound calls. Use for the processing of incoming calls and to indicate the number of digits that are used to route calls that are coming in to the SIP device. Choose the number of significant digits to collect, from 0 to 32, or choose All. **Note** Cisco Unified Communications Manager counts significant digits from the right (last digit) of the number that is called. The default value for Significant Digits specifies All.

Field	Description
Connected Line ID Presentation	Cisco Unified Communications Manager uses connected line ID presentation (COLP) as a supplementary service to provide the calling party with the connected party number. The SIP trunk level configuration takes precedence over the call-by-call configuration. The default value for Connected Line ID Presentation specifies Default, which translates to Allowed. Choose Default if you want Cisco Unified Communications Manager to send connected line information. Choose Restricted if you do not want Cisco Unified Communications Manager to send connected line information. If a call that originates from an IP phone on Cisco Unified Communications Manager encounters a device, such as a trunk, gateway, or route pattern, that has the Connected Line ID Presentation set to Default, the presentation value is automatically set to Allowed. **Note** Be aware that this service is not available when QSIG tunneling is enabled. For more information about this field, see the *Cisco Unified Communications Manager System Guide*.
Connected Name Presentations	Cisco Unified Communications Manager uses connected name ID presentation (CONP) as a supplementary service to provide the calling party with the connected party name. The SIP trunk level configuration takes precedence over the call-by-call configuration. The default value for Connected Name Presentation specifies Default, which translates to Allowed. Choose Default if you want Cisco Unified Communications Manager to send connected name information. Choose Restricted if you do not want Cisco Unified Communications Manager to send connected name information. **Note** Be aware that this service is not available when QSIG tunneling is enabled.
Calling Search Space	From the drop-down list box, choose the appropriate calling search space for the trunk. The calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number. You can configure the number of items that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more 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. Find and choose a calling search space name. **Note** To set the maximum list box items, choose **System** > **Enterprise Parameters** and choose CCMAdmin Parameters. The default value for Calling Search Space specifies None.

Field	Description
AAR Calling Search Space	Choose the appropriate calling search space for the device to use when performing automated alternate routing (AAR). 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. The default value for AAR Calling Search Space specifies None.
Prefix DN	Enter the prefix digits that are appended to the called party number on incoming calls. Cisco Unified Communications Manager adds prefix digits after first truncating the number in accordance with the Significant Digits setting. You can enter the international escape character +.
Redirecting Diversion Header Delivery - Inbound	Check this check box to accept the Redirecting Number in the incoming INVITE message to the Cisco Unified Communications Manager. Uncheck the check box to exclude the Redirecting Number in the incoming INVITE message to the Cisco Unified Communications Manager. You use Redirecting Number for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number, you should check the check box. The default value for Redirecting Number IE Deliver - Inbound specifies not checked.
Incoming Calling Party Settings	
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.

Field	Description
Incoming Number	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 (#). If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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. • Strip Digits—Enter the number of digits, up to the number 24, 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—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 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. 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. **Tip** For more information on configuring these settings, see the *Cisco Unified Communications Manager Features and Services Guide*.
Incoming Called Party Settings	
Clear Prefix Settings	To delete the prefix for unknown number type for the called party, click Clear Prefix Settings.
Default Prefix Settings	To enter the default value for the Prefix field for unknown number type, click Default Prefix Settings.

Field	Description
Unknown Number	Configure the following settings to transform incoming called party numbers that use Unknown for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called numbers that use Unknown for the Called Party Number Type. You can enter up to 16 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, you cannot configure the Strip Digits field. 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 does not apply any prefix or strip digit functionality. **Tip** To configure the Strip Digits field, 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 called party number of Unknown type before it applies the prefixes. • Calling Search Space—This setting allows you to transform the called party number of Unknown called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device. • Use Device Pool CSS—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 the device.
Connected Party Settings	

Field	Description
Connected Party Transformation CSS	This setting is applicable only for inbound calls. This setting allows you to transform the connected party number on the device to display the connected number in another format, such as a DID or E164 number. Cisco Unified Communications Manager includes the transformed number in the headers of various SIP messages, including 200 OK and mid-call update/reinvite messages. Make sure that the Connected Party Transformation CSS that you choose contains the connected party transformation pattern that you want to assign to this device. **Note** If you configure the Connected Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation pattern used for Connected Party Transformation in a non-null partition that is not used for routing.
Use Device Pool Connected Party Transformation CSS	To use the Connected 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 Connected Party Transformation CSS that you configured for this device in the Trunk Configuration window.
Outbound Calls	
Called Party Transformation CSS	This settings allows you to send the transformed called party number in INVITE message for outgoing calls made over SIP Trunk. Make sure that the Called Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device. **Note** If you configure the Called Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Called Party Transformation CSS in a non-null partition that is not used for routing.
Use Device Pool Called Party Transformation CSS	To use the Called 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 Called Party Transformation CSS that you configured for this device in the Trunk Configuration window.

Field	Description
Calling Party Transformation CSS	This settings allows you to send the transformed calling party number in INVITE message for outgoing calls made over SIP Trunk. Also when redirection occurs for outbound calls, this CSS will be used to transform the connected number that is sent from Cisco Unified Communications Manager side in outgoing reINVITE / UPDATE messages. 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** 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.
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 Trunk Configuration window.
Calling Party Selection	Choose the directory number that is sent on an outbound call. The following options specify which directory number is sent: • Originator—Send the directory number of the calling device. • First Redirect Number—Send the directory number of the redirecting device. • Last Redirect Number—Send the directory number of the last device to redirect the call. • First Redirect Number (External)—Send the external directory number of the redirecting device. • Last Redirect Number (External)—Send the external directory number of the last device to redirect the call. The default value for Calling Party Selection specifies Originator.
Calling Line ID Presentation	Cisco Unified Communications Manager uses calling line ID presentation (CLIP) as a supplementary service to provide the calling party number. The SIP trunk level configuration takes precedence over the call-by-call configuration. The default value for Calling Line ID Presentation specifies Default, which translates to Allowed. Choose Default if you want Cisco Unified Communications Manager to send calling number information. Choose Restricted if you do not want Cisco Unified Communications Manager to send the calling number information.

Field	Description
Calling Name Presentation	Cisco Unified Communications Manager uses calling name ID presentation (CNIP) as a supplementary service to provide the calling party name. The SIP trunk level configuration takes precedence over the call-by-call configuration. Choose Allowed, which is the default, if you want Cisco Unified Communications Manager to send calling name information. Choose Restricted if you do not want Cisco Unified Communications Manager to send the calling name information. The default value for Calling Name Presentation specifies Default. **Note** Be aware that this service is not available when QSIG tunneling is enabled.
Caller ID DN	Enter the pattern, from 0 to 24 digits, that you want to use to format the caller ID on outbound calls from the trunk. For example, in North America • 555XXXX = Variable Caller ID, where X represents an extension number. The Central Office (CO) appends the number with the area code if you do not specify it. • 5555000 = Fixed Caller ID. Use this form when you want the Corporate number to be sent instead of the exact extension from which the call is placed. The CO appends the number with the area code if you do not specify it. You can enter the international escape character +.
Caller Name	Enter a caller name to override the caller name that is received from the originating SIP Device.

Field	Description
Calling and Connected Party Info Format	This option allows you to configure whether Cisco Unified Communications Manager inserts a directory number, a directory URI, or a blended address that includes both the directory number and directory URI in the SIP identity headers for outgoing SIP messages. From the drop-down list box, choose one of the following options: • Deliver DN only in connected party—In outgoing SIP messages, Cisco Unified Communications Manager inserts the calling party's directory number in the SIP contact header information. This is the default setting. • Deliver URI only in connected party, if available—In outgoing SIP messages, Cisco Unified Communications Manager inserts the sending party's directory URI in the SIP contact header. If a directory URI is not available, Cisco Unified Communications Manager inserts the directory number instead. • Deliver URI and DN in connected party, if available—In outgoing SIP messages, Cisco Unified Communications Manager inserts a blended address that includes the calling party's directory URI and directory number in the SIP contact headers. If a directory URI is not available, Cisco Unified Communications Manager includes the directory number only. **Note** You should set this field to Deliver URI only in connected party or Deliver URI and DN in connected party only if you are setting up URI dialing between Cisco Unified CM systems of release 9.0 or greater, or between a Cisco Unified CM system of release 9. 0 or greater and a third party solution that supports URI dialing. Otherwise, you must set this field to Deliver DN only in connected party. For more information on URI dialing, see the URI dialing chapter in the *Cisco Unified Communications Manager System Guide*.
Redirecting Diversion Header Delivery - Outbound	Check this check box to include the Redirecting Number in the outgoing INVITE message from the Cisco Unified Communications Manager to indicate the original called party number and the redirecting reason of the call when the call is forwarded. Uncheck the check box to exclude the first Redirecting Number and the redirecting reason from the outgoing INVITE message. You use Redirecting Number for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number, you should check the check box. The default value for Redirecting Number IE Delivery - Outbound specifies check box does not get checked.
SIP Information	

Field	Description
Destination Address	The Destination Address represents the remote SIP peer with which this trunk will communicate. The allowed values for this field are an IP address, a fully qualified domain name (FQDN), or DNS SRV record only if the Destination Address is an SRV field is checked. **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. **Note** 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. **Note** For configuring SIP trunks when you have multiple device pools in a cluster, you must configure a destination address that is a DNS SRV destination port. Enter the name of a DNS SRV port for the Destination Address and check the Destination Address is an SRV Destination Port check box. 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.
Destination Address IPv6	The Destination IPv6 Address represents the remote SIP peer with which this trunk will communicate. You can enter one of the following values in this field: • A fully qualified domain name (FQDN) • A DNS SRV record, but only if the Destination Address is an SRV field is checked. 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.
Destination Address is an SRV	This field specifies that the configured Destination Address is an SRV record. The default value specifies unchecked.

Field	Description
Destination Port	Choose the destination port. Ensure that the value that you enter specifies any port from 1024 - 65535, or 0. **Note** You can now have the same port number that is specified for multiple trunks. You need not enter a value if the destination address is an DNS SRV port. The default 5060 indicates the SIP port. The default value for Destination Port specifies 5060.
MTP Preferred Originating Codec	Indicate the preferred outgoing codec: • 711ulaw • 711alaw • G729/G729a • G729b/G729ab **Note** To configure G.729 codecs for use with a SIP trunk, you must use a hardware MTP or transcoder that supports the G.729 codec. For more information, see the *Cisco Unified Communications Manager System Guide*. This field gets used only when the MTP Termination Point Required check box is checked.
Presence Group	Configure this field with the Presence feature. From the drop-down list box, choose a Presence group for the SIP trunk. The selected group specifies the destinations that the device/application/server that is connected to the SIP trunk can monitor. The default value for Presence Group specifies Standard Presence group, which gets configured with installation. Presence groups that are configured in Cisco Unified Communications Manager Administration also appear in the drop-down list box. Presence authorization works with presence groups to allow or block presence requests between groups. See the *Cisco Unified Communications Manager Features and Services Guide* for information about configuring permissions between groups. **Tip** You can apply a presence group to the SIP trunk or to the application that is connected to the SIP trunk. If a presence group is configured for both a SIP trunk and SIP trunk application, the presence group that is applied to the application overrides the presence group that is applied to the trunk.

Field	Description
SIP Trunk Security Profile	Choose the security profile to apply to the SIP trunk. You must apply a security profile to all SIP trunks that are configured in Cisco Unified Communications Manager Administration. Installing Cisco Unified Communications Manager provides a predefined, nonsecure SIP trunk security profile for autoregistration. To enable security features for a SIP trunk, configure a new security profile and apply it to the SIP trunk. If the trunk does not support security, choose a nonsecure profile. To identify the settings that the profile contains, choose **System** > **Security Profile** > **SIP Trunk Security Profile**. For information on how to configure security profiles, see the *Cisco Unified Communications Manager Security Guide*. The default value for SIP Trunk Security Profile specifies Not Selected.
Rerouting Calling Search Space	Calling search spaces determine the partitions that calling devices can search when they attempt to complete a call. The rerouting calling search space gets used to determine where a SIP user (A) can refer another user (B) to a third party (C). After the refer is completed, B and C connect. In this case, the rerouting calling search space that is used is that of the initial SIP user (A). **Note** Calling Search Space also applies to 3xx redirection and INVITE with Replaces features. The default value for Rerouting Calling Search Space specifies None.
Out-of-Dialog Refer Calling Search Space	Calling search spaces determine the partitions that calling devices can search when they attempt to complete a call. The out-of-dialog calling search space gets used when a Cisco Unified Communications Manager refers a call (B) that is coming into SIP user (A) to a third party (C) when no involvement of SIP user (A) exists. In this case, the system uses the out-of-dialog calling search space of SIP user (A). The default value for Out-of-Dialog Refer Calling Search Space specifies None.

Field	Description
SUBSCRIBE Calling Search Space	Supported with the Presence feature, the SUBSCRIBE calling search space determines how Cisco Unified Communications Manager routes presence requests from the device/server/application that connects to the SIP trunk. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the SIP trunk. From the drop-down list box, choose the SUBSCRIBE calling search space to use for presence requests for the SIP trunk. All calling search spaces that you configure in Cisco Unified Communications Manager Administration display in the SUBSCRIBE Calling Search Space drop-down list box. If you do not select a different calling search space for the SIP trunk from the drop-down list, the SUBSCRIBE calling search space defaults to None. To configure a SUBSCRIBE calling search space specifically for this purpose, you configure a calling search space as you do all calling search spaces.
SIP Profile	From the drop-down list box, choose the SIP profile that is to be used for this SIP trunk. The default value for SIP Profile specifies None Selected.
DTMF Signaling Method	Choose from the following options: No Preference (default)—Cisco Unified Communications Manager will pick the DTMF method to negotiate DTMF, so the call does not require an MTP. If Cisco Unified Communications Manager has no choice but to allocate an MTP (if the Media Termination Point Required check box is checked), SIP trunk will negotiate DTMF to RFC2833. RFC 2833—Choose this configuration if the preferred DTMF method to be used across the trunk is RFC2833. Cisco Unified Communications Manager makes every effort to negotiate RFC2833, regardless of MTP usage. Out of band provides the fallback method if the peer endpoint supports it. OOB and RFC 2833—Choose this configuration if both out of band and RFC2833 should be used for DTMF. **Note** If the peer endpoint supports both out of band and RFC2833, Cisco Unified Communications Manager will negotiate both out-of-band and RFC2833 DTMF methods. As a result, two DTMF events would get sent for the same DTMF keypress (one out of band and the other, RFC2833).
Normalization Script	

Field	Description
Normalization Script	From the drop-down list box, choose the script that you want to apply to this trunk. To import another script, go to the SIP Normalization Script Configuration window (**Device** > **Device Settings** > **SIP Normalization Script**), and import a new script file.
Parameter Name/Parameter Value	Optionally, enter parameter names and parameter values. Valid values include all characters except equals signs (=), semi-colons (;), and non-printable characters, such as tabs. You can enter a parameter name with no value. Example: Parameter Name Parameter Value CCA-ID 11223344 pbx location RTP You must choose a script from the Normalization Script drop-down list box before you can enter parameter names and values. To add another parameter line, click the + (plus) button. To delete a parameter line, click the - (minus) button.
Enable Trace	Check this check box to enable tracing within the script or uncheck this check box to disable tracing. When checked, the trace.output API provided to the Lua scripter produces SDI trace. **Note** Cisco recommends that you only enable tracing while debugging a script. Tracing impacts performance and should not be enabled under normal operating conditions.
Recording Information	
None	To disable the trunk for call recording, click the **None**radio button.
This trunk connects to a recording-enabled gateway	To establish the recording session using the recording enabled Cisco gateway directly connected by this trunk, click **This trunk connects to a recording-enabled gateway** radio button. **Note** Ensure that the gateway used for recording has media forking capabilities.
This trunk connects to other clusters with trunk	To establish recording session in the other cluster connected by this trunk, **This trunk connects to other clusters with trunk** radio button.
Geolocation Configuration	

Field	Description
Geolocation	From the drop-down list box, choose a geolocation. You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation. You can also choose a geolocation that has been configured with the **System** > **Geolocation Configuration** menu option. For an explanation of geolocations, including configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocations, see the *Cisco Unified Communications Manager Features and Services Guide*.
Geolocation Filter	From the drop-down list box, choose a geolocation filter. If you leave the <None> setting, no geolocation filter gets applied for this device. You can also choose a geolocation filter that has been configured with the **System** > **Geolocation Filter**menu option. For an explanation of geolocation filters, including configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocation filters, see the *Cisco Unified Communications Manager Features and Services Guide*.
Send Geolocation Information	Check this check box to send geolocation information for this device. For an overview and details of how logical partitioning uses geolocation information, see the the Cisco Unified Communications Manager Features and Services Guide.

Related Topics

Location Setup , on page 127
About Calling Search Space Setup , on page 273

Find Trunk

Because you might have multiple trunks in your network, Cisco Unified Communications Manager lets you search for trunks on the basis of specified criteria. Follow these steps to search for a specific trunk in the Cisco Unified Communications Manager database.

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

Procedure

Step 1 Choose **Device** > **Trunk**.
The Find and List Trunks 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; go to Step 3, on page 695.
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 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

Trunk Setup , on page 637

Set Up Trunk

Perform the following procedure to add a new trunk device or update an existing trunk device.

Note You can configure multiple trunk devices per Cisco Unified Communications Manager cluster.

Before You Begin

Configure SIP Trunk Security Profiles and SIP Profiles before you configure a SIP Trunk. For more information, see the related topics and the *Cisco Unified Communications Manager Security Guide*.

Procedure

Step 1 Choose **Device** > **Trunk**.
The Find and List Trunks window displays.

Step 2 Perform one of the followings tasks:

a) To add a new trunk device, click the Add New button. The Trunk Configuration window displays. Continue with Step 3, on page 696.

b) To update trunk settings, locate the appropriate trunk. Click the name of the trunk that you want to update. Continue with Step 7, on page 696.

Step 3 From the Trunk Type drop-down list, choose the type of trunk.

Step 4 If applicable, from the Device Protocol drop-down list, choose the device protocol.

Step 5 For SIP trunks, choose one of the following options from the Trunk Service Type drop-down list box:

a) None—Choose this option if the trunk will not be used for call control discovery, Extension Mobility Cross Cluster, or Cisco Intercompany Media Engine.

b) Call Control Discovery—Choosing this option enables the trunk to support call control discovery. If you assign this trunk to the CCD advertising service in the Advertising Service window, the trunk handles inbound calls from remote call-control entities that use the SAF network. If you assign this trunk to the CCD requesting service in the Requesting Service window, the trunk handles outgoing calls to learned patterns. For more information on the call control discovery feature, see the *Cisco Unified Communications Manager Features and Services Guide*.

c) Extension Mobility Cross Cluster—Choosing this option enables the trunk to support the Extension Mobility Cross Cluster feature. For more information on the Extension Mobility Cross Cluster feature, see the *Cisco Unified Communications Manager Features and Services Guide*.

d) Cisco Intercompany Media Engine—Ensure that the Cisco IME server is installed and available before you configure this field.

Tip After you choose Call Control Discovery, Extension Mobility Cross Cluster, or Cisco Intercompany Media Engine for the trunk service type and click Next, you cannot change the trunk to a different type.

Step 6 Click Next.

Step 7 On the Trunk Configuration window that displays, enter the appropriate settings for gatekeeper-controlled H.225 trunks, gatekeeper-controlled intercluster trunks, and non-gatekeeper-controlled intercluster trunks as described in Table 101: H.225 and Intercluster Trunks Settings , on page 638. For SIP trunks, enter the appropriate settings as described in Table 102: SIP Trunk Settings, on page 665.

Step 8 To add the new trunk, click Save.
The trunk gets added to the database.

If you are updating an existing trunk, click Apply Config to apply the new settings (this may also restart the device) and synchronize a trunk.

Note Resetting a trunk drops any calls in progress that are using that trunk. Restarting a gateway tries to preserve the calls in progress that are using that gateway, if possible. Other devices wait until calls complete before restarting or resetting. Resetting/restarting an H.323 or SIP device does not physically reset/restart the hardware; it only reinitializes the configuration that is loaded by Cisco Unified Communications Manager

Related Topics

SIP Trunk Security Profile Setup , on page 167
Trunk Setup , on page 637
H.225 and Intercluster Trunks Settings , on page 638
SIP Trunk Settings, on page 665
Find Trunk , on page 694
Synchronize Trunk , on page 699
About SIP Profile Setup , on page 745

Delete Trunk

Perform the following steps to delete a trunk.

Before You Begin

You cannot delete a trunk that is assigned to one or more route patterns. To find out which route patterns are using the trunk, in the Trunk Configuration window, choose Dependency Records from the Related Links drop-down list box and click Go. If dependency records are not enabled for the system, the Dependency Records Summary window displays a message. If you try to delete a trunk that is in use, Cisco Unified Communications Manager displays a message. Before deleting a trunk that is currently in use, you must perform either or both of the following tasks:

- Assign a different trunk to any route patterns that are using the trunk that you want to delete.
- Delete the route patterns that are using the trunk that you want to delete.

Procedure

Step 1 Choose **Device** > **Trunk**.
The Find and List Trunks window displays.

Step 2 To locate a specific trunk, enter search criteria and click Find.
A list of trunks that match the search criteria displays.

Step 3 Perform one of the following actions:

a) Check the check boxes next to the trunks that you want to delete and click Delete Selected.
b) Delete all trunks in the window by clicking Select All and then clicking Delete Selected.
c) From the list, choose the name of the trunk that you want to delete to display its current settings and click Delete.
A confirmation dialog displays.

Step 4 To delete the trunk, click OK.

Related Topics

About Route Pattern Setup , on page 211
Access Dependency Records , on page 982

Reset Trunk

Perform the following procedure to reset the trunk.

Caution Resetting devices can cause them to drop calls.

Procedure

Step 1 Choose **Device** > **Trunk**.
The Find and List Trunks window displays.

Step 2 To locate a specific trunk, enter search criteria and click Find.
A list of trunks that match the search criteria displays.

Step 3 From the list, click the name of the trunk that you want to reset.
The Trunk Configuration window displays.

Step 4 After you change any settings for the Trunk Device, click Reset.
The Device Reset dialog displays.

Step 5 Click one of the following choices:

a) Restart—Restarts the trunk device without shutting it down first.
b) Reset—Shuts down, then restarts, the internal trunk device. The Cisco Unified Communications Manager cluster unregisters (URQ) and then reregisters (RRQ) with the trunk if the trunk is gatekeeper controlled.
c) Close—Closes the Reset Device dialog without performing any action.

Note For SIP trunks, Restart and Reset behave the same way, so all active calls will disconnect when either choice is pressed. Trunks do not have to undergo a Restart or Reset when Packet Capture is enabled or disabled.

Related Topics

Trunk Setup , on page 637

Synchronize Trunk

To synchronize a trunk with the most recent configuration changes, perform the following procedure, which applies 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 **Device** > **Trunk**.
The Find and List Trunks window displays.

Step 2 Choose the search criteria to use.

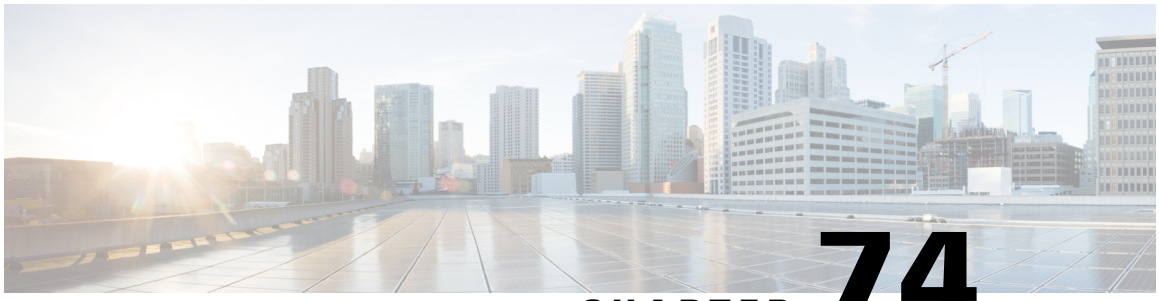
Step 3 Click Find.
The window displays a list of trunks that match the search criteria.

Step 4 Check the check boxes next to the trunks that you want to synchronize. To choose all trunks 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.

Note Active calls may get disconnected during a restart.



CHAPTER 74

Device Defaults Setup

This chapter provides information to use device defaults to set the default characteristics of each type of device that registers with a Cisco Unified Communications Manager.

About Device Defaults Setup

Use device defaults to set the default characteristics of each type of device that registers with a Cisco Unified Communications Manager. The device defaults for a device type apply to all auto-registered devices of that type within a Cisco Unified Communications Manager cluster. You can set the following device defaults for each device type to which they apply:

- Device load
- Device pool
- Phone button template

When a device auto-registers with a Cisco Unified Communications Manager, it acquires the device default settings for its device type. After a device registers, you can update its configuration individually to change the device settings.

Installing Cisco Unified Communications Manager automatically sets device defaults. You cannot create new device defaults or delete existing ones, but you can change the default settings.

Related Topics

About Device Pool Setup , on page 79
Device Defaults Settings , on page 702
Update Device Defaults , on page 702
About Phone Button Template Setup , on page 721

Device Defaults Settings

The following table describes the settings for device defaults.

Table 103: Device Defaults Settings

Field Name	Description
Device Type	This field displays the type of device for which device defaults can be set.
Protocol	This field displays the protocol that the corresponding device in the Device Type column uses.
Load Information	Enter the ID number of the firmware load that is used with a particular type of hardware device. If you install an upgrade or patch load, you must update the load information for each type of device that uses the new load.
Device Pool	Choose the device pool that is associated with each type of device. The device pool defines common characteristics for all devices in the pool.
Phone Template	Choose the phone button template that each type of Cisco Unified IP Phone uses. The template defines what keys on the phone perform that function.

Related Topics

Update Device Defaults , on page 702

Update Device Defaults

This section describes how to modify the device defaults in the Cisco Unified Communications Manager configuration database.

Before You Begin

Before updating the device defaults, perform any of the following tasks that apply to your system:

- Add new firmware files for the devices to the TFTP server.
- If you use device defaults to assign a firmware load that does not exist in the directory, those devices will fail to load the assigned firmware.
- Configure new device pools.
- If the device is a phone, configure new phone templates.

Procedure

Step 1 Choose **Device** > **Device Settings** > **Device Defaults**.

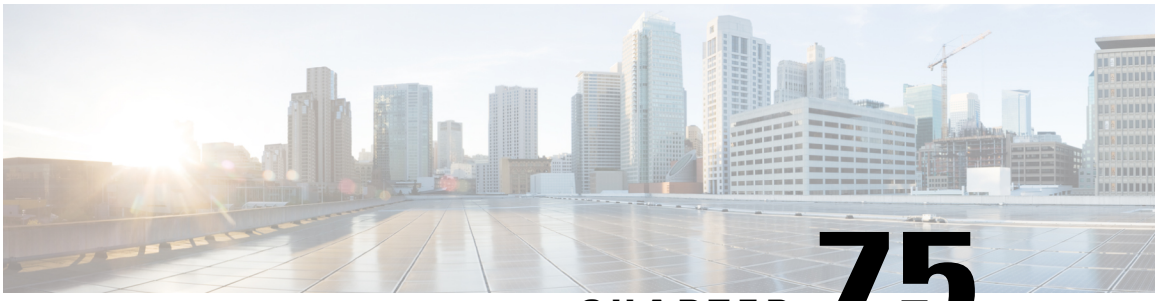
Step 2 Update the appropriate settings for the device that you want to change as described in Table 103: Device Defaults Settings , on page 702.

Step 3 To save the changes in the Cisco Unified Communications Manager configuration database, click Save.

Step 4 To reset all the devices of that type, click the Reset icon to the left of the device name and load the new defaults on all Cisco Unified Communications Managers in the cluster.
If you choose not to reset all devices of that type, only new devices that are added after you change the device defaults receive the latest defaults.

Related Topics

About Device Pool Setup , on page 79
About Phone Button Template Setup , on page 721



CHAPTER 75

Device Firmware Load Information

This chapter provides information to use device firmware load information to locate devices that are not using the default firmware load for their device type.

Find Devices with Non-default Firmware Loads

The Firmware Load Information window in Cisco Unified Communications Manager Administration enables you to quickly locate devices that are not using the default firmware load for their device type.

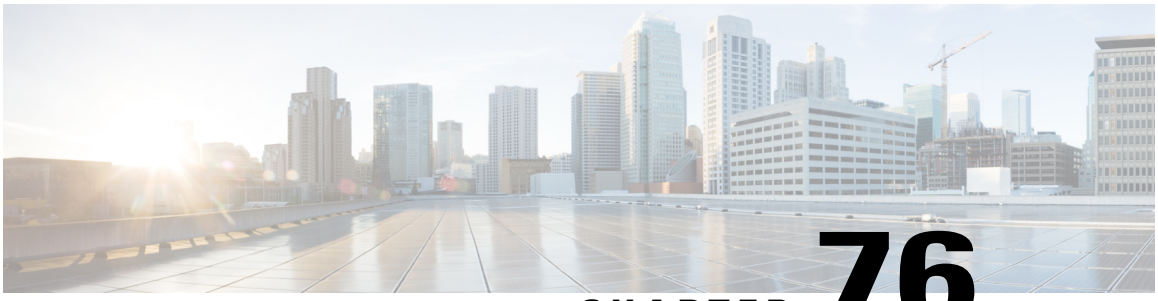
Note Each device can have an individually assigned firmware load that overrides the default.

Use the following procedure to locate devices that are not using the default firmware load.

Procedure

Step 1 Choose **Device** > **Device Settings** > **Firmware Load Information**.
The page updates to display a list of device types that require firmware loads. For each device type, the Devices Not Using Default Load column links to configuration settings for any devices that use a non-default load.

Step 2 To view a list of devices of a particular device type that are using a non-default device load, click the entry for that device type in the Devices Not Using Default Load column.
The window that opens lists the devices of a particular device type that are not running the default firmware load.



CHAPTER 76

Default Device Profile Setup

This chapter provides information about default device profile configuration.

About Default Device Profile Setup

In Cisco Unified Communications Manager Administration, use the **Device** > **Device Settings** > **Default Device Profile** menu path to configure default device profiles.

Use the default device profile for whenever a user logs on to a phone model for which no user device profile exists. To create a default device profile for each phone model that supports Cisco Extension Mobility, use the Default Device Profile Configuration window. The maximum number of default device profiles cannot exceed the number of phone models that support Cisco Extension Mobility.

For example, a user logs on to a Cisco Unified IP Phone 7960, for which there is a user device profile. The user device profile for the user gets downloaded to the phone to which the user logged on. Later, the same user logs on to a Cisco Unified IP Phone 7940, for which he does not have a user device profile. In this case, the default device profile for the 7940 gets downloaded to the phone.

A default device profile comprises the set of attributes (services and/or features) that are associated with a particular device. The default device profile contains attributes such as device type, user locale, phone button template, expansion modules, softkey template, Join Across Lines and Single Button Barge feature settings, multilevel precedence and preemption (MLPP) information, and IP phone services.

Default Device Profile Settings

The following table describes the fields that are available in the Default Device Profile Configuration window.

Table 104: Default Device Profile Settings

Field	Description
Default Device Profile Information	

Field	Description
Description	Enter a description for the default device profile configuration.
User Hold MOH Audio Source	To specify the audio source that plays when a user initiates a hold action, click the drop-down arrow and choose an audio source from the list that displays. If you do not choose an audio source, Cisco Unified Communications Manager uses the audio source that is defined in the device pool or uses the system default if the device pool does not specify an audio source ID. **Note** You define audio sources in the Music On Hold Audio Source Configuration window. For access, choose **Media Resources** > **Music On Hold Audio Source**.
User Locale	From the drop-down list 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 Manager Locale Installer documentation.
Phone Button Template	Choose the appropriate phone button template. The phone button template determines the configuration of buttons on a phone and identifies which feature (line, speed dial, and so on) is used for each button.
Softkey Template	Choose the appropriate softkey template. The softkey template determines the configuration of the softkeys on Cisco Unified IP Phones. If the device pool contains the assigned softkey template, leave this field blank.
Privacy	From the drop-down list box, choose On for each phone on which you want privacy. For more configuration information, see the *Cisco Unified Communications Manager Features and Services Guide*.

Field	Description
Single Button Barge	From the drop-down list box, choose from the following options: • Off—This device does not allow users to use the Single Button Barge/cBarge feature. • Barge—Choosing this option allows users to press the Single Button Barge shared-line button on the phone to barge into a call using Barge. • cBarge—Choosing this option allows users to press the Single Button cBarge shared-line button on the phone to barge into a call using cBarge. • Default—This device inherits the Single Button Barge/cBarge setting from the service parameter and device pool settings. **Note** If the server parameter and device pool settings are different, the device will inherit the setting from the service parameter setting. For more information, see the *Cisco Unified Communications Manager Features and Services Guide*.
Join Across Lines	From the drop-down list box, choose from the following options: • Off—This device does not allow users to use the Join Across Lines feature. • On—This device allows users to join calls across multiple lines. • Default—This device inherits the Join Across Lines setting from the service parameter and device pool settings. **Note** If the server parameter and device pool settings are different, the device will inherit the setting from the service parameter setting. For more information, see the *Cisco Unified Communications Manager System Guide*.
Always Use Prime Line	From the drop-down list box, choose one of the following options: • Off—When the phone is idle and receives a call on any line, the phone user answers the call from the line on which the call is received. • On—When the phone is idle (off hook) and receives a call on any line, the primary line gets chosen for the call. Calls on other lines continue to ring, and the phone user must select those other lines to answer these calls. • Default—Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter, which supports the Cisco CallManager service.

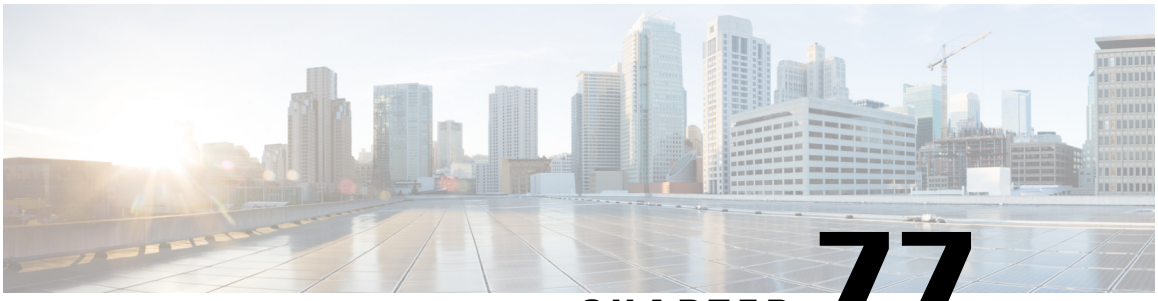
Field	Description
Always Use Prime Line for Voice Message	From the drop-down list box, choose one of the following options: • On—If the phone is idle, the primary line on the phone becomes the active line for retrieving voice messages when the phone user presses the Messages button on the phone. • Off—If the phone is idle, pressing the Messages button on the phone automatically dials the voice-messaging system from the line that has a voice message. Cisco Unified Communications Manager always selects the first line that has a voice message. If no line has a voice message, the primary line gets used when the phone user presses the Messages button. • Default—Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line for Voice Message service parameter, which supports the Cisco CallManager service.
Ignore Presentation Indicators (internal calls only)	Check the Ignore Presentation Indicators (internal calls only) check box to configure call display restrictions and ignore any presentation restriction that is received for internal calls. **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 *Cisco Unified Communications Manager Features and Services Guide*.
Do Not Disturb	Check this check box to enable Do Not Disturb on the phone.
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, including no audio or visual 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 mobile devices and dual-mode phones, you can only choose the Call Reject option. When you activate DND Call Reject on a mobile device or dual-mode phone, no call information gets presented to the device.

Field	Description
DND Incoming Call Alert	When you enable the DND Ringer Off or Call Reject option, this parameter specifies how a call displays on a phone. From the drop-down list, choose one of the following options: • None—This option specifies that the DND Incoming Call Alert setting from the Common Phone Profile window will get used for this device. • Disable—This option disables both beep and flash notification of a call but for the DND Ringer Off option, incoming call information still gets displayed. For the DND Call Reject option, no call alerts display and no information gets sent to the device. • Beep Only—For an incoming call, this option causes the phone to play a beep tone only and for the DND Ringer Off option, incoming call information gets displayed. For the DND Call Reject option, no call alerts sound and no information gets sent to the device. • Flash Only—For an incoming call, this option causes the phone to display a flash alert and for the DND Ringer Off option, incoming call information gets displayed. For the DND Call Reject option, no call alerts display and no information gets sent to the device.
Multilevel Precedence and Preemption (MLPP) Information	
MLPP Domain	Choose MLPP domain that is associated with this device from the drop-down list box.
MLPP Indication	If available, this setting specifies whether a device that is capable of playing precedence tones will use the capability when it places an MLPP precedence call. From the drop-down list box, choose a setting to assign to devices that use this default device profile from the following options: • Default—This device inherits its MLPP indication setting from its device pool. • Off—This device does not handle nor process indication of an MLPP precedence call. • On—This device does handle and process 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 or Default (when default is Off) while MLPP Preemption is set to Forceful. **Note** Turning on MLPP Indication (at the enterprise parameter, device pool, or device level) disables normal Ring Setting behavior for the lines on a device, unless MLPP Indication is turned off (overridden) for the device.

Field	Description
MLPP Preemption	If available, this 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 to assign to devices that use this default device profile from the following options: • Default—This device inherits its MLPP preemption setting from its device pool. • Disabled—This device does not allow preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. • Forceful—This device allows preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. **Note** Do not configure a default device profile with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful.
Logged Out (Default) Profile Information	
Login User Id	Enter a valid login user ID. If the user device profile is used as a logout profile, specify the login user ID that will be associated with the phone. After the user logs out from this user device profile, the phone automatically will log in to this login user ID.
Device Profile Defaults	
(listing of device profile defaults)	This pane displays a link to each default device profile that has been defined.

Related Topics

Default Device Profile Setup , on page 707
About Default Device Profile Setup , on page 707



CHAPTER 77

Device Profile Setup

This chapter provides information to configure device profiles.

About Device Profile Setup

In Cisco Unified Communications Manager Administration, use the **Device** > **Device Settings** > **Device Profile** menu path to configure device profiles.

A device profile comprises the set of attributes (services and/or features) that associate with a particular device. User device profiles include name, description, phone template, user locale, expansion modules, softkey templates, feature settings, MLPP information, directory numbers, subscribed services, and speed-dial information. You can assign the user device profile to a user, so, when the user logs in to a device, the user device profile that you have assigned to that user loads onto that device as a default login device profile. After a user device profile is loaded onto the phone, the phone picks up the attributes of that device profile.

You can also assign a user device profile to be the default logout device profile for a particular device. When a user logs out of a phone, for instance, the logout device profile loads onto the phone and gives that phone the attributes of the logout device profile. In the Cisco Unified CM Administration windows, you can create, modify, or delete the user device profile. If a user device profile is used as the logout device profile, you cannot delete the user device profile.

Cisco Unified Communications Manager also supports a device profile default. Use the device profile default for whenever a user logs on to a phone model for which no user device profile exists. To create a device profile default for each phone model that supports Cisco Extension Mobility, use the Device Profile Default Configuration window. The maximum number of device profile defaults cannot exceed the number of phone models that support Cisco Extension Mobility.

Related Topics

Default Device Profile Setup , on page 707

Device Profile Setup Tips

Make sure that phone button template(s) are already configured before you configure the device profile.

From the Association Info pane, you can configure directory numbers, speed dials, and intercom directory numbers for the device profile. For additional information about configuration settings, see the *Cisco Unified Communications Manager Features and Services Guide*.

If you click Modify Button Items, the Reorder Phone Button Configuration window opens. Use this window if you need to manage the phone button template button items.

Note You must log in to a device for changes to a user device profile to take effect.

Related Topics

Directory Number Setup , on page 289
Cisco Unified IP Phone Setup , on page 579
Modify Custom Phone Button Template Button Items , on page 630
About Phone Button Template Setup , on page 721

Additional Device Profile Setup Features

You can use the links in the Related Links drop-down list box at the top, right corner of the Device Profile Configuration window to perform additional configuration that is related to the device profile that you created. Use the following links to configure additional items:

- Add a New Line Appearance—To add a new line appearance to a device profile, select this link and click Go. The Directory Number Configuration window displays and allows you to configure a new DN that will associate to this device profile.
- Add/Update Speed Dials—To add or update the speed dial settings that are associated with a device profile, select this link and click Go. The Speed Dial and Abbreviated Dial Configuration window opens and allows you to configure the speed dial settings that will associate to this device profile.
- Add/Update Busy Lamp Field Speed Dials—To add or update the busy lamp field speed dial settings that are associated with a device profile, select this link and click Go. The Busy Lamp Field Speed Dial Configuration window opens and allows you to configure the busy lamp field speed dial settings that will associate to this device profile. See the Cisco Unified Communications Manager Features and Services Guide for configuration details of this window.
- Add/Update Busy Lamp Field Directed Call Park—To add or update the busy lamp field directed call park settings that are associated with a device profile, select this link and click Go. The Busy Lamp Field Directed Call Park Configuration window opens and allows you to configure the busy lamp field/directed call park settings that will associated to this device profile. See the *Cisco Unified Communications Manager Features and Services Guide* for configuration details of this window.
- Add/Update Service URL Buttons—To add or update the service URL buttons that are associated with a device profile, select this link and click Go. The Configure Service URL Buttons window opens and allows you to configure the service URL buttons that will associate to this device profile.

- Subscribe/Unsubscribe Services—To subscribe or unsubscribe IP phone services that are associated with a device profile, select this link and click Go. The Subscribed Cisco IP Phone Services window opens and allows you to subscribe or unsubscribe to Cisco IP Phone services that will associate to this device profile.

Related Topics

About Directory Number Setup , on page 289
Set Up Speed-dial Buttons or Abbreviated Dialing , on page 625
Set Up IP Phone Services , on page 626
Service URL Button Setup, on page 629

Device Profile Deletion

You cannot delete a device profile if it is assigned to devices. To find out which devices are using the device profile, choose Dependency Records link from the Related Links drop-down list box in the Device Profile Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. If you try to delete a device profile that is in use, Cisco Unified Communications Manager displays message. Before deleting a device profile that is currently in use, you must perform either or both of the following tasks:

- Assign a different device profile to any devices that are using the device profile that you want to delete.
- Delete the devices that are using the device profile that you want to delete.

Note If a user device profile is configured as a default logout device profile, you cannot delete it. If you want to delete a logout device profile, you must change it from a logout device profile and configure another device profile as the logout device profile for that phone. After the user device profile is no longer a logout device profile, you can delete it.

Related Topics

Access Dependency Records , on page 982

Device Profile Settings

The following table describes the available settings in the Device Profile Configuration window.

Table 105: Device Profile Settings

Field	Description
User Device Profile Information	
Product Type	This field displays the product type to which this device profile applies.
Device Protocol	This field displays the device protocol to which this device profile applies.

Field	Description
Device Profile Name	Enter a unique name. This name can comprise up to 50 characters in length.
Description	Enter a description of the device profile. For text, use anything that describes this particular user device profile.
User Hold MOH Audio Source	To specify the audio source that plays when a user initiates a hold action, choose an audio source from the User Hold MOH Audio Source drop-down list box. If you do not choose an audio source, Cisco Unified Communications Manager uses the audio source that is defined in the device pool or the system default if the device pool does not specify an audio source ID. **Note** You define audio sources in the Music On Hold Audio Source Configuration window. For access, choose **Media Resources** > **Music On Hold Audio Source**.
User Locale	From the drop-down list 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 Manager Locale Installer documentation.
Phone Button Template	From the Phone Button Template drop-down list, choose a phone button template. **Tip** If you want to configure BLF/SpeedDials for the profile for presence monitoring, choose a phone button template that you configured for BLF/SpeedDials. After you save the configuration, the Add a New BLF SD link displays in the Association Information pane. For more information on BLF/SpeedDials, see the *Cisco Unified Communications Manager Features and Services Guide*.
Softkey Template	From the Softkey Template drop-down list box, choose the softkey template from the list that displays.
Privacy	From the Privacy drop-down list box, choose On for each phone on which you want privacy. For more information, see the *Cisco Unified Communications Manager Features and Services Guide*.

Field	Description
Single Button Barge	From the drop-down list box, choose from the following options: • Off—This device does not allow users to use the Single Button Barge/cBarge feature. • Barge—Choosing this option allows users to press the Single Button Barge shared-line button on the phone to barge into a call using Barge. • Default—This device inherits the Single Button Barge/cBarge setting from the service parameter and device pool settings. **Note** If the server parameter and device pool settings are different, the device will inherit the setting from the service parameter setting. For more information, see the *Cisco Unified Communications Manager Features and Services Guide*.
Join Across Lines	From the drop-down list box, choose from the following options: • Off—This device does not allow users to use the Join Across Lines feature. • On—This device allows users to join calls across multiple lines. • Default—This device inherits the Join Across Lines setting from the service parameter and device pool settings. **Note** If the server parameter and device pool settings are different, the device will inherit the setting from the service parameter setting. For more information, see the Cisco Unified Communications Manager System Guide.
Always Use Prime Line	From the drop-down list box, choose one of the following options: • Off—When the phone is idle and receives a call on any line, the phone user answers the call from the line on which the call is received. • On—When the phone is idle (off hook) and receives a call on any line, the primary line gets chosen for the call. Calls on other lines continue to ring, and the phone user must select those other lines to answer these calls. • Default—Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter, which supports the Cisco CallManager service.

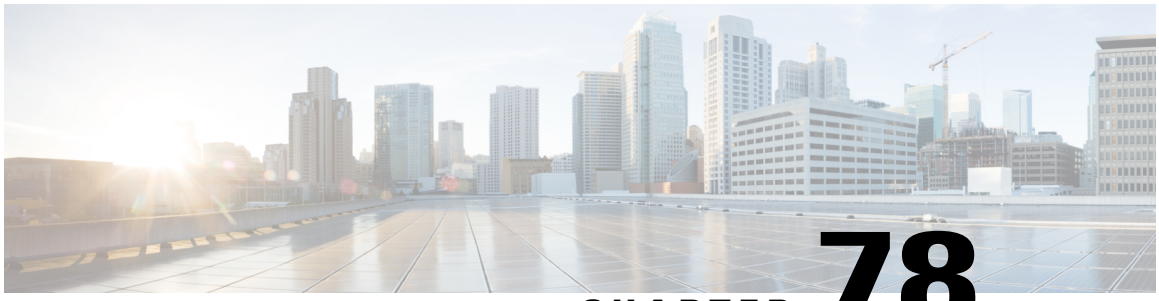
Field	Description
Always Use Prime Line for Voice Message	From the drop-down list box, choose one of the following options: • On—If the phone is idle, the primary line on the phone becomes the active line for retrieving voice messages when the phone user presses the Messages button on the phone. • Off—If the phone is idle, pressing the Messages button on the phone automatically dials the voice-messaging system from the line that has a voice message. Cisco Unified Communications Manager always selects the first line that has a voice message. If no line has a voice message, the primary line gets used when the phone user presses the Messages button. • Default—Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line for Voice Message service parameter, which supports the Cisco CallManager service.
Ignore Presentation Indicators (internal calls only)	To configure call display restrictions and ignore any presentation restriction that is received for internal calls, check the "Ignore Presentation Indicators (internal calls only)" check box. **Tip** Use this configuration in combination with the calling line ID presentation and connected line ID presentation configuration at the translation pattern level. Together, these settings allow you to configure call display restrictions to selectively present or block calling and/or connected line display information for each call. For more information about call display restrictions, see the *Cisco Unified Communications Manager Features and Services Guide*.
Do Not Disturb	Check this check box to enable Do Not Disturb.
DND Option	When you enable DND on the phone, this parameter allows you to specify how the DND feature handles incoming calls: • Call Reject—This option specifies that no incoming call information gets presented to the user. Depending on how you configure the DND Incoming Call Alert parameter, the phone may play a beep or display a flash notification of the call. • Ringer Off—This option turns off the ringer, but incoming call information gets presented to the device, so that the user can accept the call. • Use Common Phone Profile Setting—This option specifies that the DND Option setting from the Common Phone Profile window will get used for this device. **Note** For 7940/7960 phones that are running SCCP, you can only choose the Ringer Off option. For mobile devices and dual-mode phones, you can only choose the Call Reject option. When you activate DND Call Reject on a mobile device or dual-mode phone, no call information gets presented to the device.

Field	Description
DND Incoming Call Alert	When you enable the DND Ringer Off or Call Reject option, this parameter specifies how a call displays on a phone. From the drop-down list, choose one of the following options: • None—This option specifies that the DND Incoming Call Alert setting from the Common Phone Profile window will get used for this device. • Disable—This option disables both beep and flash notification of a call but for the DND Ringer Off option, incoming call information still gets displayed. For the DND Call Reject option, no call alerts display and no information gets sent to the device. • Beep Only—For an incoming call, this option causes the phone to play a beep tone only. • Flash Only—For an incoming call, this option causes the phone to display a flash alert.
Extension Mobility Cross Cluster CSS	From the drop-down list box, choose an existing Calling Search Space (CSS) to use for this device profile for the Extension Mobility Cross Cluster feature. (To configure a new CSS or modify an existing CSS, choose **Call Routing** > **Class of Control** > **Calling Search Space** in Cisco Unified Communications Manager Administration.) Default value specifies None. The home administrator specifies this CSS, which gets used as the device CSS that gets assigned to the phone when the user logs in to this remote phone. For more information, see the *Cisco Unified Communications Manager Features and Services Guide*.
Expansion Module Information	
Module 1	You can configure one or two expansion modules for this device profile by choosing phone templates from the expansion module drop-down lists in the expansion module fields. **Note** You can view a phone button list at any time by choosing the View button list link next to the phone button template fields. A separate dialog box pops up and displays the phone buttons for that particular expansion module. Choose the appropriate expansion module or None.
Module 2	Choose the appropriate expansion module or None.
Multilevel Precedence and Preemption	
MLPP Domain	If this user device profile will be used for MLPP precedence calls, choose the MLLP Domain from the drop-down list box. **Note** You define MLPP domains in the MLPP Domain Configuration window. For access, choose **System** > **MLPP Domain**.

Field	Description
MLPP Indication	If this user device profile will be used for MLPP precedence calls, assign an MLPP Indication setting to the device profile. This setting specifies whether a device that can play precedence tones will use the capability when it places an MLPP precedence call. From the drop-down list box, choose a setting to assign to this device profile from the following options: **1** Default—This device profile inherits its MLPP indication setting from the device pool of the associated device. **2** Off—This device does not handle nor process indication of an MLPP precedence call. **3** On—This device profile does handle and process indication of an MLPP precedence call. **Note** Do not configure a device profile with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful.
MLPP Preemption	If this user device profile will be used for MLPP precedence calls, assign an MLPP Preemption setting to the device profile. This setting specifies whether a device that can preempt calls in progress will use the capability when it places an MLPP precedence call. From the drop-down list box, choose a setting to assign to this device profile from the following options: **1** Default—This device profile inherits its MLPP preemption setting from the device pool of the associated device. **2** Disabled—This device does not allow preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. **3** Forceful—This device allows preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. **Note** Do not configure a device profile with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful.
Logged Out (Default) Profile Information	
Login User Id	From the Login User ID drop-down list box, choose a valid login user ID. **Note** If the device profile is used as a logout profile, specify the login user ID that will be associated with the phone. After the user logs out from this user device profile, the phone will automatically log in to this login user ID.

Related Topics

Device Profile Setup , on page 713



CHAPTER 78

Phone Button Template Setup

This chapter contains information about creating and using templates to assign a common button configuration to a large number of phones.

For example, if users in your company do not use the conference feature, you can create a template that reassigns this button to a different feature, such as speed dial. Make sure that all phones have at least one line that is assigned. Normally, use button 1 for this. You can assign additional lines to a phone, depending on the Cisco Unified IP Phone model. Phones also generally have several features, such as speed dial and call forward, that are assigned to the remaining buttons.

About Phone Button Template Setup

In Cisco Unified Communications Manager Administration, use the **Device** > **Device Settings** > **Phone Button Template** menu path to configure phone button templates.

Cisco Unified Communications Manager includes default templates for each Cisco Unified IP Phone model. When you add phones, you can assign one of these templates to the phone or create a template of your own.

You can make changes to the custom, nonstandard templates that you created, and you can change the label of the custom phone button template. You cannot change the function of the buttons in the default templates.

You can update a custom, nonstandard phone button template to add or remove features, add or remove lines and speed dials, or assign features, lines, and speed dials to different buttons on the phone. You can change the button labels in the default phone button templates, but you cannot change the function of the buttons in the default templates. If you update a phone template, be sure to inform affected users of the changes.

The Programmable Line Key (PLK) feature expands the list of features that can be assigned to the line buttons to include features that are normally controlled by softkeys; for example, New Call, Call Back, End Call, and Forward All.

If you create a template for a Cisco Unified IP Phone, you can change the default template for that phone during autoregistration.

Phone Button Template Configuration Tips

If you are creating a custom, nonstandard phone button template, see the guidelines for creating new phone button templates. See the *Cisco Unified Communications Manager System Guide*.

Cisco Unified Communications Manager includes default templates for each Cisco Unified IP Phone model. When you add phones, you can assign one of these templates to the phone or create a template of your own.

If you create a template for a Cisco Unified IP Phone, you can change the default template for that phone during auto-registration.

Note Renaming a template does not affect the phones that use that template. All Cisco Unified IP Phones that use this template continue to use this template after it is renamed. You can rename only phone button templates that display a check box in the left column. All other phone button templates serve as standard, read-only templates.

Note When you update a template, the change affects all phones that use the template. You can update only phone button templates that display a check box in the left column. All other phone button templates serve as standard, read-only templates. After you update the template, click Reset to restart devices that use the template.

Phone Button Template Deletion

You can delete phone templates that are not currently assigned to any phone in your system. You cannot delete a template that is assigned to one or more devices or device profiles or the default template for a model (which is specified in the Device Defaults Configuration window).

To find out which devices are using the phone button template, choose Dependency Records link from the Related Links drop-down list box in the Phone Button Template Configuration window and click Go. If the dependency records are not enabled for the system, the dependency records summary window displays a message. If you try to delete a phone button template that is in use, Cisco Unified Communications Manager displays a message. Before deleting a phone button template that is currently in use, you must perform either or both of the following tasks:

- Assign a different phone button template to any devices that are using the phone button template that you want to delete.
- Delete the devices that are using the phone button template that you want to delete.

Note You can delete only phone button templates that display a check box in the left column. All other phone button templates serve as standard, read-only templates.

Related Topics

Phone Deletion Preparation , on page 582
About Phone Button Template Setup , on page 721
Access Dependency Records , on page 982

Phone Button Template Settings

The following table describes the phone button template settings.

Table 106: Phone Button Template Settings

Field	Description
Phone Button Template Information	
Button Template Name	Enter a unique name that Cisco Unified Communications Manager uses to identify the template.
Button Information	
Feature	Choose the function of the phone button that you want to specify in the template. The programmable line key feature provides multiple features that can be assigned to line buttons; for example, MCID, DND, Call Park, Call Pickup, and many more. **Note** You cannot change the function of buttons in default phone button templates.
Label	Enter a description of the button.

Related Topics

Phone Button Template Setup , on page 721

Set Up Cisco Unified IP Phone Expansion Module Phone Button Template

You create a new phone button template for a Cisco Unified IP Phone Expansion Module by copying one of the Standard Cisco IP Phone phone button template, configuring the phone buttons, and saving the new phone button template.

Select a phone button template to copy by choosing the phone button template for the phone model that you are attaching the expansion module to. For example, if you are attaching an expansion module to a Cisco Unified IP Phone 9951, then you copy the Standard 9951 SIP phone button template. Use the following procedure to configure a Cisco Unified IP Phone Expansion Module.

Procedure

Step 1 Find the phone button template by using the Find and List Phone Button Templates window (**Device** > **Device Settings** > **Phone Button Template**).

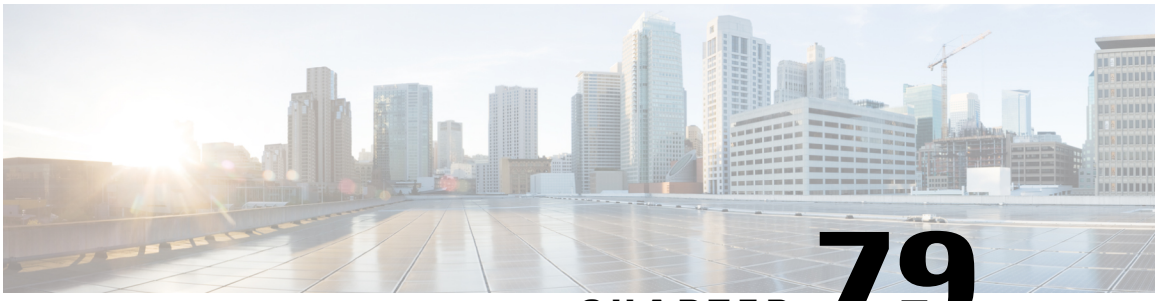
Step 2 From the list of matching records, locate the phone button template that matches the phone model that you is being attached to the phone extension module and click the Copy icon.

Step 3 For Button Template Name, enter a unique name for the phone button template (for example, Expansion Module 1).

Step 4 Click Save.

Step 5 Update the appropriate settings for Feature and Label as described in Table 106: Phone Button Template Settings , on page 723 (the button template name that you just created will already display).

Step 6 Click Save.



CHAPTER 79

Softkey Template Setup

This chapter provides details about softkey template configuration. The administrator can copy, update, or delete nonstandard softkey templates by using softkey template configuration.

About Softkey Template Setup

Softkey template configuration allows the administrator to manage softkeys that the Cisco Unified IP Phones (such as 7970) support. Cisco Unified Communications Manager supports two types of softkey templates: standard and nonstandard. Applications that support softkeys can have one or more standard softkey templates that are associated with them; for example, Cisco Unified Communications Manager has the Standard Feature and the Standard User softkey templates that are associated with it. You cannot modify standard softkey templates.

Find Softkey Template

Because you might have several softkey templates in your network, Cisco Unified Communications Manager Administration lets you locate specific softkey templates on the basis of specific criteria. Use the following procedure to locate softkey templates.

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

Procedure

Step 1 Choose **Device** > **Device Settings** > **Softkey Template**.
The Find and List Softkey Templates 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.
d) From the third drop-down list box, select whether to search for standard, non-standard, or both types of softkey templates.

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 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.

Create Nonstandard Softkey Templates

Cisco Unified Communications Manager includes standard softkey templates for call processing and applications. When creating custom, nonstandard softkey templates, copy the standard templates and make modifications as required.

Procedure

Step 1 Choose **Device** > **Device Settings** > **Softkey Template**.
The Find and List Softkey Templates window displays.

Step 2 Click Add New.
The Softkey Template Configuration window displays.

Step 3 From the drop-down list box, select a softkey template and click Copy to create a new template.
The Softkey Template Configuration window redisplays and contains the fields in which to enter a unique softkey template name and description. The window displays the applications that are associated with the softkey template that you are copying.

Step 4 In the Softkey Template Name field, enter a unique name to identify the softkey template.

Step 5 Enter a description that describes use of the template.The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).

Step 6 To designate this softkey template as the standard softkey template, click the Default Softkey Template check box.

Note If you designate a softkey template as the default softkey template, you will not be able to delete this softkey template unless you first remove the default designation.

Step 7 Click Save.
The softkey template gets copied, and the Softkey Template Configuration window redisplays.

Step 8 (Optional) If you want to, add additional application softkeys to the nonstandard softkey template.

Step 9 Configure the positions of the softkeys on the Cisco Unified IP Phone LCD screen.

Step 10 To save your configuration, click Save.

Related Topics

Add Application Softkeys to Nonstandard Softkey Templates , on page 727
Set Up Softkey Positions in Nonstandard Softkey Templates , on page 728

Add Application Softkeys to Nonstandard Softkey Templates

Cisco Unified Communications Manager includes standard softkey templates for call processing and applications. When creating custom, nonstandard softkey templates, copy the standard templates and make modifications as required. This procedure describes how to add application softkeys to a nonstandard softkey template that you created.

Procedure

Step 1 Find the softkey template.

Step 2 From the list of matching records, choose the softkey template to which you want to add application softkeys.

Note You can modify only softkey templates that display a check box in the left column. All other softkey templates are standard, read-only templates.

The Softkey Template Configuration window displays.

Step 3 To add additional application softkeys to the nonstandard softkey template, click the Add Application button.
The Add Application window displays.

Step 4 Choose the standard softkey template that you want added to the nonstandard softkey template.

Step 5 Click Save and click Close.
The softkeys that are associated with the standard softkey template that you chose get added at the end of the nonstandard softkey template. Duplicate softkeys automatically get deleted. If the number of softkeys for a particular call state exceeds 16, the optional softkeys for that call state will be removed (from the end to the front). If after the optional softkeys are removed, the number of softkeys still exceeds 16, a message displays.

Step 6 To save your softkey set configuration, click Save.

Step 7 To make the updates of the softkey template take effect and synchronize the softkey template configuration with the phone, click Apply Config.

Related Topics

Softkey Template Setup , on page 725
Find Softkey Template , on page 725
Synchronize Softkey Template Settings with Devices , on page 731

Set Up Softkey Positions in Nonstandard Softkey Templates

Cisco Unified Communications Manager includes standard softkey templates for call processing and applications. When creating custom, nonstandard softkey templates, copy the standard templates and make modifications as required. This procedure describes how to configure softkey positions for each call state in a nonstandard softkey template that you created.

Procedure

Step 1 Find the softkey template by using the procedure in the Find Softkey Template , on page 725.

Step 2 From the list of matching records, choose the softkey template in which you want to configure softkey positions.

Note You can modify only softkey templates that display a check box in the left column. All other softkey templates are standard, read-only templates.

The Softkey Template Configuration window displays.

Step 3 To configure the positions of the softkeys on the Cisco Unified IP Phone LCD screen, choose Configure Softkey Layout from the Related Links drop-down list box; then, click Go.
The Softkey Layout Configuration window displays. The Select a call state to configure drop-down list box lists each Cisco Unified Communications Manager call state for an IP phone.

Step 4 To configure the softkey positions for a call state, choose the call state from the Select a call state to configure drop-down list box.
The Softkey Layout Configuration window redisplays, and the Unselected Softkeys pane and Selected Softkeys pane display softkeys that are applicable to the call state that you chose.

Tip To create a relative place holder for a softkey, add the Undefined softkey. This allows the softkey that you added to occupy the same softkey position in all call states.

Step 5 To move softkeys from one list to the other, use the right and left arrows between the panes.

Step 6 To rearrange the positions of the Selected Softkeys, use the up and down arrows to the right of the Selected Softkeys pane.

Step 7 To save your softkey layout configuration, click Save.

Step 8 To return to the Softkey Template Configuration window, choose the Softkey Template Configuration link from the Related Links drop-down list box in the top, right-hand corner; then, click Go.

Step 9 To save your configuration, click Save.

Step 10 To make the updates of the softkey template take effect and synchronize the softkey template configuration with the phone, click Apply Config.

Related Topics

Softkey Template Setup , on page 725
Synchronize Softkey Template Settings with Devices , on page 731

Softkey Template Modification

You can make changes to custom, nonstandard softkey templates that you created.

Related Topics

Rename Softkey Template , on page 729
Delete Softkey Template , on page 730
Update Softkey Template , on page 731
Synchronize Softkey Template Settings with Devices , on page 731

Rename Softkey Template

Use this procedure to rename a nonstandard softkey template that you created.

Procedure

Step 1 Find the softkey template.

Step 2 From the list of matching records, choose the softkey template that you want to rename.

Note You can rename only softkey templates that display a check box in the left column. All other softkey templates are standard, read-only templates.

The Softkey Template Configuration page displays.

Step 3 In the Softkey Template Name field, enter the new name.

Step 4 Click Save.

The Softkey Template Configuration window redisplays with the new softkey template name.

Related Topics

Find Softkey Template , on page 725

Delete Softkey Template

Use this procedure to delete a nonstandard softkey template that you created.

Before You Begin

You cannot delete a nonstandard softkey template that is currently assigned to a device or device pool. To find out which devices and device pools are using the nonstandard softkey template, choose Dependency Records from the Related Links drop-down list box in the Softkey Configuration window and click Go. If the dependency records are not enabled for the system, the dependency records summary window displays a message. If you try to delete a nonstandard softkey template that is in use, Cisco Unified Communications Manager displays a message. Before deleting a nonstandard softkey template that is currently in use, you must perform either or both of the following tasks:

- Assign a different softkey template to any devices or device pools that are using the nonstandard softkey template that you want to delete.
- Delete the devices that are using the nonstandard softkey template that you want to delete.

Procedure

Step 1 Find the softkey template.

Step 2 From the list of matching records, choose the softkey template that you want to delete.

Note You can delete only softkey templates that display a check box in the left column. All other softkey templates represent standard, read-only templates.

The Softkey Template Configuration window displays.

Step 3 Click Delete.

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

A message verifies that you want to delete the template.

Step 4 Click OK.

The Softkey Template Configuration window redisplays with the softkey template deleted.

Related Topics

Phone Deletion Preparation , on page 582
Find Softkey Template , on page 725
IP Phone Softkey Template Assignment , on page 732
Access Dependency Records , on page 982

Update Softkey Template

Use this procedure to update a nonstandard softkey template that you created. You can update the template name, description, application softkeys that are supported, and the softkey layout.

Procedure

Step 1 Find the softkey template.

Step 2 From the list of matching records, choose the softkey template that you want to update.

Note You can update only softkey templates that display a check box in the left column. All other softkey templates represent standard, read-only templates.

The Softkey Template Configuration window displays.

Step 3 Update the settings that you want changed (such as adding an application softkey set or the softkey layout).

Step 4 Click Save.

The Softkey Template Configuration window redisplays with the softkey template updated.

Step 5 To apply the updated softkey template and synchronize the softkey template configuration with affected devices, click Apply Config.

Related Topics

Softkey Template Setup , on page 725
Find Softkey Template , on page 725
Add Application Softkeys to Nonstandard Softkey Templates , on page 727
Set Up Softkey Positions in Nonstandard Softkey Templates , on page 728
Synchronize Softkey Template Settings with Devices , on page 731

Synchronize Softkey Template Settings with Devices

To synchronize devices with a softkey template configuration that has undergone configuration changes, perform the following procedure, which applies 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 **Device** > **Device Settings** > **Softkey Template**.

The Find and List Softkey Templates window displays.

Step 2 Choose the search criteria to use.

Step 3 Click Find.

The window displays a list of softkey templates that match the search criteria.

Step 4 Click the softkey template to which you want to synchronize applicable devices. The Softkey Template 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.

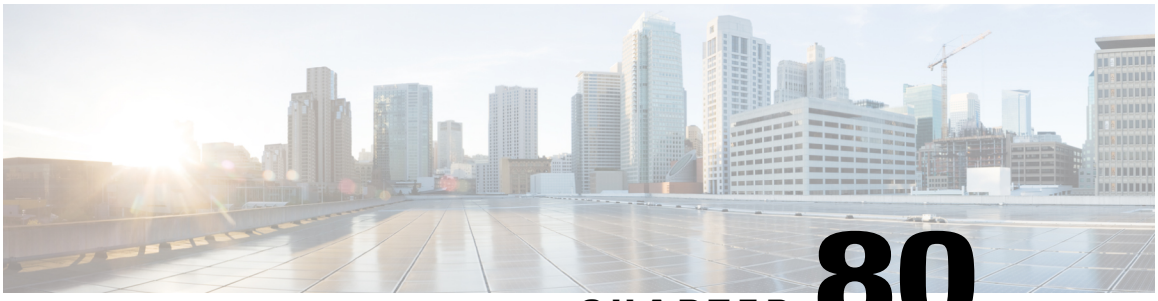
IP Phone Softkey Template Assignment

You can assign softkey templates to IP phones when the phones are configured. You can assign standard and nonstandard softkey templates. Two ways to assign a softkey template to a phone exist:

- Assign the softkey template to a common device configuration and then assign the common device configuration to the phone in the Phone Configuration window.
- Assign the softkey template to the phone in the Softkey Template field in the Phone Configuration window.

Related Topics

Set Up Cisco Unified IP Phone , on page 620
About Common Device Setup , on page 763



CHAPTER 80

IP Phone Services Setup

This chapter provides information to configure IP phone services.

About IP Phone Service Setup

In Cisco Unified Communications Manager Administration, use the **Device** > **Device Settings** > **Phone Services** menu path to configure IP phone services.

Using Cisco Unified Communications Manager Administration, you define and maintain the list of IP phone services that can display on supported Cisco Unified IP Phones models. IP phone services comprise XML applications or Cisco-signed Java MIDlets that enable the display of interactive content with text and graphics on some Cisco Unified IP Phones models.

Cisco Unified Communications Manager provides Cisco-provided default IP phone services, which install automatically with Cisco Unified Communications Manager. You can also create customized Cisco Unified IP Phone applications for your site.

After you configure the services, you can add services to the phones in the database, that is, if they are not classified as enterprise subscriptions, and you can assign the services to the Services, Directory, or Messages buttons/options, if the phone model supports these buttons/options.

Users can log in to Cisco Unified Communications Self Care Portal and subscribe to these services for their Cisco Unified IP Phones; that is, if these IP phone services are not classified as enterprise subscriptions.

IP Phone Services Configuration Tips

Caution Do not put IP phone services on any Cisco Unified Communications Manager server at your site or any server that is associated with Cisco Unified Communications Manager, such as the TFTP server or publisher database server. This precaution eliminates the possibility that errors in an IP phone service application will have an impact on Cisco Unified Communications Manager performance or interrupt call-processing services.

If the service was modified after subscriptions existed, click Update Subscriptions to rebuild all user subscriptions. You must update subscriptions if you changed the service URL, removed a phone service parameter, or changed the Parameter Name for a phone service parameter.

Note If you change the service URL, remove an IP phone service parameter, or change the name of a phone service parameter for an IP phone service to which users are subscribed, be sure to click Update Subscriptions to update all currently subscribed users with the changes. If you do not do so, users must resubscribe to the service to rebuild the URL correctly.

Note Cisco Unified Communications Manager allows you to create two or more IP phone services with identical names. Cisco recommends that you do not do so unless most or all phone users are advanced, or unless an administrator always configures the IP phone services. Be aware that if AXL or any third-party tool accesses the list of IP phone services for configuration, you must use unique names for IP phone services.

Next Steps After Configuring an IP Phone Service

Configure the Services Provisioning setting, which displays in the Phone Configuration window, Common Phone Profile Configuration window, or Enterprise Parameter Configuration window.

IP Phone Service Deletion

Tip Cisco strongly recommends that you disable IP phone services, instead of deleting these services from Cisco Unified Communications Manager Administration. Disabling the IP phone service does not remove the service from the database, but it does ensure that the service does not display on the phone. Deleting the service removes the service from the database. You disable an IP phone service in the IP Phone Services Configuration window (**Device** > **Device Settings** > **Phone Services**) for the service that you want to disable.

When you delete an IP phone service, Cisco Unified Communications Manager removes all service information, user subscriptions, and user subscription data from the database. To find out which devices are using the IP phone service, from the IP phone service Configuration window, choose Dependency Records from the Related Records drop-down list box and click Go. If the dependency records are not enabled for the system, the dependency records summary window displays a message. If you try to delete an IP phone service that is in use, Cisco Unified Communications Manager displays a message. Before deleting an IP phone service that is currently in use, you must perform either or both of the following tasks:

- Assign a different IP phone service to any devices that are using the IP phone service that you want to delete.
- Delete the devices that are using the IP phone service that you want to delete.

Related Topics

Phone Deletion Preparation , on page 582
About IP Phone Service Setup , on page 733
Access Dependency Records , on page 982

IP Phone Service Settings

The following table describes the IP phone service settings that display in the IP Phone Services Configuration window in Cisco Unified Communications Manager Administration.

Table 107: IP Phone Service Settings

Field	Description
Service Information	
Service Name	Enter the name of the service. If the service is not marked as an enterprise subscription, the service name will display in areas where you can subscribe to a service; for example, under Cisco Unified Communications Self Care Portal. Enter up to 128 characters for the service name. For Java MIDlet services, the service name must exactly match the name that is defined in the Java Application Descriptor (JAD) file. **Note** Cisco Unified Communications Manager allows you to create two or more IP phone services with identical names. Cisco recommends that you do not do so unless most or all phone users are advanced, or unless an administrator always configures the IP phone services. Be aware that if AXL or any third-party tool accesses the list of IP phone services for configuration, you must use unique names for IP phone services. **Note** When the service URL points to an external customized URL, you cannot localize the service name as per the device locale of the phone. The service name gets displayed in English alphabets only.
ASCII Service Name	Enter the name of the service to display if the phone cannot display Unicode.
Service Description	Enter a description of the content that the service provides. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), or single-quotes (').

Field	Description
Service URL	Enter the URL of the server where the IP phone services application is located. Make sure that this server remains independent of the servers in your Cisco Unified Communications Manager cluster. Do not specify a Cisco Unified Communications Manager server or any server that is associated with Cisco Unified Communications Manager (such as a TFTP server or directory database publisher server). For the services to be available, the phones in the Cisco Unified Communications Manager cluster must have network connectivity to the server. For Cisco-signed Java MIDlets, enter the location where the JAD file can be downloaded; for example, a web server or the backend application server to which the Java MIDlet communicates. For Cisco-provided default services, the service URL displays as `Application:Cisco/<name of service>` by default; for example, Application:Cisco/CorporateDirectory. If you modify the service URL for Cisco-provided default services, verify that you configured Both for the Service Provisioning setting, which displays in the Phone, Enterprise Parameter, and Common Phone Profile Configuration windows. For example, you use a custom corporate directory, so you change `Application:Cisco/CorporateDirectory` to the external service URL for your custom directory; in this case, change the Service Provisioning setting to Both.
Secure-Service URL	Enter the secure URL of the server where the Cisco Unified IP Phone services application is located. Make sure that this server remains independent of the servers in your Cisco Unified Communications Manager cluster. Do not specify a Cisco Unified Communications Manager server or any server that is associated with Cisco Unified Communications Manager (such as a TFTP server or publisher database server). For the services to be available, the phones in the Cisco Unified Communications Manager cluster must have network connectivity to the server. **Note** If you do not provide a Secure-Service URL, the device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, the device chooses the appropriate URL, based on its capabilities.
Service Category	Select a service application type (XML or Java MIDlet). If you choose Java MIDlet, when the phone receives the updated configuration file, the phone retrieves the Cisco-signed MIDlet application (JAD and JAR) from the specified Service URL and installs the application.
Service Type	Choose whether the service is provisioned to the Services, Directories, or Messages button/option on the phone; that is, if the phone has these buttons/options. To determine whether your phone these buttons/options, see the *Cisco Unified IP Phone Administration Guide* that supports your phone model.

Field	Description
Service Vendor	This field allows you to specify the vendor/manufacturer for the service. This field is optional for XML applications, but it is required for Cisco-signed Java MIDlets. For Cisco-signed Java MIDlets, the value that you enter in this field must exactly match the vendor that is defined in the MIDlet JAD file. This field displays as blank for Cisco-provided default services. You can enter up to 64 characters.
Service Version	Enter the version number for the application. For XML applications, this field is optional and is informational only. For Cisco-signed Java MIDlets, consider the following information: • If you enter a version, the service version must exactly match the version that is defined in the JAD file. If you enter a version, the phone attempts to upgrade or downgrade the MIDlet if the version is different than what is installed on the phone. • If the field is blank, the version gets retrieved from the Service URL. Leaving the field blank ensures that the phone attempts to download the JAD file every time that the phone reregisters to Cisco Unified Communications Manager as well as every time that the Cisco-signed Java MIDlet is launched; this ensures that the phone always runs the latest version of the Cisco-signed Java MIDlet without you having to manually update the Service Version field. This field displays as blank for Cisco-provided default services. You can enter numbers and periods in this field (up to 16 ASCII characters).
Enable	This check box allows you to enable or disable the service without removing the configuration from Cisco Unified Communications Manager Administration (and without removing the service from the database). Unchecking the check box removes the service from the phone configuration file and the phone.
Enterprise Subscription	This check box allows you to automatically provision the service to all devices in the cluster that can support the service. If you check this check box, you (or an end user) cannot subscribe to the service. If this check box is unchecked, you must manually subscribe to the service for it to display on the phone (either in the Phone Configuration window, in BAT, or in the Cisco Unified Communications Self Care Portal). **Tip** This setting displays only when you configure a service for the first time. After you save the service, the check box does not display in the window. To identify whether the service is provisioned to all devices in the cluster that can support the service, go to the Find and List IP Phone Services window and display the services. If true displays in the Enterprise Subscription column, you cannot manually subscribe to the service. If false displays, you can manually subscribe to the service; for example, an end user can subscribe to the service through the Cisco Unified Communications Self Care Portal.

Field	Description
Service Parameter Information	
Parameters	This pane lists the service parameters that apply to this IP phone service. Use the following buttons to configure service parameters for this pane: • New Parameter—Click this button to display the Configure Cisco Unified IP Phone Service Parameter window, where you configure a new service parameter for this IP phone service. • Edit Parameter—Highlight a service parameter that displays in the Parameters pane, then click this button to display the Configure Cisco Unified IP Phone Service Parameter window, where you can edit the selected service parameter for this IP phone service. • Delete Parameter—Highlight a service parameter that displays in the Parameters pane, then click this button to delete a service parameter for this IP phone service. A popup window asks you to confirm deletion.

Related Topics

IP Phone Services Setup , on page 733
IP Phone Service Parameter Settings , on page 738

IP Phone Service Parameter Settings

Add the IP phone service before you configure IP phone service parameters. See the documentation for the individual IP phone service for specific information about whether the service uses parameters, how those parameters should be configured, and whether you should provide optional parameter definitions.

Tip If you remove an IP phone service parameter or change the parameter name of an IP phone service for an IP phone service to which users are subscribed, be sure to click Update Subscriptions to update all currently subscribed users with the changes. If you do not do so, users must resubscribe to the service to rebuild the URL correctly.

When you subscribe devices to the IP phone 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. Click Update Subscriptions only once and wait for this propagation to complete.

The following table describes the IP phone service parameter settings.

Table 108: IP Phone Service Parameter Settings

Field	Description
Service Parameter Information	

Field	Description
Parameter Name	Enter the exact query string parameter to use when you build the subscription URL; for example, symbol.
Parameter Display Name	Enter a descriptive parameter name to display to the user in Cisco Unified Communications Self Care Portal; for example, Ticker Symbol.
Default Value	Enter the default value for the parameter. This value displays to the user when a service is being subscribed to for the first time; for example, CSCO.
Parameter Description	Enter a description of the parameter. The user can access the text that is entered here while the user is subscribing to the service. The parameter description should provide information or examples to help users input the correct value for the parameter. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), or angle brackets (<>).
Parameter is Required	If the user must enter data for this parameter before the subscription can be saved, check the Parameter is Required check box.
Parameter is a Password (mask contents)	You can mask entries in Cisco Unified Communications Self Care Portal, so asterisks display rather than the actual user entry. You may want to do this for parameters such as passwords that you do not want others to be able to view. To mask parameter entry, check the Parameter is a Password (mask contents) check box in the Configure IP Phone Service Parameter window in Cisco Unified Communications Manager Administration.

Cisco-Provided Default IP Phone Services

The following table displays the Cisco-provided default IP phone services that display if you specify the search parameter, IP Phone Service, and then click Find. Cisco Unified Communications Manager automatically provisions the Cisco-provided default services listed in the table.

To update these services, click the link in the Find and List IP Phone Service window. You can change the name of the service, where the default service displays on the phone, and the service URL. If you change the service URL for the default services, choose Both from the Service Provisioning drop-down list box, which displays in the Phone Configuration window, the Enterprise Parameter Configuration window, and the Common Phone Profile Configuration window.

Tip Some Cisco Unified IP Phone models do not support IP phone services. To determine the support for your phone model, see the Cisco Unified IP Phone Administration Guide.

Table 109: Cisco-Provided Default Services

Default Services	Description
Corporate Directory	This XML service allows the phone to display the corporate directory on the phone. By default, for phones with a Directory button/option, the corporate directory option displays when a user presses the Directory button/option on the phone. By default, the service URL is Application:Cisco/CorporateDirectory. By default, the corporate directory automatically displays on all phones that support services in the cluster, and you (or the end user) cannot subscribe to the service. If you update the corporate directory option because you want to configure this option to support a custom directory, for example, you update the Service URL to point to your custom directory, make sure that Both is chosen from the Service Provisioning drop-down list box, which displays in the Phone Configuration window, Enterprise Parameter Configuration window, or the Common Phone Profile Configuration window.
Intercom Calls	This XML service allows the phone to display the history records for intercom calls. By default, for phones with a Directory button/option, the intercom history option displays when a user presses the Directory button/option on the phone. By default, the service URL is Application:Cisco/IntercomCalls. This service does not automatically display on all phones that support services in the cluster; therefore, you must manually subscribe to the service; for example, you can subscribe to the service in the Cisco Unified Communications Self Care Portal.
Missed Calls	This XML service allows the phone to display missed calls on the phone. By default, for phones with a Directory button/option, the missed calls option displays when a user presses the Directory button/option on the phone. By default, the service URL is Application:Cisco/MissedCalls. By default, the Missed Calls option automatically displays on all phones that support services in the cluster, and you (or the end user) cannot subscribe to the service.
Personal Directory	This XML service allows a phone user to use Personal Directory. By default, for phones with a Directory button/option, the Personal Directory option displays when a user presses the Directory button/option on the phone. By default, the service URL is Application:Cisco/PersonalDirectory. By default, the Personal Directory option automatically displays on all phones that support services in the cluster, and you (or the end user) cannot subscribe to the service.
Placed Calls	This XML service allows the phone to display calls that the user has placed on the phone. By default, for phones with a Directory button/option, the placed calls option displays when a user presses the Directory button/option on the phone. By default, the service URL is Application:Cisco/PlacedCalls. By default, the Placed Calls option automatically displays on all phones that support services in the cluster, and you (or the end user) cannot subscribe to the service.

Default Services	Description
Received Calls	This XML service allows the phone to display received calls on the phone. By default, for phones with a Directory button/option, the received calls option displays when a user presses the Directory button/option on the phone. By default, the service URL is Application:Cisco/ReceivedCalls. By default, the Received Calls option automatically displays on all phones that support services in the cluster, and you (or the end user) cannot subscribe to the service.
Voicemail	This XML service allows users to retrieve voice messages on the phone. By default, for phones with a Messages button/option, the voice mail option displays when a user presses the Messages button/option on the phone. By default, the service URL is Application:Cisco/Voicemail. By default, the Voicemail option automatically displays on all phones that support services in the cluster, and you (or the end user) cannot subscribe to the service.

Related Topics

IP Phone Services Setup , on page 733

Set Up IP Phone Service Parameters

Use the following procedure to add and configure or update IP phone service parameters. Add the IP phone service before you configure parameters. See the documentation for the individual IP phone service for specific information about whether the service uses parameters, how those parameters should be configured, and whether you should provide optional parameter definitions.

Procedure

Step 1 Find the IP phone service.

Step 2 From the IP phone services list, choose the service to which you want to add parameters or update existing parameters.
The IP Phone Services Configuration window displays.

Step 3 Perform one of the followings tasks:

a) To add a new IP phone service parameter, click the New button to the right of the Parameters list box. The Configure IP Phone Service Parameter window displays. Continue with Step 4, on page 741.

b) To update an existing parameter, choose the name of the parameter that you want to update in the Parameters list box. Click Edit and continue with Step 4, on page 741.

Step 4 Enter the appropriate settings as described in Table 108: IP Phone Service Parameter Settings , on page 738. To add the new parameter, click Save. To add additional parameters, if needed, click Add New in the Configure IP Phone Service Parameter window and repeat Step 3, on page 741 and Step 4, on page 741.To add the last parameter, click Save and Close.

To apply the changes to the updated parameters, click Save, or to apply the changes and close the window, click Save and Close.

Step 5 To apply the changes, update the IP Phone Services Configuration window:

a) If the service was modified after subscriptions existed, click Update Subscriptions to rebuild all user subscriptions. You must update subscriptions if you changed the service URL, removed an IP phone service parameter, or changed the name for an IP phone service parameter.

Note If you remove an IP phone service parameter or change the parameter name of an IP phone service for an IP phone service to which users are subscribed, be sure to click Update Subscriptions to update all currently subscribed users with the changes. If you do not do so, users must resubscribe to the service to rebuild the URL correctly.

Note When you subscribe devices to the IP phone 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. Click Update Subscriptions only once and wait for this propagation to complete.

b) If the service is new and you do not need to rebuild user subscriptions, click Save.

Related Topics

IP Phone Services Setup , on page 733

IP Phone Service Parameter Deletion

Perform the following steps to delete an IP phone service parameter.

Note If you remove an IP phone service parameter or modify the Parameter Name of an IP phone service parameter for an IP phone service to which users are subscribed, you must click Update Subscriptions to update all currently subscribed users with the changes. If you do not do so, users must resubscribe to the service to rebuild the URL correctly.

Procedure

Step 1 Find the IP phone service by using Find and List IP Phone Services window (**Device** > **Device Settings** > **Phone Services** Phone Services).

Step 2 From the IP phone services list, choose the IP phone service whose parameters you want to delete.

Step 3 In the Parameters list box, choose the name of the parameter that you want to delete.

Step 4 Click Delete Parameter.
You receive a message that asks you to confirm the deletion.

Step 5 To confirm the deletion, click OK.

Step 6 To apply the changes, update the IP phone services configuration window:

a) If the service was modified after subscriptions existed, click Update Subscriptions to rebuild all user subscriptions. You must update subscriptions if you changed the service URL, removed an IP phone service parameter, or changed the Parameter Name for an IP phone service parameter.
If you click Update Subscriptions more than once, an error occurs. 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.

b) If the service is new and you do not need to rebuild user subscriptions, click Save.

Related Topics

IP Phone Services Setup , on page 733

Add IP Phone Services to Phone Buttons

If you want to do so, you can assign the service to a phone button (a speed dial button) that is configured as a service URL.

By default, the IP phone service can display under the Directory, Message, or Services button/options on the phone, depending on your configuration in the IP Phone Services Configuration window, so you only need to add an IP phone service to a phone button if you want the service to display as a speed dial.

You can only perform this procedure for IP phone services that are not marked as enterprise subscriptions. Perform the following steps to add a service to a service URL button.

Procedure

Step 1 Add the service to Cisco Unified Communications Manager.

Step 2 Customize a phone button template by configuring a Service URL button.

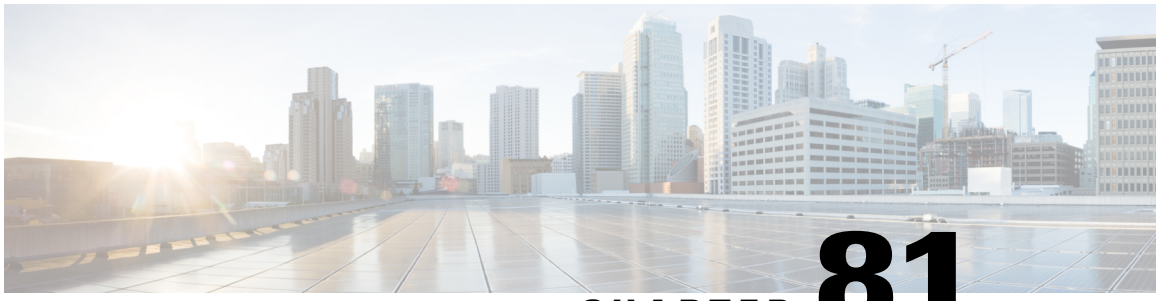
Step 3 Add the customized phone button template to the phone.

Step 4 Subscribe the service to the phone.

Step 5 Add the service URL to a phone button.

Related Topics

Set Up IP Phone Services , on page 626
Service URL Button Setup, on page 629
About Phone Button Template Setup , on page 721
IP Phone Services Setup , on page 733
About IP Phone Service Setup , on page 733



CHAPTER 81

SIP Profile Setup

This chapter provides information to configure and locate SIP profiles. A SIP profile comprises the set of SIP attributes that are associated with SIP trunks and SIP endpoints. SIP profiles include information such as name, description, timing, retry, call pickup URI, and so on. The profiles contain some standard entries that cannot be deleted or changed.

About SIP Profile Setup

A SIP profile comprises the set of SIP attributes that are associated with SIP trunks and SIP endpoints. SIP profiles include information such as name, description, timing, retry, call pickup URI, and so on. The profiles contain some standard entries that cannot be deleted or changed.

SIP Profile Reset

For instructions on how to reset a SIP profile, see the descriptions of the Reset Selected and Reset buttons in the *Cisco Unified Communications Manager System Guide*.

Related Topics

Synchronize SIP Profile Settings with SIP Devices , on page 762

SIP Profile Deletion

To find out which devices are using the SIP profile, choose Dependency Records link from the Related Links drop-down list box in the SIP Profile 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 System Guide*.

SIP Profile Settings

The following table describes the available settings in the SIP Profile Configuration window.

Table 110: SIP Profile Settings

Field	Description
SIP Profile Information	
Name	Enter a name to identify the SIP profile; for example, SIP_7905. The value can include 1 to 50 characters, including alphanumeric characters, dot, dash, and underscores.
Description	This field identifies the purpose of the SIP profile; for example, SIP for 7970. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
Default MTP Telephony Event Payload Type	This field specifies the default payload type for RFC2833 telephony event. See RFC 2833 for more information. In most cases, the default value specifies the appropriate payload type. Be sure that you have a firm understanding of this parameter before changing it, as changes could result in DTMF tones not being received or generated. The default value specifies 101 with range from 96 to 127. The value of this parameter affects calls with the following conditions: • The call is an outgoing SIP call from Cisco Unified Communications Manager. • For the calling SIP trunk, the Media Termination Point Required check box is checked on the SIP Trunk Configuration window.
Resource Priority Namespace List	Select a configured Resource Priority Namespace list from the drop-down menu. Configure the lists in the Resource Priority Namespace List menu that is accessed from **System** > **MLPP** > **Namespace**.

Field	Description
Early Offer for G.Clear Calls	The Early Offer for G.Clear Calls feature supports both standards-based G.Clear (CLEARMODE) and proprietary Cisco Session Description Protocols (SDP). To enable or disable Early Offer for G.Clear Calls, choose one of the following options: • Disabled • CLEARMODE • CCD • G.nX64 • X-CCD
SDP Session-level Bandwidth Modifier for Early Offer and Re-invites	The Session Level Bandwidth Modifier specifies the maximum amount of bandwidth needed when all the media streams are used. There are three Session Level Bandwidth Modifiers: Transport Independent Application Specific (TIAS), Application Specific (AS), and Conference Total (CT). Select one of the following options to specify which Session Level Bandwidth Modifier to include in the SDP portion of SIP Early Offer or Reinvite requests. • TIAS and AS • TIAS only • AS only • CT only
User-Agent and Server header information	This feature indicates how Unified Communications Manager handles the User-Agent and Server header information in a SIP message. Choose one of the following three options: • Send Unified Communications Manager Version Information as User-Agent Header—For INVITE requests, the User-Agent header is included with the CM version header information. For responses, the Server header is omitted. Unified Communications Manager passes through any contact headers untouched. This is the default behavior. • Pass Through Received Information as Contact Header Parameters —If this option is selected, the User-Agent/Server header information is passed as Contact header parameters. The User-Agent/Server header is derived from the received Contact header parameters, if present. Otherwise, they are taken from the received User-Agent/Server headers. • Pass Through Received Information as User-Agent and Server Header—If this option is selected, the User-Agent/Server header information is passed as User-Agent/Server headers. The User-Agent/Server header is derived from the received Contact header parameters, if present. Otherwise, they are taken from the received User-Agent/Server headers.

Field	Description
Accept Audio Codec Perferences in Received Offer	Select **On** to enable Cisco Unified Communications Manager to honor the preference of audio codecs in received offer and preserve it while processing. Select **Off** to enable CUCM to ignore the preference of audio codecs in received offer and apply the locally configured Audio Codec Preference List. The default will select the service parameter configuration.
Confidential Access Level Headers	This field determines the inclusion of Confidential Access Level headers in INVITE and 200 OK messages. Valid values are as follows: • Disabled—CAL headers are not included. • Preferred— CAL headers are included and confidential-access-level tag is added in the Supported header. • Required— CAL headers are included and confidential-access-level tag is added in the Require and Proxy-Require headers.
Confidential Access Level Headers	This field determines the inclusion of Confidential Access Level headers in INVITE and 200 OK messages. Valid values are as follows: • Disabled—CAL headers are not included. • Preferred— CAL headers are included and confidential-access-level tag is added in the Supported header. • Required— CAL headers are included and confidential-access-level tag is added in the Require and Proxy-Require headers.
SDP Transparency Profile	Displays the SDP Transparency Profile setting (read only)
Redirect by Application	Checking this check box and configuring this SIP Profile on the SIP trunk allows the Cisco Unified Communications Manager administrator to: • Apply a specific calling search space to redirected contacts that are received in the 3xx response. • Apply digit analysis to the redirected contacts to make sure that the call get routed correctly. • Prevent DOS attack by limiting the number of redirection (recursive redirection) that a service parameter can set. • Allow other features to be invoked while the redirection is taking place. Getting redirected to a restricted phone number (such as an international number) means that handling redirection at the stack level causes the call to be routed instead of being blocked. This behavior occurs if the Redirect by Application check box is unchecked.

Field	Description
Disable Early Media on 180	By default, Cisco Unified Communications Manager signals the calling phone to play local ringback if SDP is not received in the 180 or 183 response. If SDP is included in the 180 or 183 response, instead of playing ringback locally, Cisco Unified Communications Manager connects media, and the calling phone plays whatever the called device is sending (such as ringback or busy signal). If you do not receive ringback, the device to which you are connecting may be including SDP in the 180 response, but it is not sending any media before the 200OK response. In this case, check this check box to play local ringback on the calling phone and connect the media upon receipt of the 200OK response **Note** Even though the phone that is receiving ringback is the calling phone, you need the configuration on the called device profile because it determines the behavior.
Outgoing T.38 INVITE Include Audio mline	The parameter allows the system to accept a signal from Microsoft Exchange that causes it to switch the call from audio to T.38 fax. To use this feature, you must also configure a SIP trunk with this SIP profile. For more information, see Chapter 68, Trunk "Configuration." **Note** The parameter applies to SIP trunks only, not phones that are running SIP or other endpoints.
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 MTP 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 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.

Field	Description
Require SDP Inactive Exchange for Mid-Call Media Change	This feature designates how Cisco Unified Communications Manager handles mid-call updates to codecs or connection information such as IP address or port numbers. If the box is checked, during mid-call codec or connection updates Cisco Unified Communications Manager sends an INVITE a=inactive SDP message to the endpoint to break the media exchange. This is required if an endpoint is not capable of reacting to changes in the codec or connection information without disconnecting the media. This applies only to audio and video streams within SIP-SIP calls. **Note** For early offer enabled SIP trunks, this parameter will be overridden by the Send send-receive SDP in mid-call INVITE parameter. If the box is unchecked, Cisco Unified Communications Manager passes the mid-call SDP to the peer leg without sending a prior Inactive SDP to break the media exchange. This is the default behavior.
Use Fully Qualified Domain Name in SIP Requests	This feature enables Cisco Unified Communications Manager to relay an alphanumeric hostname of a caller by passing it through to the called device or outbound trunk as a part of the SIP header information. • If the box is unchecked, the IP address for Cisco Unified Communications Manager will be passed to the line device or outbound trunk instead of the user's hostname. This is the default behavior. • If the box is checked, Cisco Unified Communications Manager will relay an alphanumeric hostname of a caller by passing it through to the called endpoint as a part of the SIP header information. This enables the called endpoint to return the call using the received or missed call list. If the call is originating from a line device on the Cisco Unified Communications Manager cluster, and is being routed on a SIP trunk then the configured Organizational Top-Level Domain (e.g., cisco.com) will be used in the Identity headers, such as From, Remote-Party-ID, and P-Asserted-ID. If the call is originating from a trunk on Cisco Unified Communications Manager and is being routed on a SIP trunk then: ◦ If the inbound call provides a host or domain in the caller's information, the outbound SIP trunk messaging will preserve the hostname in the Identity headers, such as From, Remote-Party-ID, and P-Asserted-ID ◦ If the inbound call does not provide a host or domain in the caller's information, the configured Organizational Top-Level Domain will be used in the Identity headers, such as From, Remote-Party-ID, and P-Asserted-ID
Assured Services SIP conformance	This checkbox should be checked for third-party AS-SIP endpoints as well as AS-SIP trunks to ensure proper Assured Service behavior. This setting provides specific Assured Service behavior that affects services such as Conference factory and SRTP.

Field	Description
Parameters used in Phone	
Timer Invite Expires (seconds)	This field specifies the time, in seconds, after which a SIP INVITE expires. The Expires header uses this value. Valid values include any positive number; 180 specifies the default.
Timer Register Delta (seconds)	This field is intended to be used by SIP endpoints only. The endpoint receives this value via a tftp config file. The end point reregisters Timer Register Delta seconds before the registration period ends. The registration period gets determined by the value of the SIP Station KeepAlive Interval service parameter. Valid values for Timer Register Delta range from 32767 to 0. The default value is 5.
Timer Register Expires (seconds)	This field is intended to be used by SIP endpoints only. The SIP endpoint receives the value via a tftp config file. This field specifies the value that the phone that is running SIP sends in the Expires header of the REGISTER message. Valid values include any positive number; however, 3600 (1 hour) specifies the default value. If the endpoint sends a shorter Expires value than the value of the SIP Station Keepalive Interval service parameter, Cisco Unified Communications Manager responds with a 423 "Interval Too Brief". If the endpoint sends an Expires value that is greater than the SIP Station Keepalive Interval service parameter value, Cisco Unified Communications Manager responds with a 200 OK that includes the Keepalive Interval value for Expires. **Note** For mobile phones that are running SIP, Cisco Unified Communications Manager uses the value in this field instead of the value that the SIP Station KeepAlive Interval service parameter specifies to determine the registration period. **Note** For TCP connections, the value for the Timer Register Expires field must be lower than the value for the SIP TCP Unused Connection service parameter.
Timer T1 (msec)	This field specifies the lowest value, in milliseconds, of the retransmission timer for SIP messages. Valid values include any positive number. Default specifies 500.
Timer T2 (msec)	This field specifies the highest value, in milliseconds, of the retransmission timer for SIP messages. Valid values include any positive number. Default specifies 4000.
Retry INVITE	This field specifies the maximum number of times that an INVITE request gets retransmitted. Valid values include any positive number. Default specifies 6.
Retry Non-INVITE	This field specifies the maximum number of times that a SIP message other than an INVITE request gets retransmitted. Valid values include any positive number. Default specifies 10.

Field	Description
Start Media Port	This field designates the start real-time protocol (RTP) port for media. Media port ranges from 2048 to 65535. Default specifies 16384.
Stop Media Port	This field designates the stop real-time protocol (RTP) port for media. Media port ranges from 2048 to 65535. Default specifies 32766.
Call Pickup URI	This URI provides a unique address that the phone that is running SIP sends to Cisco Unified Communications Manager to invoke the call pickup feature.
Call Pickup Group Other URI	This URI provides a unique address that the phone that is running SIP sends to Cisco Unified Communications Manager to invoke the call pickup group other feature.
Call Pickup Group URI	This URI provides a unique address that the phone that is running SIP sends to Cisco Unified Communications Manager to invoke the call pickup group feature.
Meet Me Service URI	This URI provides a unique address that the phone that is running SIP sends to Cisco Unified Communications Manager to invoke the meet me conference feature.
User Info	This field configures the user= parameter in the REGISTER message. Valid values follow: • none—No value gets inserted. • phone—The value user=phone gets inserted in the To, From, and Contact Headers for REGISTER. • ip—The value user=ip gets inserted in the To, From, and Contact Headers for REGISTER.
DTMF DB Level	This field specifies in-band DTMF digit tone level. Valid values follow: • 1 to 6 dB below nominal • 2 to 3 dB below nominal • 3 nominal • 4 to 3 dB above nominal • 5 to 6 dB above nominal
Call Hold Ring Back	If you have a call on hold and are talking on another call, when you hang up the call, this parameter causes the phone to ring to let you know that you still have another party on hold. Valid values follow: • Off permanently and cannot be turned on and off locally by using the user interface. • On permanently and cannot be turned on and off locally by using the user interface.

Field	Description
Anonymous Call Block	This field configures anonymous call block. Valid values follow: • Off—Disabled permanently and cannot be turned on and off locally by using the user interface. • On—Enabled permanently and cannot be turned on and off locally by using the user interface.
Caller ID Blocking	This field configures caller ID blocking. When blocking is enabled, the phone blocks its own number or e-mail address from phones that have caller identification enabled. Valid values follow: • Off—Disabled permanently and cannot be turned on and off locally by using the user interface. • On—Enabled permanently and cannot be turned on and off locally by using the user interface.
Do Not Disturb Control	This field sets the Do Not Disturb (DND) feature. Valid values follow: • User—The dndControl parameter for the phone should specify 0. • Admin—The dndControl parameter for the phone should specify 2.
Telnet Level for 7940 and 7960	Cisco Unified IP Phones 7940 and 7960 do not support ssh for login access or HTTP that is used to collect logs; however, these phones support Telnet, which lets the user control the phone, collect debugs, and look at configuration settings. This field controls the telnet_level configuration parameter with the following possible values: • Disabled (no access) • Limited (some access but cannot run privileged commands) • Enabled (full access)
Resource Priority Namespace	This field enables the admin to select one of the cluster's defined Resource Priority Namespace network domains for assignment to a line via its SIP Profile.
Timer Keep Alive Expires (seconds)	Cisco Unified Communications Manager requires a keepalive mechanism to support redundancy. This field specifies the interval between keepalive messages that are sent to the backup Cisco Unified Communications Manager to ensure that it is available in the event that a failover is required.
Timer Subscribe Expires (seconds)	This field specifies the time, in seconds, after which a subscription expires. This value gets inserted into the Expires header field. Valid values include any positive number; however, 120 specifies the default value.

Field	Description
Timer Subscribe Delta (seconds)	Use this parameter in conjunction with the Timer Subscribe Expires setting. The phone resubscribes Timer Subscribe Delta seconds before the subscription period ends, as governed by Timer Subscribe Expires. Valid values range from 3 to 15. Default specifies 5.
Maximum Redirections	Use this configuration variable to determine the maximum number of times that the phone allows a call to be redirected before dropping the call. Default specifies 70 redirections.
Off Hook to First Digit Timer (microseconds)	This field specifies the time in microseconds that passes when the phone goes off hook and the first digit timer gets set. The value ranges from 0 - 15,000 microseconds. Default specifies 15,000 microseconds.
Call Forward URI	This URI provides a unique address that the phone that is running SIP sends to Cisco Unified Communications Manager to invoke the call forward feature.
Abbreviated Dial URI	This URI provides a unique address that the phone that is running SIP sends to Cisco Unified Communications Manager to invoke the abbreviated dial feature. Speed dials that are not associated with a line key (abbreviated dial indices) do not download to the phone. The phone uses the feature indication mechanism (INVITE with Call-Info header) to indicate when an abbreviated dial number has been entered. The request URI contains the abbreviated dial digits (for example, 14), and the Call-Info header indicates the abbreviated dial feature. Cisco Unified Communications Manager translates the abbreviated dial digits into the configured digit string and extend the call with that string. If no digit string has been configured for the abbreviated dial digits, a 404 Not Found response gets returned to the phone.
Conference Join Enabled	This check box determines whether the Cisco Unified IP Phones 7940 or 7960, when the conference initiator that is using that phone hangs up, should attempt to join the remaining conference attendees. Check the check box if you want to join the remaining conference attendees; leave it unchecked if you do not want to join the remaining conference attendees. **Note** This check box applies to the Cisco Unified IP Phones 7941/61/70/71/11 when they are in SRST mode only.
RFC 2543 Hold	Check this check box to enable setting connection address to 0.0.0.0 per RFC2543 when call hold is signaled to Cisco Unified Communications Manager. This allows backward compatibility with endpoints that do not support RFC3264.
Semi Attended Transfer	This check box determines whether the Cisco Unified IP Phones 7940 and 7960 caller can transfer the second leg of an attended transfer while the call is ringing. Check the check box if you want semi-attended transfer enabled; leave it unchecked if you want semi-attended transfer disabled. **Note** This check box applies to the Cisco Unified IP Phones 7941/61/70/71/11 when they are in SRST mode only.

Field	Description
Enable VAD	Check this check box if you want voice activation detection (VAD) enabled; leave it unchecked if you want VAD disabled. When VAD is enabled, no media gets transmitted when voice is detected.
Stutter Message Waiting	Check this check box if you want stutter dial tone when the phone goes off hook and a message is waiting; leave unchecked if you do not want a stutter dial tone when a message is waiting. This setting supports Cisco Unified IP Phones 7960 and 7940 that run SIP.
MLPP User Authorization	Check this box to enable MLPP User Authorization. MLPP User Authorization requires the phone to send in an MLPP username and password.
Normalization Script	
Normalization Script	From the drop-down list box, choose the script that you want to apply to this SIP profile. To import another script, go to the SIP Normalization Script Configuration window (**Device** > **Device Settings** > **SIP Normalization Script**), and import a new script file.
Parameter Name/Parameter Value	Optionally, enter parameter names and parameter values. Valid values include all characters except equals signs (=), semi-colons (;), and non-printable characters, such as tabs. You can enter a parameter name with no value. To add another parameter line, click the + (plus) button. To delete a parameter line, click the - (minus) button. **Note** You must choose a script from the Normalization Script drop-down list box before you can enter parameter names and values.
Enable Trace	Check this check box to enable tracing within the script or uncheck this check box to disable tracing. When checked, the trace.output API provided to the Lua scripter produces SDI trace **Note** Cisco recommends that you only enable tracing while debugging a script. Tracing impacts performance and should not be enabled under normal operating conditions.
Incoming Requests FROM URI Settings	
Caller ID DN	Enter the pattern that you want to use for calling line ID, from 0 to 24 digits. For example, in North America: • 555XXXX = Variable calling line ID, where X equals an extension number. The CO appends the number with the area code if you do not specify it. • 55000 = Fixed calling line ID, where you want the Corporate number to be sent instead of the exact extension from which the call is placed. The CO appends the number with the area code if you do not specify it. You can also enter the international escape character +.

Field	Description
Caller Name	Enter a caller name to override the caller name that is received from the originating SIP Device.
Trunk Specific Configuration	
Reroute Incoming Request to new Trunk based on	Cisco Unified Communications Manager only accepts calls from the SIP device whose IP address matches the destination address of the configured SIP trunk. In addition, the port on which the SIP message arrives must match the one that is configured on the SIP trunk. After Cisco Unified Communications Manager accepts the call, Cisco Unified Communications Manager uses the configuration for this setting to determine whether the call should get rerouted to another trunk. From the drop-down list box, choose the method that Cisco Unified Communications Manager uses to identify the SIP trunk where the call gets rerouted: • Never—If the SIP trunk matches the IP address of the originating device, choose this option, which equals the default setting. Cisco Unified Communications Manager, which identifies the trunk by using the source IP address of the incoming packet and the signaling port number, does not route the call to a different (new) SIP trunk. The call occurs on the SIP trunk on which the call arrived. • Contact Info Header—If the SIP trunk uses a SIP proxy, choose this option. Cisco Unified Communications Manager parses the contact header in the incoming request and uses the IP address or domain name and signaling port number that is specified in the header to reroute the call to the SIP trunk that uses the IP address and port. If no SIP trunk is identified, the call occurs on the trunk on which the call arrived. • Call-Info Header with purpose=x-cisco-origIP—If the SIP trunk uses a Customer Voice Portal (CVP) or a Back-to-Back User Agent (B2BUA), choose this option. When the incoming request is received, Cisco Unified Communications Manager parses the Call-Info header, looks for the parameter, purpose=x-cisco-origIP, and uses the IP address or domain name and the signaling port number that is specified in the header to reroute the call to the SIP trunk that uses the IP address and port. If the parameter does not exist in the header or no SIP trunk is identified, the call occurs on the SIP trunk on which the call arrived. **Tip** This setting does not work for SIP trunks that are connected to a Cisco Unified Presence proxy server or SIP trunks that are connected to originating gateways in different Cisco Unified CM groups.

Field	Description
RSVP Over SIP	This field configures RSVP over SIP trunks. From the drop-down list box, choose the method that Cisco Unified Communications Manager uses to configure RSVP over SIP trunks: • Local RSVP—In a local configuration, RSVP occurs within each cluster, between the end point and the local SIP trunk, but not on the WAN link between the clusters. • E2E—In an end-to-end (E2E) configuration, RSVP occurs on the entire path between the end points, including within the local cluster and over the WAN.
Resource Priority Namespace List	Select a configured Resource Priority Namespace list from the drop-down menu. Configure the lists in the Resource Priority Namespace List menu that is accessed from **System** > **MLPP** > **Namespace**.
Fall back to local RSVP	Check this box if you want to allow failed end-to-end RSVP calls to fall back to local RSVP to establish the call. If this box is not checked, end-to-end RSVP calls that cannot establish an end-to-end connection fail.
SIP Rel1XX Options	This field configures SIP Rel1XX, which determines whether all SIP provisional responses (other than 100 Trying messages) get sent reliably to the remote SIP endpoint. Valid values follow: • Disabled—Disables SIP Rel1XX. • Send PRACK if 1XX contains SDP—Acknowledges a 1XX message with PRACK, only if the 1XX message contains SDP. • Send PRACK for all 1XX messages —Acknowledges all1XX messages with PRACK. If you set the RSVP Over SIP field to E2E, you cannot choose Disabled.

Field	Description
Session Refresh Method	Session Timer with Update: The session refresh timer allows for periodic refresh of SIP sessions, which allows the Unified Communications Manager and remote agents to determine whether the SIP session is still active. Prior to Release 10.01, when the Unified Communications Manager received a refresh command, it supported receiving either Invite or Update SIP requests to refresh the session. When the Unified Communications Manager initiated a refresh, it supported sending only Invite SIP requests to refresh the session. With Release 10.01, this feature extends the refresh capability so that Unified Communications Manager can send both Update and Invite requests. Specify whether Invite or Update should be used as the Session Refresh Method. **Invite** (default): **Note** Sending a mid-call Invite request requires that an offer SDP be specified in the request. This means that the far end must send an answer SDP in the Invite response. **Update**: Unified Communications Manager sends a SIP Update request, if support for the Update method is specified by the far end of the SIP session either in the Supported or Require headers. When sending the Update request, the Unified Communications Manager includes an SDP. This simplifies the session refresh since no SDP offer/answer exchange is required. **Note** If the Update method is not supported by the far end of the SIP session, the Unified Communications Manager continues to use the Invite method for session refresh.
Video Call Traffic Class	Video Call Traffic Class determines the type of video endpoint or trunk that the SIP Profile is associated with. From the drop-down list box, select one of the following three options • Immersive—High-definition immersive video. • Desktop—Standard desktop video. • Mixed—A mix of immersive and desktop video. Cisco Unified Communications Manager Locations Call Admission Control (CAC) reserves bandwidth from two Locations video bandwidth pools, "Video Bandwidth" and/or "Immersive Bandwidth", depending on the type of call determined by the Video Call Traffic Class. Please refer to the Call Admission Control chapter of the *Cisco Unified Communications Manager System Guide* for more information.
Calling Line Identification Presentation	Select **Strict From URI presentation Only** to select the network provided identity. Select **Strict Identity Headers presentation Only** to select the user provided identity.

Field	Description
Deliver Conference Bridge Identifier	Check this check box for the SIP trunk to pass the b-number that identifies the conference bridge across the trunk instead of changing the b-number to the null value. The terminating side does not require that this field be enabled. Checking this check box is not required for Open Recording Architecture (ORA) SIP header enhancements to the Recording feature to work. Enabling this check box allows the recorder to coordinate recording sessions where the parties are participating in a conference.
Early Offer support for voice and video calls (insert MTP if needed)	Check this check box if you want to create a trunk that supports early offer. Early Offer configurations on SIP profile apply to SIP trunk calls. These configurations do not affect SIP line side calls. If this profile is shared between a trunk and a line, only the SIP trunk that uses the profile provides early offer. Because E2E RSVP provides an early offer by including an SDP in the initial INVITE, the early offer and E2E RSVP features are mutually exclusive on the SIP Profile Configuration window. When you choose E2E from the RSVP Over SIP drop-down list box, the Early Offer support for voice and video calls (insert MTP if needed) check box gets disabled. **Note** When checked, the Media Termination Required check box on the Trunk Configuration window overrides the early offer configuration on the associated SIP profile. The Cisco Unified Communications Manager sends the MTP IP address and port with a single codec in the SDP in the initial INVITE.
Send send-receive SDP in mid-call INVITE	Check this check box to prevent Cisco Unified Communications Manager from sending an INVITE a=inactive SDP message during call hold or media break during supplementary services. **Note** This check box applies only to early offer enabled SIP trunks and has no impact on SIP line calls. When you enable Send send-receive SDP in mid-call INVITE for an early offer SIP trunk in tandem mode, Cisco Unified Communications Manager inserts MTP to provide sendrecv SDP when a SIP device sends offer SDP with a=inactive or sendonly or recvonly in audio media line. In tandem mode, Cisco Unified Communications Manager depends on the SIP devices to initiate reestablishment of media path by sending either a delayed INVITE or mid-call INVITE with send-recv SDP. When you enable both Send send-receive SDP in mid-call INVITE and Require SDP Inactive Exchange for Mid-Call Media Change on the same SIP Profile, the Send send-receive SDP in mid-call INVITE overrides the Require SDP Inactive Exchange for Mid-Call Media Change, so Cisco Unified Communications Manager does not send an INVITE with a=inactive SDP in mid-call codec updates. For SIP line side calls, the Require SDP Inactive Exchange for Mid-Call Media Change check box applies when enabled. **Note** To prevent the SDP mode from being set to inactive in a multiple-hold scenario, set the Duplex Streaming Enabled clusterwide service parameter (**System** > **Service Parameters**) to True.

Field	Description
Allow Presentation Sharing using BFCP	If the box is checked, Cisco Unified Communications Manager is configured to allow supported SIP endpoints to use the Binary Floor Control Protocol to enable presentation sharing. The use of BFCP creates an additional media stream in addition to the existing audio and video streams. This additional stream is used to stream a presentation, such as a PowerPoint presentation from someone's laptop, into a SIP videophone. If the box is unchecked, Cisco Unified Communications Manager rejects BFCP offers from devices associated with the SIP profile by setting the BFCP application line and associated media line ports to 0 in the answering SDP message. This is the default behavior. **Note** BFCP is only supported on SIP networks. BFCP must be enabled on all SIP trunks, lines, and endpoints for presentation sharing to work. BFCP is not supported if the SIP line or SIP trunk uses MTP, RSVP, TRP or Transcoder. For more information on BFCP, refer to the *Cisco Unified Communications Manager System Guide*.
Allow iX Application Media	Check this check box to enable support for iX media channel.
Allow Passthrough of Configured Line Device Caller Information	Check this box to allow passthrough of configured line device caller information from the SIP trunk.
Reject Anonymous Incoming Calls	Check this box to reject anonymous incoming calls.
Reject Anonymous Outgoing Calls	Check this box to reject anonymous outgoing calls.
Allow multiple codecs in answer SDP	This option applies when incoming SIP signals do not indicate support for multiple codec negotiation and Cisco Unified Communications Manager can finalize the negotiated codec. When this check box is checked, the endpoint behind the trunk is capable of handling multiple codecs in the answer SDP. For example, an endpoint that supports multiple codec negotiation calls the SIP trunk and Cisco Unified Communications Manager sends a Delay Offer request to a trunk. The endpoint behind the trunk returns all support codecs without the Contact header to indicate the support of multiple codec negotiation. In this case, Cisco Unified Communications Manager identifies the trunk as capable of multiple codec negotiation and sends SIP response messages back to both endpoints with multiple common codecs. When this check box is left unchecked, Cisco Unified Communications Manager identifies the endpoint behind the trunk as incapable of multiple codec negotiation, unless indicated otherwise by SIP contact header URI. Cisco Unified Communications Manager continues the call with single codec negotiation.

Field	Description
Send ILS Learned Destination Route String	When this check box is checked, for calls that Cisco Unified Communications Manager routes to a learned directory URI, learned number, or learned pattern, Cisco Unified Communications Manager adds the *x-cisco-dest-route-string* header to outgoing SIP INVITE and SUBSCRIBE messages and inserts the destination route string into the header. When this check box is left unchecked, Cisco Unified Communications Manager does not add the *x-cisco-dest-route-string* header to any SIP messages. The *x-cisco-dest-route-string* header allows Cisco Unified Communications Manager to route calls across a Cisco Unified Border Element.
SIP OPTIONS Ping	
Enable OPTIONS Ping to monitor destination status for Trunks with service type "None (Default)"	Check this check box if you want to enable the SIP OPTIONS feature. SIP OPTIONS are requests to the configured destination address on the SIP trunk. If the remote SIP device fails to respond or sends back a SIP error response such as 503 Service Unavailable or 408 Timeout, Cisco Unified Communications Manager tries to reroute the calls by using other trunks or by using a different address. If this check box is not checked, the SIP trunk does not track the status of SIP trunk destinations. When this check box is checked, you can configure two request timers.
Ping Interval for In-service and Partially In-service Trunks (seconds)	This field configures the time duration between SIP OPTIONS requests when the remote peer is responding and the trunk is marked as In Service. If at least one IP address is available, the trunk is In Service; if all IP addresses are unavailable, the trunk is Out of Service. The default value specifies 60 seconds. Valid values range from 5 to 600 seconds.
Ping Interval for Out-of-service SIP Trunks (seconds)	This field configures the time duration between SIP OPTIONS requests when the remote peer is not responding and the trunk is marked as Out of Service. The remote peer may be marked as Out of Service if it fails to respond to OPTIONS, if it sends 503 or 408 responses, or if the Transport Control Protocol (TCP) connection cannot be established. If at least one IP address is available, the trunk is In Service; if all IP addresses are unavailable, the trunk is Out of Service. The default value specifies 120 seconds. Valid values range from 5 to 600 seconds.
Ping Retry Timer (milliseconds)	This field specifies the maximum waiting time before retransmitting the OPTIONS request. Valid values range from 100 to 1000 milliseconds. The default value specifies 500 milliseconds.

Field	Description
Ping Retry Count	This field specifies the number of times that Cisco Unified Communications Manager resends the OPTIONS request to the remote peer. After the configured retry attempts are used, the destination is considered to have failed. To obtain faster failure detection, keep the retry count low. Valid values range from 1 to 10. The default value specifies 6.

Synchronize SIP Profile Settings with SIP Devices

To synchronize SIP devices with a SIP profile that has undergone configuration changes, perform the following procedure, which applies 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 **Device** > **Device Settings** > **SIP Profile**.
The Find and List SIP Profiles window displays.

Step 2 Choose the search criteria to use.

Step 3 Click Find.
The window displays a list of SIP Profiles that match the search criteria.

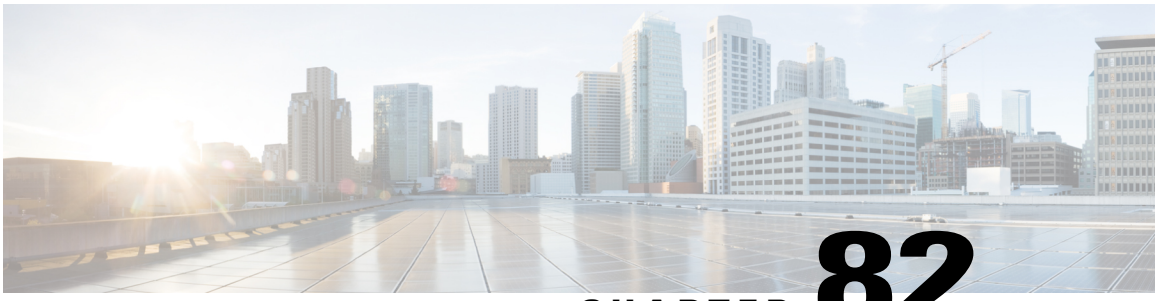
Step 4 Click the SIP profile to which you want to synchronize applicable SIP devices. The SIP Profile Configuration window displays.

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.



CHAPTER 82

Common Device Setup

This chapter provides information to configure common device configurations.

About Common Device Setup

In Cisco Unified Communications Manager Administration, use the**Device** > **Device Settings** > **Common Device Configuration** menu path to configure common device configurations.

A common device configuration comprises user-specific service and feature attributes. Ensure that each device is associated with a common device configuration for user-oriented information.

Note The Device Pool window now contains only location-related information. The Common Device Configuration window records all the user-oriented information.

Common Device Setup Deletion

You cannot delete a common device configuration that a device uses. To find out which devices are using the common device configuration, click the Dependency Records link from the Common Device Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. If you try to delete a common device configuration that is in use, Cisco Unified Communications Manager displays a message. Before deleting a common device configuration that is currently in use, you must perform either or both of the following tasks:

- Assign a different common device configuration to any devices that are using the common device configuration that you want to delete.
- Delete the devices that are using the common device configuration that you want to delete.

Related Topics

Access Dependency Records , on page 982

Common Device Settings

The following table describes the common device settings.

Table 111: Common Device Settings

Field	Description
Common Device Configuration Information	
Name	Enter a name to identify the common device configuration.
Softkey Template	From the drop-down list box, choose the softkey template for the common device configuration.
User Hold MOH Audio Source	Choose the audio source to use for MOH when a user initiates a hold action.
Network Hold MOH Audio Source	Choose the audio source to use for music on hold (MOH) when the network initiates a hold action.
User Locale	From the drop-down list box, choose the locale for the common device configuration. The user locale identifies a set of detailed information to support users, including language and font. **Note** If the user does not choose a user locale, the locale that is specified in the Cisco Unified Communications Manager clusterwide parameters as Default User Locale applies.

Field	Description
IP Addressing Mode	Choose the version of IP address that the device (SIP trunk or phone that runs 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 only an IPv4 or IPv6 is available for a device (not both types of IP addresses), the device uses the available IP address to negotiate the call. If the device has both IP address types for both signaling and media events, Cisco Unified Communications Manager uses the configuration for IP Addressing Mode Preference for Signaling setting for signaling events and the IP Addressing Mode Preference for Media enterprise parameter for media events.
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.

Field	Description
Allow Auto-Configuration for Phones	This drop-down list box supports IPv6 for dual-stack Cisco Unified IP Phones that run SCCP. 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.
Allow Duplicate Address Detection	This drop-down list box supports an IPv6 parameter for Cisco IP Phones. From the drop-down list box, choose one of the following options: • On—The phone performs duplicate address detection on each of the addresses in all the identity associations that it receives in the Reply message. • Off—The phone does not perform duplicate address detection. • Default—To use the configuration for the Allow Duplicate Address Detection enterprise parameter, choose this option.
Accept Redirect Messages	This drop-down list box supports an IPv6 parameter for Cisco IP Phones. From the drop-down list box, choose one of the following options: • On—The phone accepts the redirect messages from the same router that is used for the destination number. • Off—The phone ignores the redirect messages. • Default—To use the configuration for the Accept Redirect Messages enterprise parameter, choose this option.

Field	Description
Reply Multicast Echo Request	This drop-down list box supports an IPv6 parameter for Cisco IP Phones. From the drop-down list box, choose one of the following options: • On—The phone sends an Echo Reply message in response to an Echo Request message sent to an IPv6 address. • Off—The phone does not send Echo Reply messages. • Default—To use the configuration for the Reply Multicast Echo Request enterprise parameter, choose this option.
Use Trusted Relay Point	From the drop-down list box, choose one of the following options: • On—To allow the IP Phones to send multicast echo request messages. • Off—To disable sending multicast echo request messages. • Default—To use the configuration for the Reply Multicast Echo Request enterprise parameter, choose this option.
Use Intercompany Media Engine (IME) for Outbound Calls	Check this check box to enable the devices that associate with this common device configuration to use a trusted relay point. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified Communications Manager inserts a TRP for an endpoint if the Use Trusted Relay Point check box is checked for the endpoint or for the common device configuration with which the endpoint associates. The endpoint device can comprise any device that terminates media, including SIP, H.323, MGCP, and SCCP devices, such as phones that are running SCCP, CTI devices, MoH servers, annunciators, and conference bridges. If the Use Trusted Relay Point setting of a device specifies On or Off, the device setting overrides the Use Trusted Relay Point setting from the common device configuration with which the device associates. Cisco Unified Communications Manager places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVPAgent). If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the *Cisco Unified Communications Manager System Guide* for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified Communications Manager first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified Communications Manager first tries to find a transcoder that is also designated as a TRP. See the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.

Field	Description
Multilevel Precedence and Preemption Information	
MLPP Indication	This setting specifies whether devices that are capable of playing precedence tones will use the capability when the devices place an MLPP precedence call. From the drop-down list box, choose a setting to assign to the devices from the following options: • Default—Devices inherit MLPP Indication settings from the MLPP Indication Status enterprise parameter. • Off—Devices do not handle nor process indication of an MLPP precedence call. • On—Devices do handle and process indication of an MLPP precedence call. **Note** Do not configure the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful. **Note** Turning on MLPP Indication (at the enterprise parameter or device level) disables normal Ring Setting behavior for the lines on a device, unless MLPP Indication is turned off (overridden) for the device.
MLPP Preemption	This setting specifies whether devices that are capable of preempting calls in progress will use the capability when the devices place an MLPP precedence call. From the drop-down list box, choose a setting to assign to the devices from the following options: • Default—Devices inherit MLPP Preemption settings from the MLPP Preemption Setting enterprise parameter. • Disabled—Devices do not allow preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. • Forceful—Devices allow preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. **Note** Do not configure the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful.
Confidential Access Level	Select the appropriate CAL value from the drop-down list box.

Related Topics

Common Device Setup , on page 763

Synchronize Common Device Settings with Devices

To synchronize devices with a common device configuration that has undergone configuration changes, perform the following procedure, which applies 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 **Device** > **Device Settings** > **Common Device Configuration**.
The Find and List Common Device Configurations window displays.

Step 2 Choose the search criteria to use.

Step 3 Click Find.
The window displays a list of common device configurations that match the search criteria.

Step 4 Click the common device configuration to which you want to synchronize applicable devices. The Common Device Configuration Information window displays.

Step 5 Make any additional configuration changes.

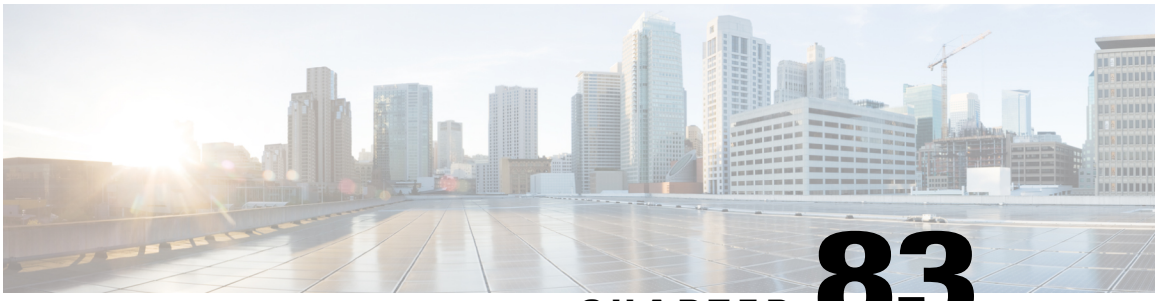
Step 6 Click Save.

Step 7 Click Apply Config.
The Apply Configuration Information dialog displays.

Step 8 Click OK.

Related Topics

Common Device Setup , on page 763



CHAPTER 83

Common Phone Profile Setup

This chapter provides information to configure and locate common phone profiles.

About Common Phone Profile Setup

In Cisco Unified Communications Manager Administration, use the **Device** > **Device Settings** > **Common Phone Profile** menu path to configure common phone profiles.

Common phone profiles provide data that Cisco TFTP requires. After you configure a common phone profile, use the Phone Configuration window to associate a phone that is running SCCP or SIP with a common phone profile.

Common Phone Profile Deletion

To find out which devices are using the common phone profile, choose Dependency Records link from the Related Links drop-down list box in the Common Phone Profile Configuration window. If dependency records are not enabled for the system, the dependency records summary window displays a message.

Note You cannot delete the Standard Common Phone Profile.

Related Topics

Access Dependency Records , on page 982

Common Phone Profile Settings

The following table describes the available settings in the Common Phone Profile Configuration window.

Note To view field descriptions and help for product-specific configuration items, click the ? question icon in the Product Specific Configuration area to display help in a popup window.

Select the "Override Common Settings" box for any setting in Product Specific Configuration area that you wish to update. If you do not check this box, the corresponding parameter setting does not take effect. Parameters that you set in the Product Specific Configuration area may also appear in the Device Configuration window for various devices and in the Enterprise Phone Configuration window. If you set these same parameters in these other windows too, the setting that takes precedence is determined in the following order: 1) Device Configuration window settings, 2) Common Phone Profile window settings, 3) Enterprise Phone Configuration window settings.

Table 112: Common Phone Profile Settings

Field	Description
Common Phone Profile Information	
Name	Enter a name to identify the common phone profile; for example, CPP_7905. The value can include 1 to 50 characters, including alphanumeric characters, dot, dash, and underscores.
Description	Identify the purpose of the common phone profile; for example, common phone profile for the 7905 phone. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
Local Phone Unlock Password	Enter the password that is used to unlock a local phone. Valid values comprise 1 to 15 characters.
DND Option	When you enable Do Not Disturb (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 the user can accept the call. **Note** For 7940/7960 phones that are running SCCP, you can only choose the Ringer Off option. For mobile devices and dual-mode phones, you can only choose the Call Reject option. When you activate DND Call Reject on a mobile device or dual-mode phone, no call information gets presented to the device.

Field	Description
DND Incoming Call Alert	When you enable the DND Ringer Off or Call Reject option, this parameter specifies how a call displays on a phone. From the drop-down list, choose one of the following options: • 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 beep. • Flash Only—For an incoming call, this option causes the phone to display a flash alert.
Feature Control Policy	From the drop-down list box, you can choose a feature control policy that has already been configured in the Feature Control Policy configuration window (Device > Device Settings > Feature Control Policy).
Wi-Fi Hotspot Profile	Select a Wi-Fi Hotspot Profile from the drop-down list box. You may also click **View Details** to display details about the Wi-Fi Hotspot Profile that you select. **Note** This field does not apply to all phone models.
Enable End User Access to Phone Background Image Setting	Check this check box to enable end users to change the background image on phones that use this common phone profile.
Secure Shell Information	
Secure Shell User	Enter a user ID for the secure shell user. Cisco Technical Assistance Center (TAC) uses secure shell for troubleshooting and debugging. Contact TAC for further assistance. See the Cisco Unified Communications Manager Security Guide for this release for information about how to configure encrypted phone configuration files to ensure that Cisco Unified Communications Manager does not send SSH credentials to the phone in the clear.
Secure Shell Password	Enter the password for a secure shell user. Contact TAC for further assistance. See the Cisco Unified Communications Manager Security Guide for this release for information about how to configure encrypted phone configuration files to ensure that Cisco Unified Communications Manager does not send SSH passwords to the phone in the clear.
Phone Personalization Information	

Field	Description
Phone Personalization	The Phone Personalization setting allows you to enable a Cisco Unified IP Phone, so it works with Phone Designer, a Cisco Unified Communications widget that allows a phone user to customize the wallpaper and ring tones on the phone. From the Phone Personalization drop-down list box, choose one of the following options: • Disabled-The user cannot customize the Cisco Unified IP Phone by using Phone Designer. • Enabled-The user can use Phone Designer to customize the phone. • Default-The phone uses the configuration from the Phone Personalization enterprise parameter if you choose Default in both the Phone Configuration and Common Phone Profile Configuration windows. If you choose Default in the Common Phone Profile Configuration window but not in the Phone Configuration window, the phone uses the configuration that you specify in the Phone Configuration window. You must install and configure Phone Designer, so the phone user can customize the phone. Before you install and configure Phone Designer, identify which Cisco Unified IP Phone models work with Phone Designer, as described in the Phone Designer documentation. For more information on Phone Designer, see the Phone Designer documentation.
Always Use Prime Line	From the drop-down list box, choose one of the following options: • Off—When the phone is idle and receives a call on any line, the phone user answers the call from the line on which the call is received. • On—When the phone is idle (off hook) and receives a call on any line, the primary line gets chosen for the call. Calls on other lines continue to ring, and the phone user must select those other lines to answer these calls. • Default—Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter, which supports the Cisco CallManager service.
Always Use Prime Line for Voice Message	From the drop-down list box, choose one of the following options: • On—If the phone is idle, the primary line on the phone becomes the active line for retrieving voice messages when the phone user presses the Messages button on the phone. • Off—If the phone is idle, pressing the Messages button on the phone automatically dials the voice-messaging system from the line that has a voice message. Cisco Unified Communications Manager always selects the first line that has a voice message. If no line has a voice message, the primary line gets used when the phone user presses the Messages button. • Default—Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line for Voice Message service parameter, which supports the Cisco CallManager service.

Field	Description
Services Provisioning	From the drop-down list box, choose how the phone will support the services: • Internal—The phone uses the phone configuration file to support the service. Choose this option or Both for Cisco-provided default services where the Service URL has not been updated; that is, the service URL indicates Application:Cisco/<name of service>; for example, Application:Cisco/CorporateDirectory. Choose Internal or Both for Cisco-signed Java MIDlets because Cisco-signed Java MIDlets are provisioned in the configuration file. • External URL—Choosing External URL indicates that the phone ignores the services in the phone configuration file and retrieves the services from a Service URL. If you configured a custom Service URL for a service, you must choose either External URL or Both; if you choose Internal in this case, the services that are associated with the custom URLs do not work on the phone. • Both—Choosing Both indicates that the phone support both the services that are defined in the configuration file and external applications that are retrieved from custom service URLs. If you have phones in your network that can obtain the service information from the phone configuration file and phones in your network that can only use custom service URLs for obtaining the information, choose Both.
VPN Information	
VPN Group	From the drop-down list, choose the VPN Group for the phone. For information about creating VPN groups, see the Virtual Private Network Configuration chapter in the Cisco Unified Communications Manager Security Guide.
VPN Profile	From the drop-down list, choose the VPN profile for the phone. For information about creating VPN profiles, see the Virtual Private Network Configuration chapter in the Cisco Unified Communications Manager Security Guide.

Related Topics

Common Phone Profile Setup , on page 771

Synchronize Common Phone Profile Settings with Devices

To synchronize devices with a common phone profile that has undergone configuration changes, perform the following procedure, which applies 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 **Device** > **Device Settings** > **Common Phone Profile**.
The Find and List Common Phone Profiles window displays.

Step 2 Choose the search criteria to use.

Step 3 Click Find.
The window displays a list of common phone profiles that match the search criteria.

Step 4 Click the common phone profile to which you want to synchronize applicable devices. The Common Phone Profile Configuration window displays.

Step 5 Make any additional configuration changes.

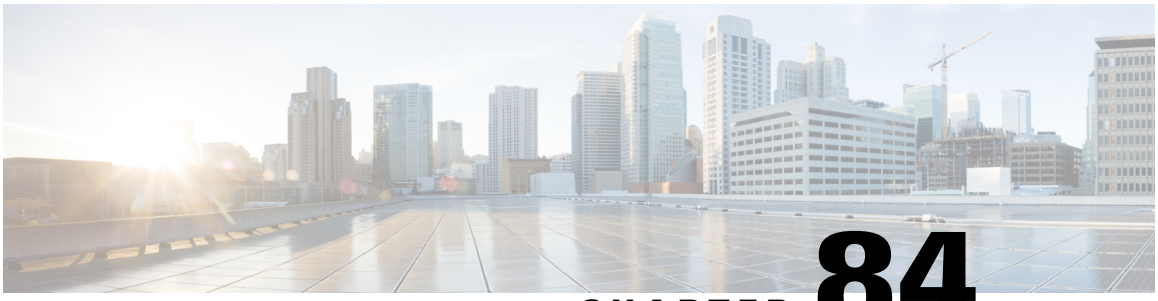
Step 6 Click Save.

Step 7 Click Apply Config.
The Apply Configuration Information dialog displays.

Step 8 Click OK.

Related Topics

Common Phone Profile Setup , on page 771



CHAPTER 84

Feature Control Policy Setup

This chapter provides information to find and add Feature Control Policies. When you disable a feature, the softkeys for the disabled feature do not appear in any call state.

About Feature Control Policy Setup

To generate a list of supported features for all phones on your Cisco Unified Communications Manager, including the Feature Control Policy, you can generate a Unified CM Phone Feature List report on Cisco Unified Reporting.

In Cisco Unified Communications Manager Administration, use the **Device** > **Device Settings** > **Feature Control Policy** menu path to configure feature control policies.

Feature Control Policies allows you to enable or disable a particular feature and thereby control the appearance of certain features and softkeys that display on the phone. You can configure multiple policies on Cisco Unified Communications Manager Administration. After you configure a Feature Control Policy, you must associate that policy to an individual phone, a group of phones, or to all phones in the system.

Note You can customize the appearance of softkeys on other Cisco Unified IP Phones by using softkey templates.

Feature Control Policies Configuration Tips

When you configure a feature control policy, specify the phone to which you want the feature control policy to apply. You can set feature control policies for all phones in your system, for a group of phones, or for an individual phone. You can also have multiple feature control policies.

- To specify a policy for all phones on the system, choose **System** > **Enterprise Parameters** and select the feature control policy that you want from the Feature Control Policy drop-down box in the Enterprise Parameters window.

- To specify a policy to a group of phones, choose **Device** > **Phone** > **Common Phone Profile** to create a new phone profile or to update an existing phone profile, select the feature control policy that you want in the Feature Control Policy drop-down box, and then select the common phone profile when you configure your phone.
- To specify a policy on an individual phone, choose **Device** > **Phone**, and select the feature control policy that you want from the Feature Control Policy drop-down box in the Phone Configuration window.

Note When feature control polices are configured in different windows, Cisco Unified Communications Manager uses the following order of precedence (Device Configuration has the highest precedence):

1. Device Configuration window settings
2. Common Phone Profile window settings
3. Enterprise Parameter Configuration window settings

Related Topics

Update Enterprise Parameters , on page 148
Phone Setup , on page 581
About Common Phone Profile Setup , on page 771
Feature Control Policy Default Values , on page 779

Feature Control Policy Deletion

You can delete a feature control policy that is not currently assigned to any phone in your system. You cannot delete a policy that is assigned to one or more phones.

To find out which phones are using the feature control policy, choose the Dependency Records link from the Related Links drop-down list box in the Feature Control Policy Configuration window and click Go. If dependency records are not enabled for the system, the dependency records summary window displays a message. If you try to delete a feature control policy that is in use, Cisco Unified Communications Manager displays a message. Before deleting a feature control policy that is currently in use, you must perform either or both of the following tasks:

- Assign a different feature control policy to the phones that are using the feature control policy that you want to delete.
- Delete the phones that are using the feature control policy that you want to delete.

Related Topics

Phone Deletion Preparation , on page 582
About Feature Control Policy Setup , on page 777
Access Dependency Records , on page 982

Feature Control Policy Settings

The following table describes the Feature Control Policy settings.

Table 113: Feature Control Policy Settings

Field	Description
Feature Control Policy Info	
Name	Enter a name in the Feature Control Policy 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 feature control policy name is unique to the system.
Description	Enter a description in the Description field. The description can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_).
Feature Control Section	
Feature Control	For each feature listed, choose whether you want to override the system default and enable or disable the setting: • If the feature is enabled by default and you want to disable the setting, check the check box under Override Default and uncheck the check box under Enable Setting. • If the feature is disabled by default and you want to enable the setting, check the check box under Override Default and check the check box under Enable Setting.

Feature Control Policy Default Values

The following table lists the features, default value, and associated softkeys for feature control policies.

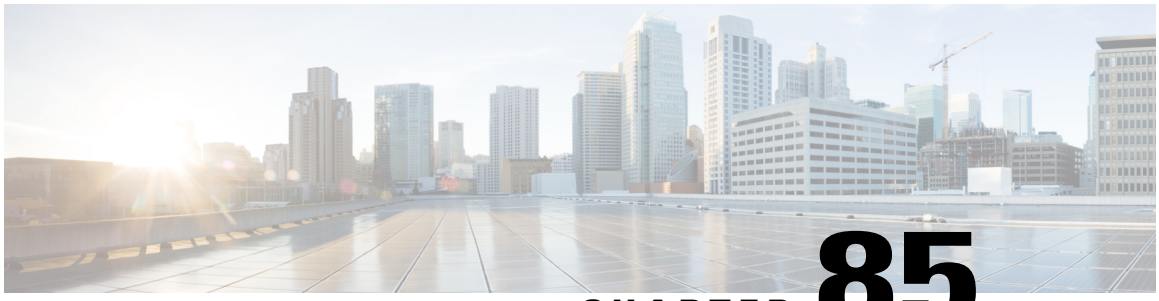
Table 114: Feature Control Policy Default Values

Feature	Default Value	Softkeys Displayed on the Phone
Barge	Enabled	Barge
Call Back	Enabled	Call Back
Call Pick Up	Disabled	Call Pick Up
Conference List	Enabled	Show Detail

Feature	Default Value	Softkeys Displayed on the Phone
Divert (Alerting)	Disabled	Divert
Divert (Connected)	Disabled	Divert
Forward All	Enabled	Forward All
Group Call Pick Up	Disabled	Group Call Pick Up
Meet Me	Disabled	Meet Me
Mobility	Disabled	Mobility
Other Call Pick Up	Disabled	Other Call Pick Up
Park	Disabled	Park and Resume
Redial	Enabled	Redial
Report Caller	Disabled	Report Caller
Report Quality	Disabled	Report Quality
Speed Dial	Enabled	Speed Dial

Related Topics

Feature Control Policy Setup , on page 777



CHAPTER 85

Recording Profile Setup

This chapter provides information to configure recording profiles.

About Recording Profile Setup

In Cisco Unified Communications Manager Administration, use the **Device** > **Phone** > **Recording Profile** menu path to configure recording profiles.

To provision line appearances of agents for call recording, you create one or more call recording profiles. You then select a recording profile for a line appearance.

Recording Profile Deletion

You cannot delete a recording profile that a line appearance uses. To find out which line appearances are using the recording profile, choose Dependency Records from the Related Links drop-down list box that is on the Recording Profile Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. If you try to delete a recording profile that is in use, Cisco Unified Communications Manager displays a message. Before deleting a recording profile that is currently in use, you must perform either or both of the following tasks:

- Assign a different recording profile to any line appearances that are using the recording profile that you want to delete.
- Delete the line appearances that are using the recording profile that you want to delete.

Related Topics

Access Dependency Records , on page 982

Recording Profile Settings

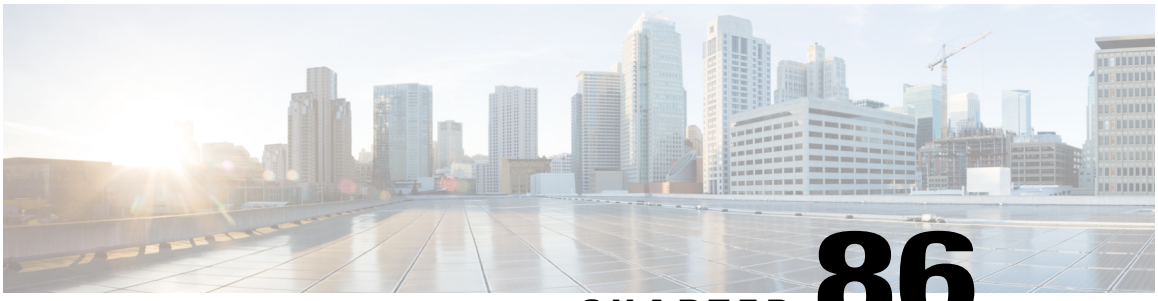
The following table describes the recording profile settings.

Table 115: Recording Profile Settings

Field	Description
Name	Enter a name to identify the recording profile.
Recording Calling Search Space	From the drop-down list box, choose the calling search space that contains the partition of the route pattern that is associated with the SIP trunk that is configured for the recorder.
Recording Destination Address	Enter the directory number (DN) or the URL of the recorder that associates with this recording profile. This field allows any characters except the following characters: double quotation marks ("), back quote (`), and space ( ).

Related Topics

Recording Profile Setup , on page 781



CHAPTER 86

SIP Normalization Script Setup

This chapter provides information about Cisco Unified Communications Manager SIP normalization script configuration.

About SIP Normalization Script Setup

In Cisco Unified Communications Manager Administration, use the**Device** > **Device Settings** > **SIP Normalization Script** menu path to configure SIP normalization and transparency scripts.

SIP trunks can connect to a variety of endpoints, including PBXs, gateways, and service providers. Each of these endpoints implements the SIP protocol a bit differently, causing a unique set of interoperability issues. To normalize messages per trunk, Cisco Unified Communications Manager allows you to add or update scripts to the system and then associate them with one or more SIP trunks. The normalization scripts that you create allow you to preserve, remove, or change the contents of any SIP headers or content bodies, known or unknown.

Transparency refers to the ability to pass information from one call leg to the other. REFER transparency allows Cisco Unified Communications Manager to pass on REFER requests to another endpoint rather than acting on them. REFER transparency is key in call center applications, where the agent sending the REFER (initiating the transfer) resides in a geographic area remote from both of the other call parties.

After you configure a script in Cisco Unified Communications Manager, you associate the script with a SIP trunk by configuring the Normalization Script fields in the Trunk Configuration window. You can only associate one script per trunk, but you can associate the same script to multiple trunks.

SIP Normalization Scripts Configuration Tips

You cannot edit the refer-passthrough script. If you want to use the content of the refer-passthrough script in a custom script, display the script in the SIP Normalization Script window. Copy the information from the Content field, click the Add New button to create a new script record, and paste the information from the refer-passthrough script into the new record.

Related Topics

About Trunk Setup , on page 637

SIP Normalization Script Deletion

You cannot delete the refer-passthrough script.

SIP Normalization Script Settings

The following table describes the SIP normalization script settings.

Table 116: SIP Normalization Script Settings

Field	Description
Name	Enter a unique identifier for the script. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_).
Description	Enter a descriptive name for the script.
Content	This field displays the content of the imported script. You can edit the script in this text box.

Field	Description
Script Execution Error Recovery Action	Choose the action that you want the system to perform when an execution error gets detected while executing a script message handler. An execution error can occur due a number of issues, such as a script invokes one of the Cisco SIP Message APIs but passes in the wrong number of arguments, or a script passes a nil string to a string library API. When an execution error gets detected, the system automatically exits the message handler at the point of the failure, restores the message to its original content prior to executing the message handler (in other words, performs message rollback), and continues as if the message handler was never invoked. After the automatic error message handling, the system performs the action that you choose from the drop-down list box: • SIP Message Rollback Only—(Default) The script continues to execute for subsequent messages. • SIP Disable Script—Cisco Unified Communications Manager closes the script and does not execute it for subsequent messages. The Lua state remains closed and the system reclaims all of the memory. You must manually reset the trunk to re-enable the script. • SIP Reset Script—Cisco Unified Communications Manager closes and immediately reloads the script. When the script is closed, the Lua state is closed and the system reclaims all of the memory. Any state that the script maintains is lost. After the script reloads, Cisco Unified Communications Manager automatically uses the script for subsequent messages. • SIP Script Reset Trunk—The system immediately resets the trunk, which affects existing calls. Cisco Unified Communications Manager closes the script while the trunk resets. After the trunk restarts, Cisco Unified Communications Manager automatically reopens the script.

Field	Description
System Resource Error Recovery Action	Choose the action that you want Cisco Unified Communications Manager to take when a script aborts during execution because Memory Threshold and Lua Instruction Threshold values were exceeded. Resource errors can occur when the script is loading, initializing, or executing a message handler. If the script fails to load or initialize, it is immediately disabled. The configured System Resource Error Recovery Action does not apply to load and initialization errors. This action applies only to execution errors. Execution errors occur only while executing message handlers. When a resource error occurs while a script executes a message handler, the system automatically exits the message handler at the point of the failure, restores the message to its original content prior to executing the message handler (in other words, performs message rollback), and continues as if the message handler was never invoked. After the automatic error message handling, the system performs the action that you choose from the drop-down list box: • SIP Disable Script—(Default) The script closes and does not execute for subsequent messages. The Lua state remains closed and the system reclaims all of the memory. You must manually reset the trunk to re-enable the script. • SIP Reset Script—The script closes and then immediately reloads. When the script closes, the Lua state closes and the system reclaims all of the memory. Any state that the script maintains is lost. After the script reloads, Cisco Unified Communications Manager automatically uses the script for subsequent messages. • SIP Script Reset Trunk—The system immediately resets the trunk, which affects existing calls. The script closes while the trunk resets. After the trunk restarts, the script reopens automatically.
Memory Threshold	Enter the memory threshold value in kilobytes. You must enter an integer into this field. If memory usage exceeds 80 percent of this value, the SIPNormalizationScriptResourceWarning resource warning alarm gets generated. The script continues to execute until the memory usage exceeds 100 percent of this value. If memory usage exceeds 100 percent during script loading or initialization, a script error alarm gets generated, and the script gets closed and disabled. If memory usage exceeds 100 percent during script execution, a script error alarm gets generated, and Cisco Unified Communications Manager performs the action that the System Resource Error Recovery Action field specifies. For example, if you enter 50 kilobytes into this field, the warning alarm gets generated if the script exceeds 40 kilobytes. The script continues to run until memory usage exceeds 50 kilobytes. The default value specifies 50 kilobytes.

Field	Description
Lua Instruction Threshold	This field specifies the maximum number of Lua instructions that a given message handler is allowed to invoke. If a script exceeds 50 percent of this value, a resource warning alarm generates. The script continues to execute until the script exceeds 100 percent of this value. If the script exceeds 100 percent of the Lua Instruction Threshold value during script loading or initialization script, the SIPNormalizationScriptResourceWarning resource warning alarm gets generated and Cisco Unified Communications Manager closes and disables the script. If the script exceeds 100 percent of the Lua Instruction Threshold value during script execution, the SIPNormalizationScriptResourceWarning alarm gets generated and Cisco Unified Communications Manager performs the action that the System Resource Error Recovery Action field specifies. For example, if you enter 1000 in this field, a warning alarm gets generated if the script exceeds 500 instructions. The script continues to run until it exceeds 1000 instructions. The default value specifies 1000 instructions per message handler invocation.
Reset	Click this button to shut down, then restart, the internal trunk device or devices with which this script associates.
Import File	Click this button to import a script. In the Import File popup window that opens, search for the file by clicking the Browse... button to the right of the Import File field. Use the File Upload popup window to navigate to the file to you want to upload. After you find the file, click the desired filename and click Open. The path to the chosen script file displays in the Import File field of the Import File popup window. To upload the specified script file, click Import File. To close the Import File popup window without taking any action, click Close. After the script file uploads, the Status area of the Import File window tells you the result of the upload. The contents of the script file display in the Content field.

Related Topics

SIP Normalization Script Setup , on page 783

Import SIP Normalization Script

Perform the following procedure to import a SIP normalization script into Cisco Unified Communications Manager.

Procedure

Step 1 Choose**Device** > **Device Settings** > **SIP Normalization Script**.

The Find and List SIP Normalization window displays.

Step 2 Perform one of the followings tasks:

a) To add a new script instance, click the Add New button. The SIP Normalization Script Configuration window displays.

b) To update an existing script instance, locate the appropriate script instance, and click the name of the script that you want to update.

Step 3 To import a script, click the Import File button.
The Import File dialog box displays.

Step 4 Click the Browse button to locate the file that you want to import, and click the Open button.

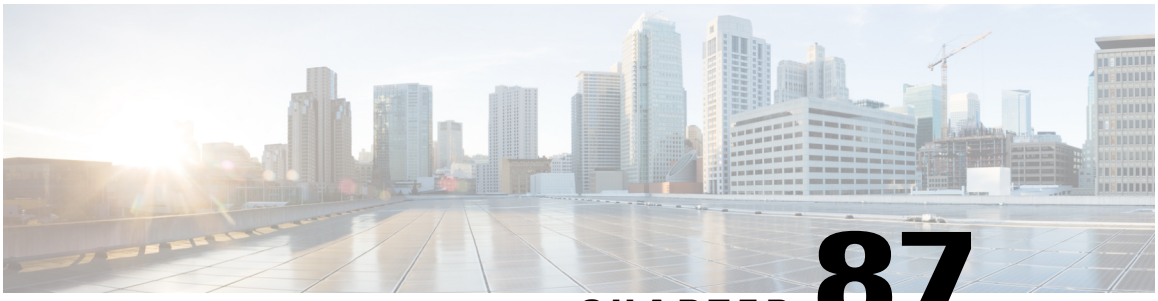
Step 5 Click the Import File button.
The contents of the script file display in the Content field.

Step 6 Modify any of the necessary fields on the window.

Step 7 Click Save and then click Reset.

Related Topics

SIP Normalization Script Setup , on page 783
About SIP Normalization Script Setup , on page 783



CHAPTER 87

Session Description Protocol Transparency

Session Description Protocol Transparency

About Session Description Protocol Transparency Profile Setup

The Session Description Protocol (SDP) Transparency Profile can be configured to selectively allow declarative parameters or to allow all unrecognized parameters to pass from the ingress call leg to the egress call leg.

Session Description Protocol Transparency for Declarative Parameters

The Session Description Protocol Transparency for Declarative Parameters allows the administrator to specify declarative SDP attributes that are not natively supported by Cisco Unified Communications Manager (Unified Communications Manager) to be passed from the ingress call leg to the egress call leg. If the Unified Communications Manager receives attributes that are not explicitly identified by the administrator to send to the egress leg, Unified Communications Manager drops the attribute from the outgoing SDP similar to previous versions of Unified Communications Manager. This feature allows the administrator to identify attributes that are sent to the egress leg in multiple ways, such as configuring all property attributes with a particular name, all value attributes with a particular name, or all value attributes with a specific name and specific value to be passed through. The administrator can also configure all unrecognized attributes to be passed along in the outgoing SDP.

Note SDP Transparency for Declarative Parameters only applies to declarative attributes, not to negotiated attributes.

The Cisco Unified Communications Manager first looks at the name field of an incoming attribute. If the default "Pass all unknown SDP attributes" profile is not used, Unified Communications Manager looks for

an exact match among the attributes designated to be passed through. An exact match between the name field of the attribute arriving on the ingress call leg and the name defined by the administrator occurs only if the two strings are identical (case sensitive). If an exact match is not found, then the attribute is not passed through.

The following are the three attributes that can be configured:

- Property attributes: When an administrator configures a property attribute in the SDP Transparency Profile, the attribute is passed through unless the incoming attribute has a value. If the incoming attribute has a value, Unified Communications Manager categorizes the incoming attribute as a value attribute and it is not passed through.
- Value attributes: When an administrator configures a value attribute of any value in the SDP Transparency Profile to be passed through, the attribute is passed through if it contains a value that includes at least one non-white space character (horizontal tab or space). If the value payload consists of all white space characters, Unified Communications Manager categorizes it as a value attribute and it is not passed through.
- Value attributes configured for value from list: The attribute is passed through only if the value matches one of the five specified values identified by the administrator. If the value does not match one of the five specified values or the there is no value, then the attribute is not passed through.

Session Description Protocol Transparency for All Unrecognized Attributes

An administrator can configure the SDP Transparency Profile to pass all unrecognized SDP attributes from the ingress call leg to the egress call leg when the SDP Transparency Profile is set to "Pass all unknown SDP attributes". To prevent all unrecognized SDP attributes from passing through set the SDP Transparency Profile to "None". The SDP Transparency Profile is selected as "Pass all unrecognized SDP attributes" by default for:

- Standard SIP Profile for Cisco VCS
- Standard SIP Profile for Telepresence Conferencing
- Standard SIP Profile for Telepresence Endpoints

Limitations

This feature does not support attribute names longer than 64 characters.

Errors can also result from non-standard attribute formatting. It is recommended that devices passing SDP to the Unified Communications Manager in the ingress leg conform to RFC 4566 which define attribute syntax as:

- a=<name> for property attributes
- a=<name>:<value> for value attributes

Exceptions

Unknown attributes are not passed through if:

- One or more of Media Termination Point (MTP), Transcoder (Xcoder), RSVP, and/or Trusted Relay Point (TRP) that does not support pass through are allocated.
- Media Termination Point Required is selected.
- The ingress call leg is using Delayed Offer and the egress call leg is using Early Offer.

- Attributes belonging to a media line that is rejected in the process of negotiating media (the port is set to 0) are not passed through.

Session Description Protocol Transparency Profile Settings

The following table describes the available fields in the SDP Profile window.

Table 117: SDP Transparency Profile Settings

Field	Description
Profile Information	
Name	The name of the SDP Transparency Profile **Note** The name must be unique among all SDP Transparency Profiles in the cluster.
Description	The administrator may also include an additional description about this particular profile
Attribute Information	
Name	Name of the attribute that is passed through
Type	Any Value: signifies that the attribute is passed through regardless of the value **Note** If the attribute is not a value attribute, it is not passed through.
	Property: signifies that the attribute is a property attribute and therefore does not have a value Example: a=foo In this example "foo" represents the property to be passed through.
	Value From List: signifies that attributes that only contain specified values are passed through **Note** The administrator is limited to specifying up to five different values. Example: a=foo:bar In this example foo represents the field, and bar represents one of the values that can be assigned.

Set Up Session Description Protocol Transparency Profile

Procedure

Step 1 To set up a new Session Description Protocol (SDP) Transparency Profile from Cisco Unified Communications Manager Administration, select **Device** > **Device Settings** > **SDP Transparency Profile**.
The Find and List SDP Transparency Profile page lists all available SDP Transparency Profiles. You may need to click **Find** or **Clear Filter** if no SDP Transparency Profiles appear on the list. This list may also

contain several SDP Transparency pre-configured profiles that come with Unified Communications Manager. These profiles may be copied and modified to suit your needs.

Step 2 Perform one of the following:

- Select **Add New** to create a new SDP Transparency Profile.
- Open an existing SDP Transparency Profile.

Note You cannot edit the Pass all unknown SDP attributes profile.

Step 3 Enter the Profile Information.
See the SDP Transparency Profile settings table.

Step 4 Enter the Attribute Information.
See the SDP Transparency Profile settings table.

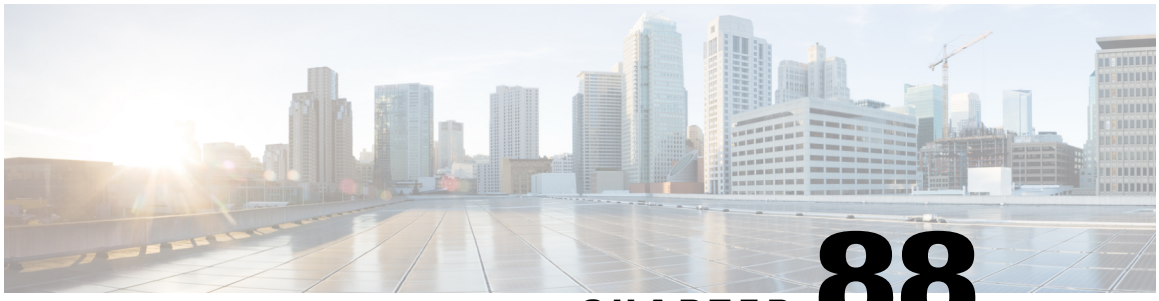
Step 5 Click **Save**.
After the SDP Transparency Profile is ready, it needs to be associated with a SIP Profile.

Step 6 From Cisco Unified Communications Manager Administration, select **Device** > **Device Settings** > **SIP Profile**.

Step 7 On the SIP Profile page, select the desired SDP Transparency Profile from the drop-down list box

Step 8 Click **Save**.
Devices using the SIP Profile must be reset for the changes to take effect.

Note The administrator can configure that all unrecognized attributes are passed to the egress leg by selecting the preconfigured SDP Transparency Profile named **Pass all unknown SDP attributes** from the SDP Transparency Profile drop-down list box. No other configuration is needed to pass through any unrecognized attribute.



CHAPTER 88

Wireless LAN Profile Setup

Wireless LAN Profiles

The Wireless LAN Profile feature removes the need for users to configure Wi-Fi parameters on their phones by allowing the administrator to configure Wi-Fi profiles for them. The user devices can automatically download the Wi-Fi configuration from the Cisco Unified Communications Manager TFTP server, and the configuration is then applied to these devices.

Before you create a Wireless LAN Profile, you can configure a Network Access Profile, which contains information about VPN connectivity and HTTP proxy settings. Create a Network Access Profile from the **Device** > **Device Settings** > **Network Access Profile** menu.

After you create one or more Wireless LAN Profiles, you can add them to a Wireless LAN Profile Group, which you can configure from the **Device** > **Device Settings** > **Wireless LAN Profile Group** menu. You can also specify the enterprise-wide default group.

Note You may add up to four Wireless LAN Profiles to a Wireless LAN Profile Group.

Note The Cisco Desktop Collaboration Experience DX650 (SIP) supports Wireless LAN Profiles.

To use the Wireless LAN Profile feature, consider the following work flow:

1. (Optional) You can configure a Network Access Profile.
2. Create one or more Wireless LAN Profiles, and add a Network Access Profile if you configured one.
3. After you create one or more Wireless LAN Profiles, you can add them to a Wireless LAN Profile Group. You can also specify the enterprise-wide default group.
4. You can add a Wireless LAN Profile Group to a device pool or device-level configuration.
5. After Step 4, TFTP adds the Wireless LAN Profile Group to the existing device configuration file, which the device proceeds to download.

Network Access Profile Settings

The following table displays the Network Access Profile settings.

Table 118: Network Access Profile Settings

Name	Description
Network Access Profile Information	
Name	Enter a name for the Network Access Profile. The value can include 1 to 50 characters, including alphanumeric characters, dot, dash, and underscores.
Description	Enter a description for the Network Access Profile. The description can include up to 63 characters in any language, but it cannot include double quotation marks ("), percentage sign (%), ampersand (&), backslash (\), or angle brackets (<>).
VPN Required	Specify whether virtual private networking (VPN) is required. Available options include: **Off** Specifies that VPN is not required. **On** Specifies that VPN is required. **Default** Uses the system setting.
HTTP Proxy Settings	

Name	Description
Proxy Settings	Controls how the HTTP proxy settings are provided for this Network Access Profile. Available options comprise: **None** No HTTP proxy settings are provided for this Network Access Profile. **Manual** When you select this option, the following fields appear: • Proxy Hostname: Enter an ASCII string of up to 255 characters. • Proxy Port: Enter a proxy port number; the acceptable range is 1-65535 (Default = 8080) • Proxy Requires Authentication: Enter a username and password of up to 64 characters. (Optional.) • Bypass Proxy for: Enter the domain names for which proxy will be bypassed. **Auto** When you select this option, the following fields appear: • Proxy Auto-Config (PAC) Location: Enter the URL for PAC; the URL is limited to 255 characters. • Proxy Requires Authentication: Enter a username and password of up to 64 characters. (Optional.) • Bypass Proxy for: Enter the domain names for which proxy will be bypassed.

Wireless LAN Profile Settings

The following table displays the Wireless LAN Profile settings.

Table 119: Wireless LAN Profile Settings

Name	Description
Wireless LAN Profile Information	
Name	Enter a name for the Wireless LAN Profile. The value can include 1 to 50 characters, including alphanumeric characters, dot, dash, and underscores.

Name	Description
Description	Enter a description for the Wireless LAN Profile. The description can include up to 63 characters in any language, but it cannot include double quotation marks ("), percentage sign (%), ampersand (&), backslash (\), or angle brackets (<>).
Wireless Settings	
SSID (Network Name)	Enter the Service Set Identifier (SSID) for the Wireless LAN Profile. The SSID refers to the wireless network name. When the wireless endpoint is disconnected from the network and sees this SSID, it attempts to join that wireless LAN using the settings from this profile. The SSID can include up to 32 ASCII characters.
Frequency Band	Select one of the following frequency band settings from the drop-down list box: **Auto** The wireless endpoint automatically chooses a frequency band. Auto is the default setting. **2.4 GHz** The wireless endpoint uses the 2.4 GHz frequency band. **5 GHz** The wireless endpoint uses the 5 GHz frequency band.
User Modifiable	Select one of the following user modifiable options from the drop-down list box: **Allowed** Indicates that the user can change any profile settings. Allowed is the default setting. **Disallowed** Indicates that the user cannot make any changes to the profile. **Restricted** Indicates that users can change the username and password if they use an authentication method that requires username and password, but not any other profile settings.
Authentication Settings	

Name	Description
Authentication Method	Specify the authentication method that is used to secure access to the Wi-Fi network. Depending on the method you choose, a password, passphrase, or key field appears so that you can provide the credentials that are required to join this Wi-Fi network. The following authentication methods are available: **EAP-FAST** (Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling) This method requires a username and password (up to 64 characters). **PEAP-MSCHAPV2** (Protected Extensible Authentication Protocol - Microsoft Challenge Handshake Authentication Protocol version 2) This method requires a username and password (up to 64 characters). **PEAP-GTC** (Protected Extensible Authentication Protocol - Generic Token Card) This method requires a username and password (up to 64 characters). **PSK** (Pre-Shared Key) This method requires a passphrase to be entered, which is a 8-63 ASCII character string or a 64 hexadecimal character string. **WEP** (Wired Equivalent Privacy) This method requires a WEP Key, which is either a 5 or 13 ASCII character string or a 10 or 26 HEX character string. **None** This method requires no authentication.
Network Access Settings	
Network Access Profile	Specify the Network Access Profile. The Network Access Profile contains information about VPN connectivity and HTTP proxy settings. After you select a Network Access Profile, you can click **View Details** and a popup window will appear with the Network Access Profile settings.

Wireless LAN Profile Group Settings

The following table displays the Wireless LAN Profile Group settings.

Table 120: Wireless LAN Profile Group Settings

Name	Description
Wireless LAN Profile Group Information	
Name	Enter a name for the Wireless LAN Profile Group. The value can include 1 to 50 characters, including alphanumeric characters, dot, dash, and underscores.
Description	Enter a description for the Wireless LAN Profile Group. The description can include up to 63 characters in any language, but it cannot include double quotation marks ("), percentage sign (%), ampersand (&), backslash (\), or angle brackets (<>).
Profiles for this Wireless LAN Profile Group	
Available Profiles	Specifies the profiles that are available to be added to the Wireless LAN Profile Group. You can move profiles that are listed here to the Selected Profiles field. Highlight the ones you want to move, then click the down arrow.
Selected Profiles	The profiles that you selected to be part of this Wireless LAN Profile Group. The profiles are listed in priority order. If the wireless endpoint sees more than one network SSID for which it has a profile definition, it first attempts to join the one with the highest priority. **Note** You can add up to four profiles to a Wireless LAN Profile Group.

Create Network Access Profile

Procedure

Step 1 From Cisco Unified Communications Manager Administration, select **Device** > **Device Settings** > **Network Access Profile**

Step 2 Click **Add New**.
The Network Access Profile settings window appears.

Step 3 Enter Network Access Profile settings.

Step 4 Click **Save**.

The Network Access Profile is created.

What to Do Next

- Create a Wireless LAN Profile
- Add this Network Access Profile to a Wireless LAN Profile

Create Wireless LAN Profile

Before You Begin

Optionally, create a Network Access Profile to associate to a Wireless LAN Profile.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, select **Device** > **Device Settings** > **Wireless LAN Profile**

Step 2 Click **Add New**.
The Wireless LAN Profile settings window appears.

Step 3 Enter the Wireless LAN Profile settings.

Step 4 Click **Save**.
The Wireless LAN Profile is created.

What to Do Next

- Create another Wireless LAN Profile
- Combine Wireless LAN Profiles into a Wireless LAN Profile Group

Create Wireless LAN Profile Group

Procedure

Step 1 From Cisco Unified Communications Manager Administration, select **Device** > **Device Settings** > **Wireless LAN Profile Group**

Step 2 Click **Add New**.
The Wireless LAN Profile Group settings window appears.

Step 3 Enter the Wireless LAN Profile Group settings.

Step 4 Click **Save**.

The Wireless LAN Profile is created.

What to Do Next

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

Link Wireless LAN Profile Group with Device

You can link a Wireless LAN Profile Group at the device or device pool level.

Note If you link a Wireless LAN Profile Group at the device and device pool level, Cisco Unified Communications Manager uses the device pool level.

Before You Begin

Create a Wireless LAN Profile Group.

Procedure

Step 1 Perform one of the following actions:

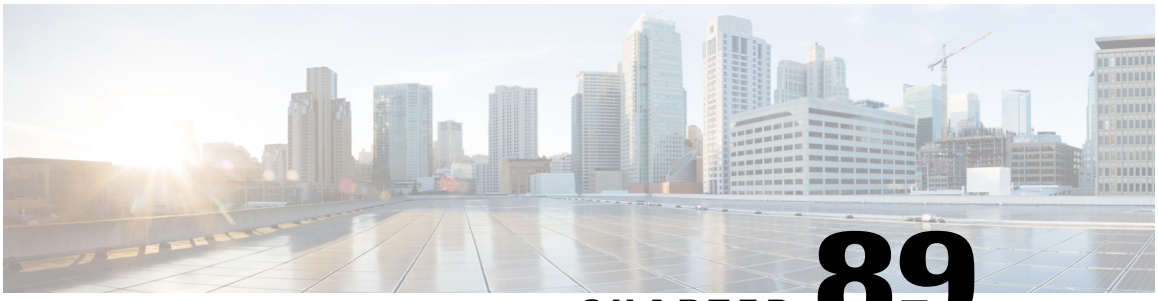
- Select **Device** > **Phone**.
- Select **System** > **Device Pool**

Step 2 Perform one of the following actions:

- Find an existing device or create a new device.
- Find an existing device pool or create a new device pool.

Step 3 Select a Wireless LAN Profile Group from the drop-down list box.

Step 4 Select **Save**.
The Wireless LAN Profile Group is linked to the device or Device Pool.



CHAPTER 89

Wi-Fi Hotspot Profile Setup

This chapter provides information on configuring Wi-Fi Hotspot Profiles for desk phones.

About Wi-Fi Hotspot Profile Setup

The Wi-Fi Hotspot Profile feature allows users to use their desk phones to provide a Wi-Fi Hotspot, so that they can connect a Wi-Fi device such as a tablet or a mobile phone to the network through the desk phone. The desk phones can automatically download the Wi-Fi Hotspot configuration from the Cisco Unified Communications Manager, and the configuration is then applied to these devices.

To use the Wi-Fi Hotspot Profile feature, you must configure a Wi-Fi Hotspot Profile on the Cisco Unified Communications Manager administrative interface. After the profile is created, you must associate it with a phone. To associate a Wi-Fi Hotspot Profile to a phone, you can configure the profile at the Enterprise Parameters, Common Phone Profile, or individual phone level. Configuring a Wi-Fi Hotspot Profile on the Phone page overrides the Enterprise Parameters and Common Phone Profile settings. After the desk phones download the TFTP configuration file, the users can enable Wi-Fi Hotspot and connect the Wi-Fi devices.

Important No endpoints currently support the Wi-Fi Hotspot Profile feature.

By default, the Wi-Fi Hotspot Profile feature is disabled in Cisco Unified Communications Manager. If you want to enable the Wi-Fi Hotspot for a desk phone, you can enable the Wi-Fi Hotspot feature at the Enterprise Phone Configuration, Common Phone Profile or individual phone level and then apply a Wi-Fi Hotspot Profile to the Enterprise Parameters, Common Phone Profile or individual phone level. The Wi-Fi Hotspot setting on the Phone page overrides the setting on the Common Phone Profile page, which overrides the setting on the Enterprise Phone Configuration page.

Wi-Fi Hotspot Profile Settings

The following table displays the Wi-Fi Hotspot Profile settings.

Name	Description
Wi-Fi Hotspot Profile Information	
Name	Enter a name for the Wi-Fi Hotspot Profile. The value can include 1 to 50 characters, including alphanumeric characters, dots, dashes, and underscores.
Description	Enter a description for the Wi-Fi Hotspot Profile. The description can include up to 50 characters in any language, but it cannot include double quotation marks ("), percentage sign (%), ampersand (&), backslash (\), or angle brackets (<>).
User Modifiable	Select one of the following options from the drop-down list box: **Allowed** Indicates that the user can change any profile settings. This is the default setting. **Disallowed** Indicates that the user cannot make any changes to the profile. **Restricted** Indicates that some settings (Enable/Disable, SSID Suffix, PSK Passphrase, WEP Key) can be modified, but other settings (Frequency Band, Authentication Method, Authentication Server, Port, Shared Secret) cannot be modified.
Wireless Settings	
SSID (Network Name) Prefix	Enter the Service Set Identifier (SSID) Prefix for the Wi-Fi Hotspot Profile. The SSID Prefix that you enter here is combined with the SSID suffix, which is generated automatically based on the local endpoint information, to create a unique SSID for the Wi-Fi Hotspot of the phone. The value can include 1 to 20 alphanumeric characters.

Name	Description
Frequency Band	Select one of the following frequency band settings from the drop-down list box: **Auto** The profile automatically chooses a frequency band. **2.4 GHz** The profile automatically chooses 2.4 GHz as the frequency band. **5 GHz** The profile automatically chooses 5 GHz as the frequency band. **Note** If you select the Auto option, a single channel will be used to serve clients because dual-band operation is currently not supported.
Authentication	

Name	Description
Authentication Method	

Name	Description
	Specify the authentication method that is used to secure access to the Wi-Fi Hotspot. Depending on the method you choose, a PSK Passphrase, WEP key, or password description field appears so that you can provide the credentials that are required to connect to this Wi-Fi Hotspot. The following authentication methods are available: **EAP-FAST** (Extensible Authentication Protocol - Flexible Authentication through Secure Tunneling) If you choose this method, the Wi-Fi client that is connecting to the Wi-Fi Hotspot must be configured with a valid username and password. **PEAP-MSCHAPV2** (Protected Extensible Authentication Protocol - Microsoft Challenge Handshake Authentication Protocol Version 2) If you choose this method, the Wi-Fi client that is connecting to the Wi-Fi Hotspot must be configured with a valid username and password. **PEAP-GTC** (Protected Extensible Authentication Protocol - Generic Token Card) If you choose this method, the Wi-Fi client that is connecting to the Wi-Fi Hotspot must be configured with a valid username and password. **WPA2-PSK** (Wi-Fi Protected Access Pre-Shared Key) This method uses Advanced Encryption Standard (AES) encryption. If you select this method, you must enter a passphrase, which is an 8 to 63 ASCII character string or a 64 HEX character string. **WPA-PSK** This method uses Temporal Key Integrity

Name	Description
	Protocol (TKIP) encryption. If you select this method, you must enter a passphrase, which is an 8 to 63 ASCII character string or a 64 HEX character string. **WEP** (Wired Equivalent Privacy) WEP requires a WEP Key, which is either a 5 or 13 ASCII character string or a 10 or 26 HEX character string. **None** No authentication is required.
Server Settings	
Host Name/IP Address	Enter the DNS hostname (up to 255 characters) or IP address of the authentication server.
Port	Enter the port number. 1812 is the default port. The accepted port range is 1-65535.
Shared Secret	Enter the shared secret. The value can include 1 to 32 characters. The shared secret is used to authenticate against the authentication server. The shared secret specified in the Wi-Fi Hotspot Profile must match with the shared secret specified in the authentication server.
Note The server settings are displayed only if you select the authentication method as EAP-FAST, PEAP-MSCHAPv2, or PEAP-GTC.	

Create Wi-Fi Hotspot Profile

Use the following procedure to create a new Wi-Fi Hotspot Profile. After you create a Wi-Fi Hotspot Profile, you can apply it at the Enterprise Parameters, Common Phone Profile or individual phone level.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, select **Device** > **Device Settings** > **Wi-Fi Hotspot Profile**.

Step 2 Click **Add New**.

The Wi-Fi Hotspot Profile settings window appears.

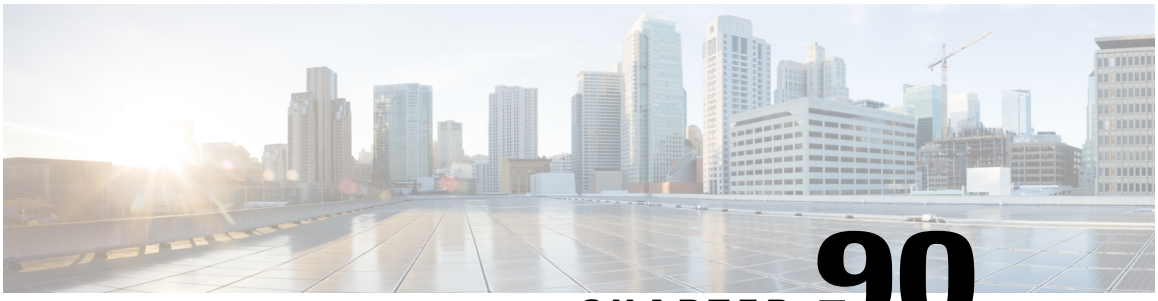
Step 3 Enter the Wi-Fi Hotspot Profile settings.

Step 4 Click **Save.**
The Wi-Fi Hotspot Profile is created.

Repeat this procedure for each Wi-Fi Hotspot Profile that you want to create.

Related Topics

Enterprise parameter setup
Common Phone Profile Settings , on page 772
Phone Settings, on page 583



CHAPTER 90

Other Device Menu Options

This chapter provides brief descriptions of selected Device menu options that other documents describe in greater detail. A pointer to the document that contains more details is provided for each Device menu option.

Remote Destination Setup

In Cisco Unified Communications Manager Administration, use the **Device** > **Device Settings** > **Remote Destination** menu path to configure remote destinations.

The Cisco Unified Mobility Cisco Unified Mobility feature allows users to manage business calls using a single phone number and pick up in-progress calls on the desktop phone and mobile phone. Mobile Voice Access is the associated integrated voice response (IVR) system, which allows users to turn Cisco Unified Mobility on or off and to initiate calls from a mobile phone or other remote phone as if the call were initiated from the desktop phone.

Remote destinations represent the mobile (or other) phones that are able to accept transfers from the user desktop phone and can be used to initiate calls using Mobile Voice Access.

For more information on Cisco Unified Mobility, Mobile Voice Access, and other Cisco Unified Mobility features, as well as how to configure remote destinations, see the *Cisco Unified Communications Manager Features and Services Guide*.

Remote Destination Profile Setup

In Cisco Unified Communications Manager Administration, use the **Device** > **Device Settings** > **Remote Destination Profile** menu path to configure remote destination profiles.

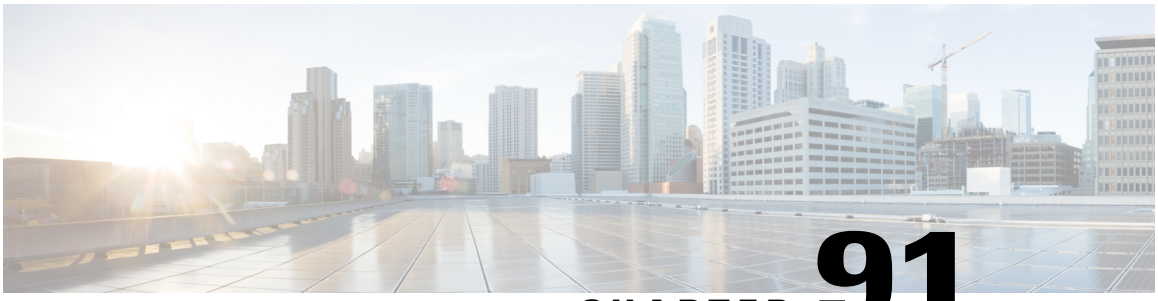
Cisco Unified Mobility allows users to manage business calls using a single phone number and pick up in-progress calls on the desktop phone and cellular phone. Mobile Voice Access is the associated integrated voice response (IVR) system, which allows users to turn Cisco Unified Mobility on or off and to initiate calls from a cellular phone or other remote phone as if the call were initiated from the desktop phone.

A user remote destination profile contains the parameters that apply to all the remote destinations (cellular or other phones) available for in-progress call transfers and initiation of calls by way of Mobile Voice Access.

For more information on Cisco Unified Mobility and Mobile Voice Access and how to configure remote destination profiles, see the *Cisco Unified Communications Manager Features and Services Guide*.

PART VII

Application Setup



CHAPTER 91

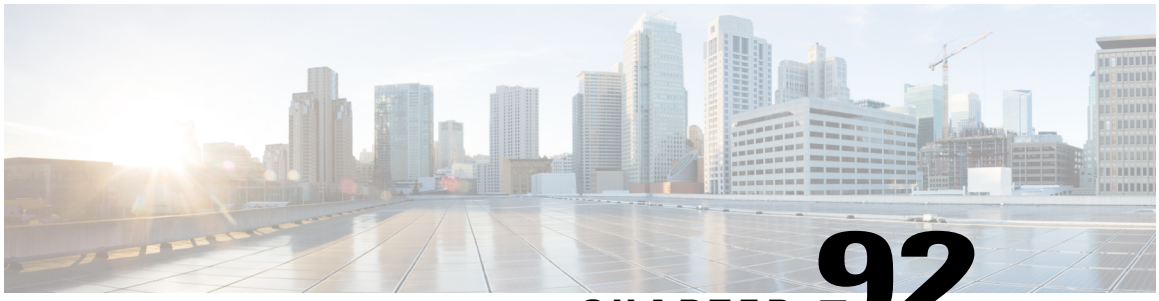
Cisco Unified Communications Manager Assistant Configuration Wizard

Cisco Unified Communications Manager Assistant Configuration Wizard

With the Cisco Unified Communications Manager Assistant Configuration Wizard, Cisco Unified Communications Manager Assistant configuration takes less time and eliminates errors. The partitions, calling search spaces, route point, and translation pattern automatically get created when the administrator successfully runs and completes the configuration wizard. The wizard also creates BAT templates for the Cisco Unified Communications Manager Assistant manager phone, the Cisco Unified Communications Manager Assistant 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.

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.

For more information on how to use the Cisco Unified Communications Manager Assistant Configuration Wizard, see the *Cisco Unified Communications Manager Features and Services Guide*.



CHAPTER 92

Plug-In Setup

This chapter provides information to install and update Application plug-ins for the Cisco Unified Communications Manager.

Update Plugin URL Settings

Application plug-ins extend the functionality of Cisco Unified Communications Manager. For example, the JTAPI plug-in allows a computer to host applications that access the Cisco Unified Communications Manager via the Java Telephony Application Programming Interface (JTAPI).

The following table describes the Update Plugin URL configuration settings.

Table 121: Update Plugin URL Configuration Settings

Field	Description
Plugin Settings	
Plugin Name	The plug-in name automatically displays.
URL	The existing URL automatically displays.
Custom URL	Use only alphanumeric characters for the custom URL.
Show Plugin on User Option Pages	Check this check box to show the plug-in on the user option window.

Install Plug-Ins

Perform the following procedure to install any plug-in.

Tip After Cisco Unified Communications Manager upgrades, you must reinstall all plug-ins except the Cisco CDR Analysis and Reporting plug-in.

Tip Before you install any plug-ins, disable all intrusion detection or antivirus services that run on the server where you plan to install the plug-in.

Procedure

Step 1 Choose **Application** > **Plugins**.
The Find and List Plugins 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) From the third drop-down list box, select Application Menu, Installation, User Menu, or Telecaster Menu.
d) 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 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 To reverse the sort order, click the up or down arrow, if available, in the list header.

Step 4 Click Download for the plug-in you want to install.

Update Plugin URL

During the Cisco Unified Communications Manager install process, records that are added to the Plugins table specify the URLs that the Administration applications use to build the Application drop-down menu. The domain name server (DNS) provides the basis for the URL that is constructed at installation time. If the DNS changes, the URL does not get updated.

Perform the following procedure to update the URL of the Plugin URL.

Procedure

Step 1 Choose **Application** > **Plugins**.
The Find and List Plugins window displays. Display the list of available plug-ins.

Step 2 Click the Plugin name that you want to update.
The Update Plugin URL window displays.

Step 3 Enter the update plugin URL configuration settings.

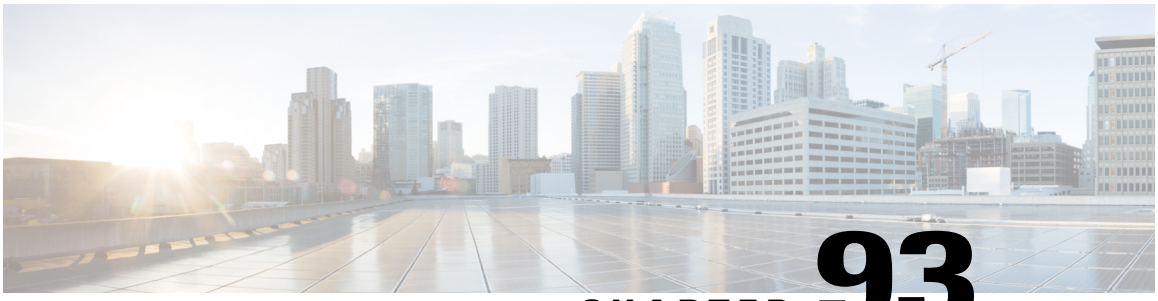
Step 4 Click the Save icon that displays in the tool bar in the upper, left corner of the window (or click the Save button that displays at the bottom of the window) to update and save the URL.

Related Topics

Update Plugin URL Settings, on page 815
Install Plug-Ins , on page 816

PART VIII

User Management Setup



CHAPTER 93

Credential Policy Default Setup

This chapter provides information to configure credential policies.

About Credential Policy Default Setup

In Cisco Unified Communications Manager Administration, use the **User Management** > **Credential Policy Default** menu path to configure credential policy defaults.

This chapter describes how to assign default credential policies to a credential group.

The Credential Policy Default window provides options to change the default credential policy assignment for a user and credential type (for example, end user PINs). At installation, Cisco Unified Communications Manager assigns the system Default Credential Policy to end user passwords, end user PINS, and application user passwords. The system applies the application password that you configured at installation to all application users. You can assign a new default credential policy and configure new default credentials after installation.

Credential Policy Defaults Configuration Tips

The system provides the default credential policy to facilitate installs and upgrades. The default credential policy settings in Table 122: Credential Policy Default Settings , on page 822 differ from the credential policy defaults settings that are used to add a new credential policy.

Note The system does not support empty (null) credentials. If your system uses LDAP authentication, you must configure end user default credentials immediately after installation, or logins will fail.

You can also assign a new user credential policy, manage user authentication events, or view credential information for a user in the user configuration windows.

Related Topics

Manage Application User Credential Information , on page 837
Manage End User Credential Information , on page 853

Credential Policy Default Settings

The following table describes the credential policy default settings.

Table 122: Credential Policy Default Settings

Field	Description
Credential User	This field displays the user type for the policy that you selected in the Find and List Credential Policy Defaults window. You cannot change this field.
Credential Type	This field displays the credential type for the policy that you selected in the Find and List Credential Policy Defaults window. You cannot change this field.
Credential Policy	Choose a credential policy default for this credential group. The list box displays the predefined Default Credential Policy and any credential policies that you created.
Change Credential	Enter up to 127 characters to configure a new default credential for this group.
Confirm Credential	For verification, reenter the login credential that you entered in the Change Credential field.
User Cannot Change	Check this check box to block users that are assigned this policy from changing this credential. You cannot check this check box when User Must Change at Next Login is checked. The default setting for this check box specifies unchecked.
User Must Change at Next Login	Check this check box to require users that are assigned this policy to change this credential at next login. Use this option after you assign a temporary credential. You cannot check this check box when the User Cannot Change check box is checked. The default setting for this check box specifies checked.
Does Not Expire	Check this check box to block the system from prompting the user to change this credential. You can use this option for low-security users or group accounts. If this check box is checked, the user can still change this credential at any time. When this check box is unchecked, the expiration setting in the associated credential policy applies. The default setting for this check box specifies unchecked.

Related Topics

Credential Policy Default Setup , on page 821
Credential Policy Setup , on page 825

Assign and Set Up Credential Policy Defaults

This section describes how to assign a new credential policy and new default credentials to a credential group. At installation, the system assigns a default credential policy to the credential groups.

Note Upgrades from 5.x releases automatically migrate application and end user passwords and PINs.

Before You Begin

To assign a default credential policy other than the predefined Default Credentials Policy, you must first create the policy.

Procedure

Step 1 Choose **User Management** > **Credential Policy Default**.
The Find and List Find and List Credential Policy Defaults window displays.

Step 2 Click the list item to change.
The Credential Policy Default Configuration window displays with the current settings.

Step 3 Enter the appropriate settings, as described in Table 122: Credential Policy Default Settings , on page 822, using these guidelines:

a) To change the applied credential policy, select the policy from the drop-down list box.
b) To change the default credential, enter and confirm the new credential in the appropriate fields.
c) To change credential requirements, check or uncheck the appropriate check boxes.

Step 4 Click the Save button or the Save icon.

What to Do Next

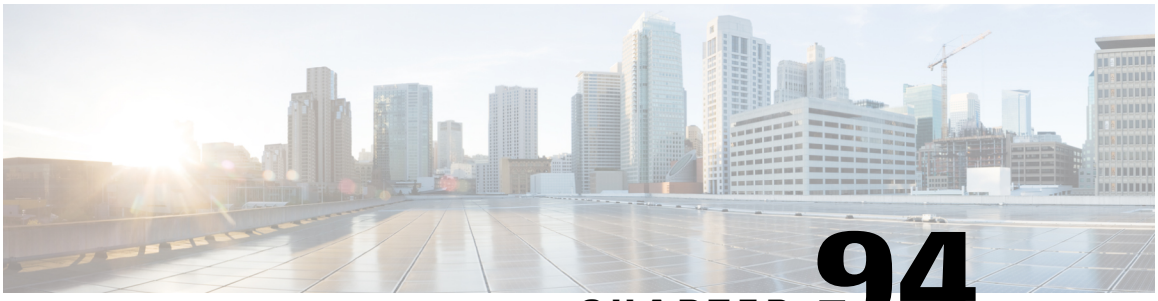
You can assign a new user credential policy, manage user authentication events, view credential information for a user, or configure a unique password for the user.

The Bulk Administration Tool (BAT) allows administrators to define common credential parameters, such as passwords and PINs, for a group of users in the BAT User Template. See the Cisco Unified Communications Manager Bulk Administration Guide for more information.

End users can change PINs at the phone user pages; end users can change passwords at the phone user pages when LDAP authentication is not enabled. See the documentation for your Cisco Unified IP Phone for more information.

Related Topics

Credential Policy Setup , on page 825
Change Application User Password , on page 837
Manage Application User Credential Information , on page 837
Change End User Password , on page 852
Change End User PIN , on page 852
Manage End User Credential Information , on page 853



CHAPTER 94

Credential Policy Setup

This chapter provides information to configure credential policies.

About Credential Policy Setup

In Cisco Unified Communications Manager Administration, use the **User Management** > **Credential Policy** menu path to configure credential policies.

The Credential Policy Configuration window in Cisco Unified Communications Manager Administration allows you to configure credential policies to secure user accounts.

A policy comprises a set of rules that controls access to a system or network resource. A credential policy defines password requirements and account lockouts for user accounts. Credential policies that are assigned to user accounts control the authentication process in Cisco Unified Communications Manager. After you add a credential policy, you can assign the new policy as the default policy for a credential type or to an individual application or end user.

At installation, Cisco Unified Communications Manager assigns a static credential policy to end user PINs and to application and end user passwords. The policy contains settings for failed login resets, lockout durations, expiration periods, and credential requirements. The Credential Policy Configuration window allows you to configure new credential policies for your system or site. You cannot change the static policy.

Credential Policies Configuration Tips

The system provides trivial credential checks to disallow credentials that are easily hacked. You enable trivial credential checks by checking the Check for Trivial Passwords check box in the Credential Policy Configuration window.

Passwords can contain any alphanumeric ASCII character and all ASCII special characters. A non-trivial password meets the following criteria:

- Must contain three of the four allowable characteristics: uppercase character, lowercase character, number, symbol.

- Must not use a character or number more than three times consecutively.
- Must not repeat or include the alias, username, or extension.
- Cannot consist of consecutive characters or numbers (for example, passwords such as 654321 or ABCDEFG)

PINs can contain digits (0-9) only. A non-trivial PIN meets the following criteria:

- Must not use the same number more than two times consecutively.
- Must not repeat or include the user extension or mailbox or the reverse of the user extension or mailbox.
- Must contain three different numbers; for example, a PIN such as 121212 is trivial.
- Must not match the numeric representation (that is, dial by name) for the first or last name of the user.
- Must not contain groups of repeated digits, such as 408408, or patterns that are dialed in a straight line on a keypad, such as 2580, 159, or 753.

Tip You cannot modify the system Default Credential Policy.

Next Steps

You can assign the new credential policy as a default policy for a credential type, or to individual users.

Related Topics

Assign and Set Up Credential Policy Defaults , on page 823
Manage Application User Credential Information , on page 837
Manage End User Credential Information , on page 853

Credential Policy Deletion

Note You cannot delete a credential policy if it is assigned as the default policy for end user passwords, end user PINS, or application user passwords.

To find out which default policies use the credential policy, choose Dependency Records from the Related Links drop-down list box in the Credential Policy Configuration window and click Go.

If the dependency records feature is not enabled for the system, the dependency records summary window displays a message that shows the action that you can take to enable the dependency records. The message also displays information about high CPU consumption that is related to the dependency records feature.

If you attempt to delete a credential policy that is in use, a message displays. To delete a credential policy that is currently in use, you must either choose a different credential policy for the user or create and assign a new policy.

Related Topics

About Credential Policy Setup , on page 825

Access Dependency Records , on page 982

Credential Policy Settings

The following table describes the credential policy settings.

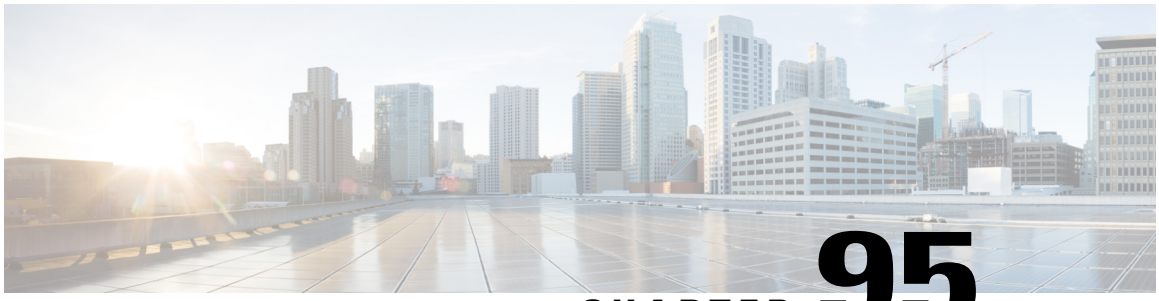
Table 123: Credential Policy Settings

Field	Description
Display Name	Specify the credential policy name. Enter up to 64 characters, except for quotation marks. Do not enter tab.
Failed Logon / No Limit for Failed Logons	Specify the number of allowed failed login attempts. When this threshold is reached, the system locks the account. Enter a number in the range 1-100. To allow unlimited failed logins, enter 0 or check the No Limit for Failed Logons check box. Uncheck the check box to enter a value greater than 0. The default setting specifies 3.
Reset Failed Logon Attempts Every	Specify the number of minutes before the counter is reset for failed login attempts. After the counter resets, the user can try logging in again. Enter a number in the range 1-120. The default setting specifies 30.
Lockout Duration / Administrator Must Unlock	Specify the number of minutes an account remains locked when the number of failed login attempts exceeds the specified threshold. Enter a number in the range 1-1440. Enter 0 or check the Administrator Must Unlock check box, so accounts will remain locked until an administrator manually unlocks them. Uncheck the check box to enter a value greater than 0. The default setting specifies 30.
Minimum Duration Between Credential Changes	Specify the number of minutes that are required before a user can change credentials again. Enter 0 to allow a user to change credentials at any time. Uncheck the check box to enter a value greater than 0. The default setting specifies 0.
Credential Expires After / Never Expires	Specify the number of days before a credential will expire. Enter a number in the range 1-365.To allow credentials to never expire, enter 0 or check the Never Expires check box. Uncheck the check box to enter a value greater than 0. Use the 0 option for low-security accounts or multiple user accounts, for example. The default setting specifies 180.
Minimum Credential Length	Specify the minimum length for user credentials (password or PIN). Do not enter 0 because blank passwords are not allowed. The default setting specifies 8. The minimum setting must equal at least 1.

Field	Description
Stored Number of Previous Credentials	Specify the number of previous user credentials to store. This setting prevents a user from configuring a recently used credential that is saved in the user list. Enter a number in the range 0-25. If no previous credentials should be stored, enter 0. The default setting specifies 12.
Inactive Days Allowed	Specify the number of days that a password can remain inactive before the account gets locked. Enter a number in the range 0-5000. The default setting specifies 0.
Expiry Warning Days	Enter a number in the range 0-90 to specify the number of days before a user password expires to start warning notifications. The default setting specifies 0.
Check for Trivial Passwords	Check this check box to require the system to disallow credential that are easily hacked, such as common words, repeated character patterns, and so on. The default setting checks the check box.

Related Topics

Credential Policy Setup , on page 825



CHAPTER 95

Application User Setup

This chapter provides information on managing application user information.

About Application User Setup

In Cisco Unified Communications Manager Administration, use the **User Management** > **Application User** menu path to configure application users.

The Application User Configuration window in Cisco Unified Communications Manager Administration allows the administrator to add, search, display, and maintain information about Cisco Unified Communications Manager application users.

Application Users Configuration Tips

Click **Add New** to set up a new application user. Complete the fields in the Application User Configuration window to configure settings for the application user. For details, see Application User Settings , on page 831.

Note Installation provides a set of default application users for Cisco Unified Communications Manager.

Note If you are adding an administrator account for Cisco Unity or Cisco Unity Connection, you must use the same user name and password that you defined in Cisco Unity and Cisco Unity Connection Administration.The user ID provides authentication between Cisco Unity or Cisco Unity Connection and Cisco Unified Communications Manager Administration. See the applicable Cisco Unified Communications Manager Integration Guide for Cisco Unity or Cisco Unity Connection.

You can configure a Cisco Unified Communications Manager Administration application user as a Cisco Unity or Cisco Unity Connection user by using the Create a Cisco Unity Application User option in the Application User Configuration window. You can then configure any additional settings in Cisco Unity or Cisco Unity Connection Administration.

To show the user privilege report for this application user, from the Related Links drop-down list box, choose User Privilege Report and click Go.

The User Privilege window displays for this application user.

After you display the user privilege report for this application user, you can return to the Application User Configuration window for this application user. From the Related Links drop-down list box in the User Privilege window, choose Back to Application User and click Go.

Next Steps

You can associate devices with this application user, manage the application user credentials, and add an administrator user to Cisco Unity or Cisco Unity Connection.

Related Topics

Add Administrator User to Cisco Unity or Cisco Unity Connection , on page 835
Manage Application User Credential Information , on page 837
Associate Devices to Application Users , on page 839
View User Roles, Access Control Groups, and Permissions , on page 875

Add Application User

To add an application user, perform the following steps:

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **Application User**.

Step 2 Click **Add New**.

Step 3 Complete the fields in the Application User Configuration window and click **Save**. For field descriptions, see Application User Settings , on page 831.

Step 4 Click **Save**.

What to Do Next

To associate a device to an application user, see Associate Devices to Application Users , on page 839.

Application User Deletion

Before deleting the application user, determine whether the devices or profiles that are associated with the end user need to be removed or deleted.

You can view the profiles and permissions that are assigned to the application user from the CAPF Information and Permissions Information areas of the Application User Configuration window. You can also choose Dependency Records from the Related Links drop-down list box in the Application User Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message.

Next Steps

If this user is configured in Cisco Unity or Cisco Unity Connection, the user association to Cisco Unified Communications Manager is broken when you delete the user in Cisco Unified Communications Manager Administration. You can delete the orphaned user in Cisco Unity or Cisco Unity Connection Administration. See the applicable User Moves, Adds, and Changes Guide for Cisco Unity Connection for more information. See the applicable System Administration Guide for Cisco Unity for more Cisco Unity information.

Related Topics

Access Dependency Records , on page 982

Application User Settings

The following table describes the application user settings.

Table 124: Application User Settings

Field	Description
Application User Information	
User ID	Enter a unique application user identification name. Cisco Unified Communications Manager allows you to modify an existing user ID (provided synchronization with the LDAP server is not enabled).
Password	Enter alphanumeric or special characters for the application user password. You must enter at least the minimum number of characters that are specified in the assigned credential policy. **Note** Do not use special characters when you create an AXL password for an application user.
Confirm Password	Enter the user password again.
Digest Credentials	Enter a string of alphanumeric characters. Cisco Unified Communications Manager uses the digest credentials that you specify here to validate the SIP user agent response during a challenge to the SIP trunk. For information on digest authentication, see the *Cisco Unified Communications Manager Security Guide*.

Field	Description
Confirm Digest Credentials	To confirm that you entered the digest credentials correctly, enter the credentials in this field.
Edit Credential	The Edit Credential button displays after you add this user to the database. Click this button to manage credential information for this user.
Presence Group	Configure this field with the Presence feature. **Note** If you are not using this application user with presence, leave the default (None) setting for presence group. From the drop-down list box, choose a Presence group for the application user. The group selected specifies the destinations that the application user, such as IPMASysUser, can monitor. The Standard Presence group gets configured at installation. Presence groups configured in Cisco Unified Communications Manager Administration also appear in the drop-down list box. Presence authorization works with presence groups to allow or block presence requests between groups. See the *Cisco Unified Communications Manager Features and Services Guide* for information about configuring permissions between groups.
Accept Presence Subscription	Configure this field with the Presence feature for presence authorization. If you enabled application-level authorization in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified Communications Manager performs application-level authorization. Check this check box to authorize Cisco Unified Communications Manager to accept presence requests that come from this SIP trunk application user. If you check this check box in the Application User Configuration window and do not check the Enable Application Level Authorization check box in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified Communications Manager sends a 403 error message to the SIP user agent that is connected to the trunk. For more information on authorization, see the *Cisco Unified Communications Manager Security Guide*.

Field	Description
Accept Out-of-Dialog REFER	If you enabled application-level authorization in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified Communications Manager performs application-level authorization. Check this check box to authorize Cisco Unified Communications Manager to accept Out-of-Dialog REFER requests that come from this SIP trunk application user. For example, to use SIP-initiated transfer features and other advanced transfer-related features, you must authorize Cisco Unified Communications Manager to accept incoming Out-of-Dialog REFER requests for this application user. If you check this check box in the Application User Configuration window and do not check the Enable Application Level Authorization check box in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified Communications Manager sends a 403 error message to the SIP user agent that is connected to the trunk. For more information on authorization, see the *Cisco Unified Communications Manager Security Guide*.
Accept Unsolicited Notification	If you enabled application-level authorization in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified Communications Manager performs application-level authorization. Check this check box to authorize Cisco Unified Communications Manager to accept unsolicited notifications that come from this SIP trunk application user. For example, to provide MWI support, you must authorize Cisco Unified Communications Manager to accept incoming unsolicited notifications for this application user. If you check this check box in the Application User Configuration window and do not check the Enable Application Level Authorization check box in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified Communications Manager sends a 403 error message to the SIP user agent that is connected to the trunk. For more information on authorization, see the *Cisco Unified Communications Manager Security Guide*.

Field	Description
Accept Replaces Header	If you enabled application-level authorization in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified Communications Manager performs application-level authorization. Check this check box to authorize Cisco Unified CM to accept header replacements in messages from this SIP trunk application user. For example, to transfer an external call on a SIP trunk to an external device or party, as in attended transfer, you must authorize Cisco Unified CM to accept SIP requests with replaces header in REFERS and INVITES for this application user. If you check this check box in the Application User Configuration window and do not check the Enable Application Level Authorization check box in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified CM sends a 403 error message to the SIP user agent that is connected to the trunk. For more information on authorization, see the *Cisco Unified Communications Manager Security Guide*.
Device Information	
Available Devices	This list box displays the devices that are available for association with this application user. To associate a device with this application user, select the device and click the Down arrow below this list box. If the device that you want to associate with this application user does not display in this pane, click one of these buttons to search for other devices: • Find more Phones—Click this button to find more phones to associate with this application user. The Find and List Phones window displays to enable a phone search. • Find more Route Points—Click this button to find more route points to associate with this application user. The Find and List CTI Route Points window displays to enable a CTI route point search. • Find more Pilot Points—Click this button to find more pilot points to associate with this application user. The Find and List Pilot Points window displays to enable a pilot point search.
Controlled Devices	This field lists the devices that are associated with the application user. To remove a device, select the device name and click the Up arrow above this list box. To add a device, select a device in the Available Devices list box and click the Down arrow.
CAPF Information	

Field	Description
Associated CAPF Profiles	This pane displays the Instance ID from the CAPF Profile that you configured for this user. To view or update the profile, double-click the Instance ID or click the Instance ID to highlight it; then, click View Details. The Application User CAPF Profile Configuration window displays with the current settings. For information on how to configure the Application User CAPF Profile, see the *Cisco Unified Communications Manager Security Guide*.
Permissions Information	
Groups	This list box displays after an application user record has been saved. The list box displays the groups to which the application user belongs. To add the user to one or more user groups, click the Add to Access Control Group button. The Find and List Access Control Groups window opens as a separate window. Locate the groups to which you want to add the user, click in the check boxes beside those groups, and click Add Selected at the bottom of the window. The Find and List Access Control Groups window closes, and the Application User Configuration window displays, now showing the selected groups in the Groups list box. To remove the user from a group, highlight the group in the Groups list box and click the Remove from Access Control Group button. To view or update a group, double-click the group name or click the group name to highlight it; then, click View Details. The Access Control Group Configuration window displays with the current settings.
Roles	This list box displays after an application user has been added, the Groups list box has been populated, and the user record saved. The list box displays the roles that are assigned to the application user. To view or update a role, double-click the role name or click the role name to highlight it; then, click View Details. The Role Configuration window displays with the current settings.

Related Topics

Application User Setup , on page 829
Manage Application User Credential Information , on page 837
Role Setup , on page 865
Access Control Group Setup , on page 869

Add Administrator User to Cisco Unity or Cisco Unity Connection

The Create Cisco Unity Application User link in the Application Configuration window allows you to add a user as an administrator user to Cisco Unity or Cisco Unity Connection. With this method, you configure the application user in Cisco Unified Communications Manager Administration; then, configure any additional settings for the user in Cisco Unity or Cisco Unity Connection Administration.

If you are integrating Cisco Unified Communications Manager with Cisco Unity Connection 7.x, you can use the import feature that is available in Cisco Unity Connection 7.x instead of performing the procedure that is described in the this section. For information on how to use the import feature, see the User Moves, Adds, and Changes Guide for Cisco Unity Connection 7.x.

The Create Cisco Unity User link displays only if you install and configure the appropriate Cisco Unity or Cisco Unity Connection software. See the applicable Cisco Unified Communications Manager Integration Guide for Cisco Unity or the applicable Cisco Unified Communications Manager SCCP Integration Guide for Cisco Unity Connection.

Before You Begin

Ensure that you have defined an appropriate template for the user that you plan to push to Cisco Unity or Cisco Unity Connection. For Cisco Unity Connection users, see the applicable User Moves, Adds, and Changes Guide for Cisco Unity Connection. For Cisco Unity users, see the System Administration Guide for Cisco Unity.

Procedure

Step 1 Find the application user.

Step 2 From the Related Links drop-down list box, choose the Create Cisco Unity Application User link and click Go.
The Add Cisco Unity User dialog box displays.

Step 3 From the Application Server drop-down list box, choose the Cisco Unity or Cisco Unity Connection server on which you want to create a Cisco Unity or Cisco Unity Connection user and click Next.

Step 4 From the Application User Template drop-down list box, choose the template that you want to use.

Step 5 Click Save.
The administrator account gets created in Cisco Unity or Cisco Unity Connection. The link in Related Links changes to Edit Cisco Unity User in the Application User Configuration window. You can now view the user that you created in Cisco Unity Administration or Cisco Unity Connection Administration.

Note When the Cisco Unity or Cisco Unity Connection user is integrated with the Cisco Unified CM Application User, you cannot edit fields such as Alias (User ID in Cisco Unified Communications Manager Administration), First Name, Last Name, Extension (Primary Extension in Cisco Unified Communications Manager Administration), and so on, in Cisco Unity Administration or Cisco Unity Connection Administration. You can only update these fields in Cisco Unified Communications Manager Administration.

Note Cisco Unity and Cisco Unity Connection monitor the synchronization of data from Cisco Unified Communications Manager. You can configure the sync time in Cisco Unity Administration or Cisco Unity Connection Administration on the Tools menu. For Cisco Unity Connection, see the User Moves, Adds, and Changes Guide for Cisco Unity Connection for more information. For Cisco Unity, see the System Administration Guide for Cisco Unity.

Related Topics

Application User Setup , on page 829

Change Application User Password

Use the following procedure to change an application user password.

Procedure

Step 1 Find the application user whose password you want to change.
The Application User Configuration window displays information about the chosen application user.

Step 2 In the Password field, double-click the existing, encrypted password and enter the new password.

Step 3 In the Confirm Password field, double-click the existing, encrypted password and enter the new password again.

Step 4 Click Save.

Related Topics

Application User Setup , on page 829

Manage Application User Credential Information

Use the following procedure to change or view credential information, such as the associated authentication rules, the associated credential policy, or the time of last password change for an application user. You can edit user credentials only after the user exists in the database.

You cannot save settings in the user Credential Configuration window that conflict with the assigned credential policy. For example, if the policy has the Never Expires check box checked, you cannot uncheck and save the Does Not Expire check box in the user Credential Configuration window. You can, however, set a different credential expiration for the user, including Does Not Expire, if the Never Expires policy setting is not checked; the user setting overrides the policy setting.

You cannot change settings in the user Credential Configuration window that conflict with other settings in the user Credential Configuration window. For example, if the User Cannot Change box is checked, you cannot check the User Must Change at Next Login check box.

The Credential Configuration window provides approximate event times; the system updates the form at the next authentication query or event.

Before You Begin

Create the application user in the database.

Procedure

Step 1 Use the Finding an Application User window to find the application user configuration (**User Management** > **Application User**).
The Application User Configuration window displays the configuration information.

Step 2 To change or view password information, click the Edit Credential button next to the Password field. The user Credential Configuration window displays.

Step 3 View the credential data for the user or enter the appropriate settings, as described in Table 125: Application User and End User Credential Settings and Fields , on page 838.

Step 4 If you have changed any settings, click Save.

Credential Settings and Fields

The following table describes credential settings for application users and end users. These settings do not apply to application user or end user digest credentials.

Table 125: Application User and End User Credential Settings and Fields

Field	Description
Locked By Administrator	Check this check box to lock this account and block access for this user. Uncheck this check box to unlock the account and allow access for this user. Use this check box when the credential policy specifies that an Administrator Must Unlock this account type after an account lockout.
User Cannot Change	Check this check box to block this user from changing this credential. Use this option for group accounts. You cannot check this check box when User Must Change at Next Login check box is checked.
User Must Change at Next Login	Check this check box to require the user to change this credential at next login. Use this option after you assign a temporary credential. You cannot check this check box when User Cannot Change check box is checked.
Does Not Expire	Check this check box to block the system from prompting the user to change this credential. You can use this option for low-security users or group accounts. If checked, the user can still change this credential at any time. When the check box is unchecked, the expiration setting in the associated credential policy applies. You cannot uncheck this check box if the policy setting specifies Does Not Expire.

Field	Description
Reset Hack Count	Check this check box to reset the hack count for this user and clear the Time Locked Due to Failed Login Attempts field. The hack count increments whenever authentication fails for an incorrect credential. If the policy specifies No Limit for Failed Logons, the hack count always specifies 0.
Authentication Rule	Select the credential policy to apply to this user credential.
Time Last Changed	This field displays the date and time of the most recent credential change for this user.
Failed Logon Attempts	This field displays the number of failed login attempts since the last successful login, since the administrator reset the hack count for this user credential, or since the reset failed login attempts time expired.
Time of Last Field Logon Attempt	This field displays the date and time for the most recent failed login attempt for this user credential.
Time Locked by Administrator	This field displays the date and time that the administrator locked this user account. This field goes blank after the administrator unlocks the credential.
Time Locked Due to Failed Logon Attempts	This field displays the date and time that the system last locked this user account due to failed login attempts. Time of hack lockout gets set whenever failed login attempts exceed the configured threshold in the applied credential policy.

Associate Devices to Application Users

Before You Begin

To assign devices to an application user, you must access the Application User Configuration window for that user. Use the Finding an Application User window (**User Management** > **Application User**) to find an application user. When the Application User Configuration window displays, perform the following procedure to assign devices.

Procedure

Step 1 In the Available Devices list box, choose a device that you want to associate with the application user and click the Down arrow below the list box. The selected device moves to the applicationuser.controlledDevices list box.

Step 2 To limit the list of available devices, click the Find more Phones, Find more Route Points, or Find more Pilot Points button:

a) If you click the Find more Phones button, the Find and List Phones window displays. Perform a search to find the phones to associate with this application user.
b) If you click the Find more Route Points button, the Find and List CTI Route Points window displays. Perform a search to find the CTI route points to associate with this application user.
c) If you click the Find more Pilot Points button, the Find and List Pilot Points window displays. Perform a search to find the pilot points to associate with this application user.

Step 3 Repeat the preceding steps for each device that you want to assign to the application user.

Step 4 When you complete the assignment, click Save to assign the devices to the application user.

Related Topics

Application User Setup , on page 829

CHAPTER 96

End User Setup

This chapter provides information about managing end user directory information.

About End User Setup

In Cisco Unified Communications Manager (Unified CM) Administration, use the **User Management** > **End User** menu path to configure end users.

The End User Configuration window in Unified CM Administration allows the administrator to add, search, display, and maintain information about Unified CM end users. End users can control phones after you associate a phone in the **End User Configuration** window. You can also enable end users for IM and Presence.

End User Setup Tips

Consult the following information before you begin to configure end users:

- To verify whether the Enable Synchronizing from LDAP Server check box is checked, choose **System** > **LDAP** > **LDAP System**. If the check box is checked, LDAP synchronization is enabled; if not, LDAP synchronization is disabled.
- If you enable LDAP synchronization in Unified CM Administration, you cannot change some existing user information, including user IDs, for LDAP synchronized users in the End User Configuration windows. Instead, you must use the corporate LDAP directory to update some user information for those users. For local users, all the user information remains editable.
- If you configure your system to authenticate users against the LDAP directory, you cannot configure or change end user passwords for LDAP synchronized users in Unified CM Administration. You configure and change end user passwords for those users in the corporate LDAP directory. For local users, you configure and change the end user passwords in Unified CM Administration.
- You can import Cisco Unity Connection users in Cisco Unity Connection, as described in the applicable User Moves, Adds, and Changes Guide for Cisco Unity Connection. Or, if you want to do so, you can configure a Unified CM Administration end user as a Cisco Unity Connection user by using the Create a Cisco Unity User option in the End User Configuration window. You can then configure any additional settings in Cisco Unity Connection Administration.

Note Before you can create a Cisco Unity Connection mailbox for the end user, you must configure the end user with a phone device association and a primary extension, and the integration between Unified CM and Cisco Unity Connection must be complete. For more information, see the *Cisco Unified Communications Manager SCCP Integration Guide* for Cisco Unity Connection or the *Cisco Unified Communications Manager SIP Trunk Integration Guide* for Cisco Unity Connection.

Next Steps to Configure an End User

You can associate devices to this end user and manage the end user credentials.

You can create a Cisco Unity Connection Voice Mailbox for this user in Unified CM Administration.

You can specify this cluster as the home cluster for the end user.

You can configure this end user for IM and Presence service.

You can include end user meeting and calendar information in IM and Presence service.

You can associate a service profile to this end user.

You can associate users to their line appearances for presence.

Related Topics

Manage Application User Credential Information , on page 837
Create Cisco Unity Connection Voice Mailbox , on page 851
Associate Devices to End User , on page 856

End-User Setup for IM and Presence

Perform the following tasks to set up an end user for IM and Presence Service:

- Specify the home cluster service for the end user.

- Set the Enable IM and Presence parameter for the end user, and configure IM and Presence Service in the associated UC service profile.
- Associate a line appearance to this end user for IM and Presence Service using the Controlled Devices parameter to enable on-the-phone status information when off-hook.
- Assign the end user to an IM and Presence Service server that is installed in the cluster if the system is non-balanced.

You can assign users to an IM and Presence Service server from the Cisco Unified Communications Manager Administration menu path **User Management** > **Assign Presence User**. Alternatively, you can assign end users to a server from the **Server Configuration** window of an IM and Presence Service server when you click the **Assigned Users** link in the information pane.

When you assign end users to an IM and Presence Service server, you can either select a server or allow Cisco Unified Communications Manager to choose a server for optimal load balancing when more than one IM and Presence Service server is installed in the cluster. You can manually initiate rebalancing, which redistributes end users across all IM and Presence Service servers in a cluster for optimal load balancing.

See the *Cisco Unified Communications Manager Bulk Administration Guide* for information about assigning end users to an IM and Presence Service node using the Bulk Administration Tool.

Note The enterprise parameter User Assignment Mode for Presence Server automatically handles user assignment. The default setting is Balanced assignment. No manual user assignment is required unless you set the User Assignment Mode for Presence Server parameter to None.

IM and Presence End-User Setup Considerations

Observe the following before you set up users for IM and Presence Service:

- You must install a Unified Communications Manager IM and Presence Service node along with the Unified Communications Manager cluster.
- The end user should only be homed to one cluster within the enterprise.
- You cannot unlicense an end user for IM and Presence Service when that user is assigned to an IM and Presence Service server.

Related Topics

IM and Presence Service User Assignment, on page 858

End User Deletion

Before you delete an end user, determine whether you must remove the devices or profiles that are associated with the end user.

You can view the devices and profiles that are assigned to the end user from the Device Associations, Extension Mobility, Directory Number Associations, CAPF Information, and Permissions Information areas of the End User Configuration window. You can also choose Dependency Records from the Related Links drop-down list box in the End User 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.

Next Steps

If this user is configured in Cisco Unity Connection, the user association to Cisco Unified Communications Manager (Unified CM) is broken when you delete the user in Unified CM Administration. You can delete the orphaned user in Cisco Unity Connection Administration. See the applicable *User Moves, Adds, and Changes Guide for Cisco Unity Connection*. Deleting the user deletes all messages in the user voice mailbox.

Related Topics

Access Dependency Records , on page 982

End User Settings

The following table describes the end user settings.

Table 126: End User Settings

Field	Description
User Information	
User Status	This field indicates whether the user is a local user or LDAP synchronized.
User ID	Enter the unique end user identification name. You can enter any character, including alphanumeric and special characters. No character restrictions exist for this field. You can modify the user ID only for local users. For LDAP synchronized users, you can view the user ID, but you cannot modify it. **Note** Cisco recommends that you do not use a slash (/) in the User ID field. Cisco User Data Services will not function properly for the user when the User ID contains a slash.
Password/Edit Credential	This field does not display for LDAP synchronized users if LDAP Authentication is enabled. Enter alphanumeric or special characters for the end user password. You must enter at least the minimum number of characters that are specified in the assigned credential policy (1-127 characters). The Edit Credential button displays after this user is added to the database. Click the Edit Credential button to manage credential information for this user.
Confirm Password	This field does not display for LDAP Synchronized users if LDAP Authentication is enabled. Enter the end user password again.
Self-Service User ID	This field is a DTMF digit string that is used to identify the (typically same as their directory number). **Note** If the DN pattern contains only digits or if the DN contains \+ only at the beginning of the DN pattern, and the rest of the pattern contains only digits, only then the Self-Service User ID is generated.

Field	Description
PIN/Edit Credential	Enter numeric characters for the end user PIN. You must enter at least the minimum number of characters that are specified in the assigned credential policy (1-127 characters). The Edit Credential button appears after you add this user to the database. Click the Edit Credential button to manage credential information for this user.
Confirm PIN	Enter the PIN again.
Last Name	Enter the end user last name.
Middle Name	Enter the end user middle name.
First Name	Enter the end user first name.
Title	Enter the end user title.
Directory URI	Enter the directory URI that you want to associate to this end user. A directory URI looks like an email address and follows the user@host format. For information about valid formats for directory URIs, see Directory URI formats in the "Intercluster Directory URI" chapter of the *Cisco Unified Communications Manager Administrative Guide*. **Note** If you enter a directory URI and also enter a directory number in the Primary Extension field, this directory URI automatically becomes the primary directory URI that is associated to that directory number.
Work Number	Enter the end user work number. You may use the following special characters: (,), and -.
Home Number	Enter the end user home number. You may use the following special characters: (,), and -.
Mobile Number	Enter the end user mobile number. You may use the following special characters: (,), and -.
Pager Number	Enter the end user pager number. You may use the following special characters: (,), and -.
Mail ID	Enter the end user e-mail address.
Manager User ID	Enter the user ID of the end user manager ID. **Tip** The manager user ID that you enter does not have to exist in the same cluster as the end user; therefore, Unified CM does not require that you enter a user ID that already exists in the database.
Department	Enter the end user department information (for example, the department number or name).

Field	Description
User Locale	From the drop-down list box, choose the locale that is associated with the end user. The user locale identifies a set of detailed information to support end users, including language and font. Unified Communications Manager uses this locale for extension mobility and the Cisco Unified Communications Self Care Portal. For Cisco Extension Mobility login, the locale that is specified takes precedence over the device and device profile settings. For Cisco Extension Mobility logout, Unified Communications Manager uses the end user locale that the default device profile specifies. **Note** If you do not choose an end user locale, the locale that is specified in the Cisco CallManager service parameters as Default User Locale applies.
Associated PC	This required field applies for Cisco IP Softphone users.
Digest Credentials	Enter a string of alphanumeric characters. Unified Communications Manager uses the digest credentials that you specify here to validate the credentials that the phone offers during digest authentication. The digest credentials that you enter in this field get associated with the phone when you choose a digest user in the Phone Configuration window. **Note** For more information about digest authentication, see the *Cisco Unified Communications Manager Security Guide*.
Confirm Digest Credentials	To confirm that you entered the digest credentials correctly, re-enter the credentials in this field.
Convert User Account	
Convert LDAP Synchronized User to Local User	This check box appears for LDAP synchronized end users. Check this check box then save changes to convert an LDAP synchronized user to a local user.
Service Settings	
Home Cluster	Check this check box if the end user is homed to this cluster. The end user should only be homed to one cluster within the enterprise. **Note** IM and Presence does not function properly if an end user is assigned to more than one home cluster. **Note** After an upgrade to Unified Communications Manager Release 10.0(1), when new users are synced from LDAP, the home cluster is not enabled. You must modify your existing LDAP synchronization agreement and add a Feature Group Template which has the home cluster enabled.

Field	Description
Enable User for IM and Presence	Check this check box to enable the end user (on the home cluster) for IM and Presence. Configure IM and Presence in the associated service profile. **Note** You must install a Unified Communications Manager IM and Presence node along with this Unified Communications Manager cluster. Use the **User Management** > **User Settings** > **UC Services** menu to configure the IM and Presence service.
Include meeting information in Presence	Check this check box to enable the end user to include meeting and calendar information in IM and Presence Service. The end user must be on the home cluster and have IM and Presence enabled. Also ensure that an Exchange Presence Gateway is configured on the Cisco Unified Communications Manager IM and Presence Service server.
Presence Viewer for User	Select the Presence Viewer for User link to open the End User Presence Viewer. For more information, see topics related to the End User Presence Viewer.
UC Service Profile	Choose a UC service profile from the drop-down list box. To view the settings for each UC service profile, click the More Details link.
Device Associations	
Controlled Devices	After you associate the device, this field displays the description information (for example, the MAC address) that the end user controls. Adding a device to the list of controlled devices for the end user does not move the device from “Unassigned Devices” to “Users” in the License Usage Report. You must assign a user ID to the device. **Note** To associate a line appearance to this end user for presence, select the Line Appearance Association from Presence button. Doing so enables the on-the-phone status information to IM and Presence clients when this line appearance is off-hook. The Line Appearance choices presented depend on the lines associated with the controlled devices. **Note** If you want additional line appearance associations, or multiple user associations for a single line appearance, choose **Call Routing** > **Directory Number** to see the Directory Number window.
Available Profiles	This drop-down list box displays the device profiles that are available for association with this end user.
CTI Controlled Profiles	This drop-down list box displays the CTI-controlled profiles that are available for association with an end user who is configured for CTI.
Extension Mobility **Note** Extension Mobility is not supported for third-party AS-SIP.	

Field	Description
Available Profiles	This list box displays the extension mobility profiles that are available for association with this end user. To search for an extension mobility profile, click Find. Use the Find and List Device Profiles window that appears to search for the extension mobility profile that you want. To associate an extension mobility profile with this end user, select the profile and click the Down arrow below this drop-down list box.
Controlled Profiles	This field displays a list of controlled device profiles that are associated with an end user who is configured for Cisco Extension Mobility.
Default Profile	From the drop-down list box, choose a default extension mobility profile for this end user.
BLF Presence Group	Use this field to configure the BLF Presence feature. From the drop-down list box, choose a BLF presence group for the end user. The selected group specifies the destinations that the end user can monitor. The default value for BLF Presence Group specifies Standard Presence group, configured with installation. BLF Presence Groups that are configured in Cisco Unified Administration also appear in the drop-down list box. BLF Presence Group authorization works with BLF Presence Groups to allow or block presence requests between groups. See the *Cisco Unified Communications Manager Features and Services Guide*.
SUBSCRIBE Calling Search Space	Supported with the BLF Presence feature, the SUBSCRIBE calling search space determines how Unified Communications Manager routes presence requests that come from the end user. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the end user. From the drop-down list box, choose the SUBSCRIBE calling search space to use for presence requests for the end user. All calling search spaces that you configure in Cisco Unified CM Administration appear in the SUBSCRIBE Calling Search Space drop-down list box. If you do not select a different calling search space for the end user from the drop-down list box, the SUBSCRIBE calling search space defaults to None. To configure a SUBSCRIBE calling search space specifically for this purpose, you configure a calling search space as you do all calling search spaces.
Allow Control of Device from CTI	If this check box is checked, when the user logs in to a device, the AllowCTIControlFlag device property becomes active, which allows control of the device from CTI applications. Until the user logs in to a device, this setting has no effect. **Note** The Allow Control of Device from CTI setting in the end user configuration overrides the AllowCTIControlFlag device property of the device to which the user logs in.

Field	Description
Enable Extension Mobility Cross Cluster	Check this box to enable this end user to use the Cisco Extension Mobility Cross Cluster feature. For more information about the Cisco Extension Mobility Cross Cluster feature, see the *Cisco Unified Communications Manager Features and Services Guide*.
Directory Number Associations	
Primary Extension	This field represents the primary directory number for the end user. End users can have multiple lines on their phones. When you associate devices to the end user, directory numbers that are configured on the associated device become available in the drop-down list box for Primary Extension. From the drop-down list box, choose a primary extension for this end user. If the system is integrated with Cisco Unity Connection, the Create Cisco Unity User link displays in the Related Links menu.
IPCC Extension	From the drop-down list box, choose an IPCC extension for this end user. **Note** This field appears only if the IPCC Express Installed enterprise parameter is set to True.
Mobility Information	
Enable Mobility	Check this check box to activate Cisco Unified Mobility, which allows the user to manage calls by using a single phone number and to pick up in-progress calls on the desktop phone and cellular phone. Checking this check box triggers licensing to consume device license units for Cisco Unified Mobility.
Enable Mobile Voice Access	Check this check box to allow the user to access the Mobile Voice Access integrated voice response (IVR) system to initiate Cisco Unified Mobility calls and activate or deactivate Cisco Unified Mobility capabilities.
Maximum Wait Time for Desk Pickup	Enter the maximum time in milliseconds that is permitted to pass before the user must pick up a call that is transferred from the mobile phone to desktop phone.
Remote Destination Limit	Enter the maximum number of phones to which the user is permitted to transfer calls from the desktop phone.
Remote Destination Profiles	This field lists the remote destination profiles that were created for this user. To view the details of a particular remote destination profile, choose a remote destination profile in the list and click the View Details link.
Mutilevel Precedence and Preemption Authorization	

Field	Description
MLPP User Identification Number	This pane displays the Instance ID from the CAPF Profile that you configured for this user. To view or update the profile, double-click the Instance ID or click the Instance ID to highlight it; then, click View Details. The End User CAPF Profile Configuration window displays with the current settings. **Note** The MLPP User Identification number must comprise 6 - 20 numeric characters. For information on how to configure the End User CAPF Profile, see the *Cisco Unified Communications Manager Security Guide*.
MLPP Password	Enter the MLPP password. **Note** The MLPP Password must comprise 4 - 20 numeric characters.
Confirm MLPP Password	Confirm the MLPP password. **Note** To confirm that you entered the MLPP Password correctly, re-enter the password in this field.
MLPP Precedence Authorization Level	Set the MLPP Precedence Authorization Level. The following precedence levels indicate the priority level that is associated with a call: • 0: Flash Override (highest) • 1: Flash • 2: Immediate • 3: Priority • 4: Routine (lowest) You can set the Precedence Authorization Level to any standard precedence level from Routine to Executive Override. Calls of equal or lower precedence are authorized to be originated by the user.

Related Topics

Calling Search Space Setup , on page 273
End User Setup , on page 841
Associate Devices to End User , on page 856
Role Setup , on page 865
Access Control Group Setup , on page 869

Create Cisco Unity Connection Voice Mailbox

The Create Cisco Unity User link on the End User Configuration window allows you to create individual Cisco Unity Connection voice mailboxes in Cisco Unified Communications Manager (Unified CM) Administration.

Before You Begin

- You must configure Unified CM for voice messaging.
- You must configure the Cisco Unity Connection server to use the integrated mailbox feature. See the "Creating Multiple User Accounts from Unified CM Users" chapter of the applicable *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.
- For Cisco Unity Connection integration, create an AXL connection via Cisco Unity Connection, as described in the "Managing the Phone System Integrations" chapter in the System Administration Guide for Cisco Unity Connection.
- Ensure that you define an appropriate template and Class of Service (COS) for any voice-messaging users that you plan to add in Unified CM Administration. For Cisco Unity Connection users, see the applicable *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.
- You must associate a device and a Primary Extension Number to the end user before the Create Cisco Unity User link displays. The link appears in the Related Links menu.
- You can use the import feature that is available in Cisco Unity Connection instead of performing the procedure that is described in this section. For information about how to use the import feature, see the "Creating Multiple User Accounts from Unified CM Users" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

Note The Directory Number Configuration window also displays the "Create Cisco Unity User" link in the Related Links drop-down list box.

Procedure

Step 1 Use the **User Management** > **End User** menu option to find the end user.

Step 2 Verify that a primary extension number is associated with this user.

Note You must define a primary extension; otherwise, the Create Cisco Unity User link does not appear in the Related Links drop-down list box.

Step 3 From the Related Links drop-down list box, choose the Create Cisco Unity User link, and then click **Go**. The Add Cisco Unity User dialog box appears.

Step 4 From the Application Server drop-down list box, choose the Cisco Unity Connection server on which you want to create a Cisco Unity Connection user, and then click **Next**.

Step 5 From the Subscriber Template drop-down list box, choose the subscriber template that you want to use.

Step 6 Click **Save**.

The mailbox is created. The link in the Related Links drop-down list box changes to Edit Cisco Unity User in the End User Configuration window. In Cisco Unity Connection Administration, you can now view the user that you created.

Note After you integrate the Cisco Unity Connection user with the Unified CM end user, you cannot edit fields in Cisco Unity Connection Administration such as Alias (User ID in Unified CM Administration), First Name, Last Name, and Extension (Primary Extension in Unified CM Administration). You can only update these fields in Unified CM Administration.

Related Topics

End User Setup , on page 841

Change End User Password

Use the following procedure to change the password for an end user in Cisco Unified Communications Manager Administration.

Note You cannot change an end user password when LDAP authentication is enabled.

Procedure

Step 1 Use the **User Management** > **End User** menu option to find the end user.
The End User Configuration window displays the configuration information.

Step 2 In the Password field, double-click the existing password, which is encrypted, and enter the new password. You must enter at least the minimum number of characters that are specified in the assigned credential policy (1-127 characters).

Step 3 In the Confirm Password field, double-click the existing, encrypted password and enter the new password again.

Step 4 Click Save.

Related Topics

End User Setup , on page 841

Change End User PIN

Use the following procedure to change the personal identification number (PIN) for an end user.

Procedure

Step 1 Use the **User Management** > **End User** menu option to find the end user.

The End User Configuration window displays the configuration information.

Step 2 In the PIN field, double-click the existing PIN, which is encrypted, and enter the new PIN. You must enter at least the minimum number of characters that are specified in the assigned credential policy (1-127 characters).

Step 3 In the Confirm PIN field, double-click the existing, encrypted PIN and enter the new PIN again.

Step 4 Click Save.

Related Topics

End User Setup , on page 841

Manage End User Credential Information

Use the following procedure to change or view credential information, such as the associated authentication rules, the associated credential policy, or the time of last password change for an end user. You can edit user credentials only after the user exists in the database.

In the user Credential Configuration window, you cannot save settings that conflict with the assigned credential policy.

In the user Credential Configuration window, you cannot change settings that conflict with other settings in the user Credential Configuration window. For example, if the User Cannot Change check box is checked, you cannot check the User Must Change at Next Login check box.

The credential configuration window reports approximate event times; the system updates the form at the next authentication query or event.

Before You Begin

Create the end user in the database.

Procedure

Step 1 Use the **User Management** > **End User** menu option to find the end user.
The End User Configuration window displays the configuration information.

Step 2 To change or view password information, click the Edit Credential button next to the Password field. To change or view PIN information, click the Edit Credential button next to the PIN field.

Step 3 Enter the appropriate settings as described in Table 127: Application User and End User Credential Settings and Fields , on page 854.

Step 4 If you have changed any settings, click Save.

Related Topics

End User Setup , on page 841
About End User Setup , on page 841

Credential Settings and Fields

The following table describes the credential settings for end users and application users. These settings do not apply to application user or end user digest credentials.

Table 127: Application User and End User Credential Settings and Fields

Field	Description
Locked By Administrator	Check this check box to lock this account and block access for this user. Uncheck this check box to unlock the account and allow access for this user.
User Cannot Change	Check this check box to block this user from changing this credential. Use this option for group accounts. You cannot check this check box when User Must Change at Next Login check box is checked.
User Must Change at Next Login	Check this check box to require the user to change this credential at next login. Use this option after you assign a temporary credential. You cannot check this check box when User Cannot Change check box is checked.
Does Not Expire	Check this check box to block the system from prompting the user to change this credential. You can use this option for low-security users or group accounts. If this check box is checked, the user can still change this credential at any time. When this check box is unchecked, the expiration setting in the associated credential policy applies.
Reset Hack Count	Check this check box to reset the hack count for this user and clear the Time Locked Due to Failed Login Attempts field. After the counter resets, the user can try logging in again The hack count increments whenever an authentication fails for an incorrect credential. If the policy specifies No Limit for Failed Logons, the hack count always equals 0.
Authentication Rule	Select the credential policy to apply to this user credential.
Time Last Changed	This field displays the date and time of the most recent change for this user credential.
Failed Logon Attempts	This field displays the number of failed login attempts since the last successful login, since the administrator reset the hack count for this user credential, or since the reset failed login attempts time has expired.

Field	Description
Time of Last Failed Logon Attempt	This field displays the date and time for the most recent failed login attempt for this user credential.
Time Locked by Administrator	This field displays the date and time that the administrator locked this user account.
Time Locked Due to Failed Logon Attempts	This field displays the date and time that the system last locked this user account due to failed login attempts. The associated credential policy defines lockouts due to failed login attempts.

Related Topics

End User Setup , on page 841

Set Up End User Information

After you add a new end user, you can configure additional information that is related to the end user. This information allows each end user to personalize phone features, Manager Configuration, Assistant Configuration, Cisco Extension Mobility, Cisco Unified Communications Manager Auto-Attendant, and Cisco IP Softphone capability.

Before You Begin

Make sure that the end user is in the database.

Procedure

Step 1 Use the **User Management** > **End User** menu option to find the end user whose application profiles you want to configure.
The End User Configuration window appears with information about the chosen end user.

Step 2 Click the user ID.

Step 3 To configure a manager for Cisco Unified Communications Manager Assistant for this end user, from the Related Links drop-down list box, choose Manager Configuration, and then click **Go**.
The Manager Configuration window appears for this end user. For more information about configuring Cisco Unified Communications Manager Assistant, see topics related to Cisco Unified Communications Manager Assistant with proxy line support and shared line support in the *Cisco Unified Communications Manager Features and Services Guide*.

After you configure the manager information for this end user, you can return to the End User Configuration window for this end user. From the Related Links drop-down list box in the Manager Configuration window, choose Back to User Configuration, and then click **Go**.

Step 4 To configure an assistant for Cisco Unified Communications Manager Assistant for this end user, from the Related Links drop-down list box, choose Assistant Configuration, and then click **Go**.
The Assistant Configuration window appears for this end user. For more information about configuring Cisco Unified Communications Manager Assistant, see topics related to Cisco Unified Communications Manager

Assistant with proxy line support and shared line support in the *Cisco Unified Communications Manager Features and Services Guide*.

After you configure the assistant information for this end user, you can return to the End User Configuration window for this end user. From the Related Links drop-down list box in the Assistant Configuration window, choose Back to User Configuration and click Go.

Step 5 To show the user privilege report for this end user, from the Related Links drop-down list box, choose User Privilege Report, and then click **Go**.
The User Privilege window appears for this end user.

After you display the user privilege report for this end user, you can return to the End User Configuration window for this end user. From the Related Links drop-down list box in the User Privilege window, choose Back to User, and then click **Go**.

Related Topics

End User Setup , on page 841
View User Roles, Access Control Groups, and Permissions , on page 875

Associate Devices to End User

You can associate devices over which end users have control. End users can control some devices, such as phones. Applications that are identified as users can control other devices, such as CTI ports. When end users have control of a phone, they can control certain settings for that phone, such as speed dial and call forwarding.

Note For devices that are not CTI-controllable, such as H.323 devices, an asterisk (*) appears next to the device icon in the list of available devices. All device association behavior remains identical regardless of the type of device for which the feature is configured.

Before You Begin

To associate devices with an end user, you must access the End User Configuration window for that user. Use the **User Management** > **End User** menu option to find the end user. When the End User Configuration window appears, perform the following procedure to assign devices.

Do not attempt to associate devices to a new end user before you finish adding the new end user. Be sure to click Save on the End User Configuration window before you add device associations for a new end user.

Procedure

Step 1 In the Device Associations pane, click **Device Association**.
The User Device Association window appears.

Because you may have several devices in your network, Cisco Unified Communications Manager (Unified CM) lets you locate specific devices on the basis of specific criteria. Use the following steps to locate devices.

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

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3, on page 857.

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 Click **Find**.
All or matching records appear. You can change the number of items that appears in each window by choosing a different value from the Rows per Page drop-down list box.

Associating a Device

Step 4 From the Device association for (this particular user) pane, choose the devices that you want to associate with this end user by checking the box to the left of the device names.
Use the buttons at the bottom of the window to select and deselect devices to associate with the end user.

Note The buttons function to select and deselect only the devices that were found as a result of any search for devices that you performed in the preceding steps.

Tip Check the Show the devices already associated with user check box to display the devices that are already associated with this end user.

Use the buttons to perform the following functions:

a) **Select All**: Click this button to select all devices that appear in this window.
b) **Clear All—**Click this button to uncheck the check boxes next to all devices that appear in this window.
c) **Select All in Search—**Click this button to select all devices that match the search criteria that you specified in the Search Options portion of the window. The button performs the search anew and selects all the matching devices.
d) **Clear All in Search—**Click this button to deselect all devices that match the search criteria that you specified in the Search Options portion of the window. The button performs the search anew and deselects all the matching devices.
e) **Save Selected/Changes—**Click this button to associate the devices that you selected with this end user.
f) **Remove All Associated Devices—**Click this button to disassociate all devices that are already associated with this end user. After you click this button, a dialog box asks you to confirm that you want to remove all device associations from this end user. To confirm, click OK.

Step 5 Repeat the preceding steps for each device that you want to assign to the end user.

Step 6 To complete the association, click **Save Selected/Changes**.

Step 7 From Related Links drop-down list box, choose Back to User, and then click **Go**.
The End User Configuration window appears, and the associated devices that you chose appear in the Controlled Devices pane.

Related Topics

End User Setup , on page 841

Associate Cisco Extension Mobility Profile to Cisco Unified IP Phone

Use Cisco Extension Mobility to configure a Cisco Unified IP Phone to temporarily display as the phone of an end user. The end user can sign in to a phone, and the Extension Mobility profile (including line and speed-dial numbers) for the end user resides on the phone. This feature applies primarily in environments where end users are not permanently assigned to physical phones.

- To associate an Extension Mobility profile to an end user, you must access the End User Configuration window for that end user. Use the **User Management** > **End User** menu option to find the end user. To configure and associate Cisco Extension Mobility for end users, see the *Cisco Unified Communications Manager Features and Services Guide*.

Related Topics

End User Setup , on page 841

IM and Presence Service User Assignment

For end users to receive the availability and Instant Messaging (IM) services of IM and Presence Service, they must be assigned to IM and Presence Service servers on your nodes and clusters.

The User Assignment Mode enterprise parameter, which has a default value that is set to Balanced, enables users to be automatically assigned to servers when they are added to the system. No manual user assignment is required when the User Assignment Mode enterprise parameter is set to Balanced.

You can manually assign end users to a selected IM and Presence Service server or initiate the rebalance user assignment procedure, which automatically assigns end users across all servers in a cluster to optimize load balancing. Use Cisco Unified Communications Manager Administration to manually assign end users to IM and Presence Service servers.

Note You must set up and enable IM and Presence Service for the end user before using this feature.

Related Topics

Assign Users for IM and Presence , on page 858
End-User Setup for IM and Presence , on page 842
Rebalance User Assignments, on page 861
Unassign IM and Presence User, on page 860
View Users Assigned to IM and Presence Server, on page 861

Assign Users for IM and Presence

Use Cisco Unified Communications Manager Administration to assign end users to IM and Presence Service server nodes and clusters for end users to receive the availability and Instant Messaging (IM) services of IM and Presence Service. You can assign selected users or all users to an IM and Presence Service server on the cluster or you can allow the system to automatically select the server for optimized loading.

Before You Begin

- Specify the home cluster service for the end user.
- Set the Enable IM and Presence parameter for the end user, and configure IM and Presence Service in the associated UC service profile.
- Associate a line appearance to this end user for IM and Presence Service using the Controlled Devices parameter to enable on-the-phone status information when off-hook.

Procedure

Step 1 Open the **Find and List Presence User Assignment** window using one of the following methods:

- Select **User Management** > **Assign Presence User**. The **Find and List Presence User Assignment** window displays.
- Navigate from the **IM and Presence Server Configuration** window to autopopulate the **Find and List Presence User Assignment** window with the selected server information:

  1. Select **System** > **Server**. The **Find and List Servers** window appears.
  2. Select the server search parameters, and then click **Find**. Matching records appear.
  3. Select the IM and Presence server that is listed in the **Find and List Servers** window. The **Server Configuration** window appears.
  4. Click the Assigned Users link in the IM and Presence Server Information section of the **Server Configuration** window.

     The **Find and List Presence User Assignment** window displays with the server information autopopulated.

Step 2 Select the end-user search parameters, and then click **Find.**
Matching records appear.

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 **Clear Filter** to remove all added search criteria.

Step 3 Check the check box beside the user records to assign those users.

Tip Click **Select All** to select all users that appear in this window, or click **Clear All** to uncheck the check boxes next to all end users that appear in this window.

Step 4 Perform one of the following to select the users to assign:

- Click **Assign Selected Users** to assign the selected end users.
- Click **Assign All Users** to assign all the end users in the system.

The **Assign Users** window appears.

Note To rebalance end users across all IM and Presence Service servers in the node and clusters, see tasks that are related to rebalancing user assignments.

Step 5 Click **Server** in the **Assign Users** window, and then select a server from the drop-down list to assign the users to that server.

Step 6 Click **Save**.

Related Topics

End-User Setup for IM and Presence , on page 842
Rebalance User Assignments, on page 861

Unassign IM and Presence User

Use Cisco Unified Communications Manager Administration to unassign end users from IM and Presence Service server nodes and clusters.

Procedure

Step 1 Open the **Find and List Presence User Assignment** window using one of the following methods:

- Select **User Management** > **Assign Presence User**. The **Find and List Presence User Assignment** window displays.
- Navigate from the **IM and Presence Server Configuration** window to autopopulate the **Presence User Assignment** window with the selected server information:
  1. Select **System** > **Server**. The **Find and List Servers** window appears.
  2. Select the server search parameters, and then click **Find**. Matching records appear.
  3. Select the IM and Presence Service server that is listed in the **Find and List Servers** window. The **Server Configuration** window appears.
  4. Click on the Assigned Users link in the IM and Presence Server Information section of the **Server Configuration** window.

The **Find and List Presence User Assignment** window displays with the server information autopopulated.

Step 2 Select the end-user search parameters, and then click **Find.**
Matching records appear.

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** to remove all added search criteria.

Step 3 Check the check box beside the user records to unassign those users from the selected server.

Tip Click **Select All** to select all users that appear in this window, or click **Clear All** to uncheck the check boxes next to all end users that appear in this window.

Step 4 Select **Unassigned** in the Assign Users pane, and then click **Save**.
The selected users are unassigned from the IM and Presence Service servers.

Rebalance User Assignments

Use Cisco Unified Communications Manager Administration to rebalance end-user assignments across all IM and Presence Service server nodes and clusters for optimized loading.

The rebalance procedure is not needed if the User Assignment Mode enterprise parameter is set to Balanced (default) before users are added to the system.

Note Users who are not assigned to a node before rebalancing will remain unassigned.

Before You Begin

The rebalance procedure that is performed depends on the User Assignment Mode that is configured for IM and Presence Service server using **Server** > **Enterprise Parameters**. The options are:

- Balanced: Evenly distribute users across all servers.
- Active-Standby: Assign users to only one server (the active server) per redundancy group and the other server is a backup in case the users fail over (standby).
- None: Rebalance operation is disabled.

Procedure

Step 1 Select **User Management** > **Assign Presence User**.
The **Find and List Presence User Assignment** window displays.

Tip You can also navigate to the **Find and List Presence User Assignment** window when you click the Assigned Users link on the **IM and Presence Server Configuration** window.

Step 2 Click **Rebalance Users** to rebalance end users across all IM and Presence Service servers in the node and clusters.

View Users Assigned to IM and Presence Server

Use Cisco Unified Communications Manager Administration to view the number of end users that are currently assigned to IM and Presence Service nodes and information about those end users. The following end-user information is displayed:

- User ID: The system-assigned user ID.
- First Name: The first name of the user.
- Last Name: The last name of the user.
- Server: This field displays the server IP address or hostname of the IM and Presence Service node to which the user is assigned.
- Presence Redundancy Group: This field indicates whether or not the assigned IM and Presence Service node is a member of a presence redundancy group. If the node belongs to a presence redundancy group, the name is displayed.

Procedure

Step 1 Select **System** > **Server**.
The **Find and List Servers** window appears.

Step 2 Select the server search parameters, and then click **Find**.
Matching records appear.

Step 3 Select the IM and Presence Service server that is listed in the **Find and List Servers** window.
The **Server Configuration** window appears. The number of users that are assigned to the selected server is displayed in the Assigned Users link.

Step 4 Click on the **Assigned Users** link in the IM and Presence Server Information section of the **Server Configuration** window.
The **Find and List Presence User Assignment** window for the server appears.

Include Meeting Information in IM and Presence Service

Use Cisco Unified Communications Manager Administration to include meeting and calendar information in IM and Presence Service for an end user. You can access the option to enable the inclusion of meeting and calendar information from either the End User Configuration or the Feature Group Template Configuration windows in Cisco Unified Communications Manager Administration.

For information about enabling the inclusion of meeting and calendar information for an end user using the Bulk Administration Tool, see the *Cisco Unified Communications Manager Bulk Administration Guide*.

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

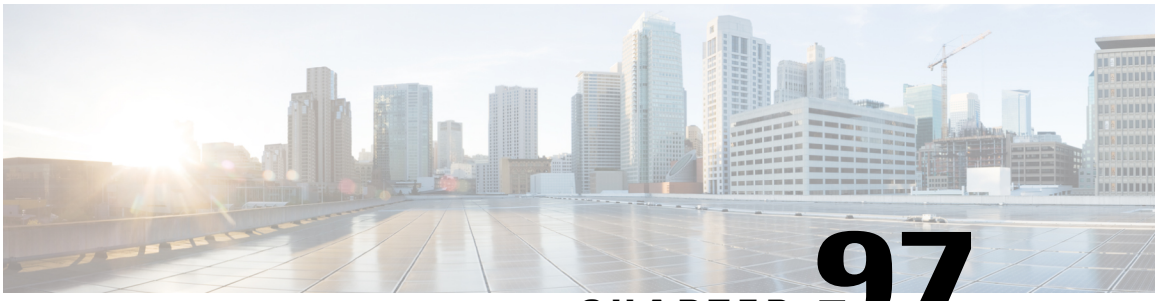
Step 1 Perform one of the following:

- Select **User Management** > **End User** to find the end user. The End User Configuration window displays.
- Select **User Management** > **User/Phone Add** > **Feature Group Template** to find the Feature Group Template.

Step 2 Check the **Include meeting information in Presence** check box.

Note This check box is available for selection only if the Home Cluster and Enable User for Unified CM IM and Presence check boxes are checked.

Step 3 Click **Save**.



CHAPTER 97

Role Setup

This chapter provides information to configure roles.

Role Setup

In Cisco Unified Communications Manager Administration, use the **User Management** > **User Settings** > **Role** menu path to configure roles.

Roles allow Cisco Unified Communications Manager administrators who have full administration privilege (access) to configure end users and application users with different levels of privilege. Administrators with full administration privilege configure roles and user groups. In general, full-access administration users configure the privilege of other administration users and end users to Cisco Unified Communications Manager Administration and to other applications.

Different levels of privilege exist for each application. For example, for Cisco Unified Communications Manager Administration, two levels of privilege exist: read privilege and update privilege. These privilege levels differ as follows:

- Users with update privilege can view and modify the Cisco Unified Communications Manager Administration windows to which the user group of the user has update privilege.
- A user with read privilege can view the Cisco Unified Communications Manager Administration windows that belong to the roles to which the user group of the user has read privilege. A user with read privilege for a window cannot, however, make any changes on those administration windows to which the user has only read privilege. For a user with read privilege, the Cisco Unified Communications Manager Administration application does not display any update buttons or icons.

Roles comprise groups of resources for an application. If you want to do so, you can create custom roles that comprise custom groupings of resources for an application. At installation, default standard roles are created for various administrative functions. For example, to configure Audit Log Administration, choose the Standard Audit Log Administration role. When the Role Configuration window displays, check the Read or Update check box for the resource you want to configure and click Save.

Tip Certain standard roles have no associated application nor resource. These roles provide login authentication for various applications.

Example Add or Copy Roles

To configure Audit Log Administration, choose the Standard Audit Log Administration role. When the Role Configuration window displays, click the Read or Update check box for the resource that you want to configure and click Save.

Note Copying a role also copies the privileges that are associated with that role.

If you are adding a new role, choose an application from the Application drop-down list box and click Next. In the Role Configuration window that displays, enter the appropriate settings as described in Table 128: Role Settings , on page 866.

Role Deletions

You cannot delete a standard role.

Role Settings

The following table describes the role settings.

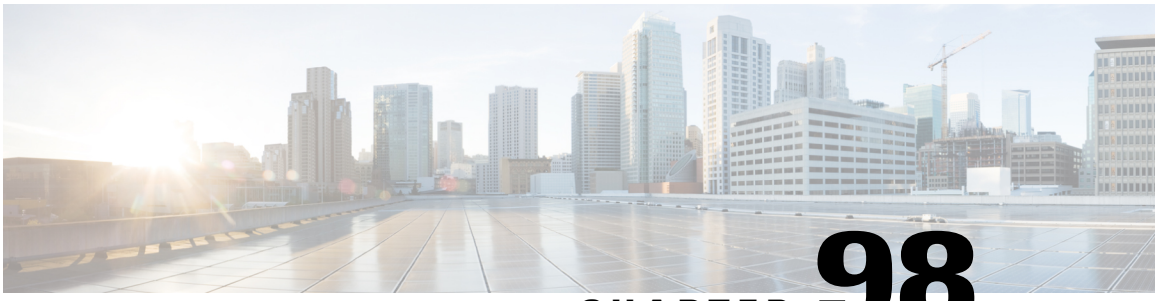
Table 128: Role Settings

Field	Description
Role Information	
Application	From the drop-down list box, choose the application with which this role associates.
Name	Enter a name for the role. Names can comprise up to 128 characters. Valid characters include letters, numbers, dashes, dots (periods), spaces, and underscores.
Description	Enter a description for the role. Descriptions can have up to 128 characters.
Resource Access Information	

Field	Description
(list of resource names for the chosen application)	In the Resource Access Information pane, click the check box(es) next to the resource(s) that you want this role to include. **Note** In some applications, only one check box applies for each resource. In the Cisco Unified Communications Manager Administration application, a read check box and an update check box apply to each resource.
Grant access to all	Click this button to grant privileges for all resources that display on this page for this role. **Note** If the list of resources displays on more than one page, this button applies only to the resources that display on the current page. You must display other pages and use the button on those pages to change the access of the resources that are listed on those pages.
Deny access to all	Click this button to remove privileges for all resources that display on this page for this role. **Note** If the list of resources displays on more than one page, this button applies only to the resources that display on the current page. You must display other pages and use the button on those pages to change the access of the resources that are listed on those pages.

Related Topics

Role Setup , on page 865



CHAPTER 98

Access Control Group Setup

This chapter provides information to configure access control groups, assign users to access control groups, and view the roles, access control groups, and permissions of a user.

About Access Control Group Setup

The role and access control group menu options in the Cisco Unified Communications Manager (Unified CM) Administration User Management menu allow users with full access to configure different levels of access for Unified CM administrators. Users with full access configure roles, access control groups, and access privileges for roles. In general, full-access users configure the access of other users to Unified CM Administration.

Access control groups comprise lists of application users and end users. A user may belong to multiple access control groups. After you add an access control group, you then add users to an access control group. After these steps, you can assign roles to an access control group. If a user belongs to multiple access control groups, the MLA permission enterprise parameter determines the effective privilege of the user.

Reduced Permissions for Access Control Groups

Problem When you add a new access control group to existing users, the level of privileges for some pre-existing access control groups is unexpectedly reduced.

Solution Users can belong to multiple access control groups. When you add a new access control group to existing users, the current level of privileges for some pre-existing access control groups may be reduced if

the new access control group has the “Effective Access Privileges for Overlapping User Groups and Roles” Enterprise parameter set to minimum.

Access privilege reduction can occur inadvertently, for example, during an upgrade of Cisco Unified CM Administration. If the upgrade version supports the Standard RealTimeAndTrace Collection user group, which has the “Effective Access Privileges for Overlapping User Groups and Roles” Enterprise parameter set to minimum, all users are automatically added to that user group during the upgrade. To resolve the permissions issue in this example, you can remove users from the Standard RealTimeAndTrace Collection user group.

Find Access Control Group

Because you might have several access control groups in your network, Cisco Unified Communications Manager (Unified CM) lets you locate specific access control groups on the basis of specific criteria. Use the following procedure to locate access control group.

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

Procedure

Step 1 Choose **User Management** > **User Settings** > **Access Control Group**.
The Find and List Access Control Groups window appears. 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.

a) From the drop-down list box, select a search pattern.
b) 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 Click **Find**.
All matching records appear. You can change the number of items that appear 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 then clicking Delete Selected. You can delete all configurable records for this selection by clicking Select All, and then clicking Delete Selected.

Note You cannot delete the standard access control groups.

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.

Related Topics

Access Control Group Setup , on page 869

Set Up Access Control Group

This section describes how to add, copy, and update an access control group to and in the Cisco Unified Communications Manager Administration.

The following example provides more detail about configuring an access control group.

To allow a user to change Audit Log settings, choose Standard Audit Users, and then click Add End Users to Group. When the Find and List Users window appears, choose the user that you want to add to the group and click Add Selected.

Procedure

Step 1 Choose **User Management** > **User Settings** > **Access Control Group**.
The Find and List Access Control Group window appears.

Step 2 Perform one of the followings tasks:

a) To copy an existing access control group, locate the appropriate access control group, and then click **Copy** next to the access control group that you want to copy. In the popup window that appears, enter a name for the new access control group, and then click **OK**. Continue with Step 3, on page 871.

b) To add a new access control group, click **Add New**. Enter a name for the new access control group, and then click **OK**. Continue with Step 3, on page 871.

Note The access control group name can contain up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that the access control group name is unique.

c) To update an existing access control group, locate the appropriate access control group. Click the name of the access control group that you want to update. The access control group that you chose appears. Update the appropriate settings. Continue with Step 3, on page 871.

Note You cannot delete a standard access control group, but you can update the user membership for a standard access control group.

Step 3 Click **Save**.

Step 4 Add users to this access control group.

Step 5 Assign roles to the access control group.

Related Topics

Access Control Group Setup , on page 869
Find Access Control Group , on page 870
Add Users to Access Control Groups , on page 872
Assign Roles to Access Control Group , on page 874

Delete Access Control Group

This section describes how to delete an access control group from Unified CM Administration. Use the following procedure to delete an access control group entirely.

Before You Begin

When you delete an access control group, Cisco Unified Communications Manager (Unified CM) removes all access control group data from the database. To find out which roles are using the access control group, in the Access Control Group Configuration window, choose Dependency Records from the Related Links drop-down list box, and then click Go. If dependency records are not enabled for the system, the Dependency Records Summary window displays a message.

Procedure

Step 1 Choose **User Management** > **User Settings** > **Access Control Group**.
The Find and List Access Control Groups window appears.

Step 2 Find the access control group that you want to delete.

Step 3 Click the name of the access control group that you want to delete.
The access control group that you chose appears. The list shows the users in this access control group in alphabetical order.

Step 4 If you want to delete the access control group entirely, click **Delete**.
A dialog box appears to warn you that you cannot undo the deletion of access control groups.

Step 5 To delete the access control group, click **OK** or to cancel the action, click **Cancel**. If you click **OK**, Unified CM removes the access control group from the database.

Related Topics

Access Control Group Setup , on page 869
Find Access Control Group , on page 870
Delete Users from Access Control Groups, on page 874
Access Dependency Records , on page 982

Add Users to Access Control Groups

This section describes how to add end users and application users to an access control group in Cisco Unified Communications Manager (Unified CM) Administration.

Procedure

Step 1 Choose **User Management** > **User Settings** > **Access Control Group**.
The Find and List Access Control Groups window appears.

Step 2 Find the access control group to which you want to add users.

Step 3 Click the name of the access control group that you want to update.
The access control group that you chose appears. The Users list shows the users that currently belong to the access control group.

Step 4 To add end users, click **Add End Users to Group**. To add application users, skip to step 8.
The Find and List Users window appears.

Step 5 Use the Find User drop-down list boxes to find the end users that you want to add, and then click **Find**.

Note You can perform the search for users in a variety of ways. You can enter the first name, middle name, last name, user ID, or department of a user. Alternatively, you can leave the field blank, which results in display of all users.

A list of end users that matches your search criteria appears.

Note The list of search results does not display end users that already belong to the access control group.

Step 6 In the list of search results, check the check box next to the users that you want to add to this access control group. If the list comprises multiple pages, use the links at the bottom to see more results.

Step 7 Click **Add Selected**.
The Access Control Group Configuration window reappears with the users that you added listed in the Users pane.

Note After you add a user, you can view the roles by clicking the i icon in the Permission column for that user.

Step 8 To add application users, click **Add App Users to Group**.
The Find and List Application Users window appears.

Step 9 Use the Find Application User drop-down list boxes to find the application users that you want to add and click Find.

Note You can perform the search for application users by searching for user ID. Alternatively, you can leave the field blank, which results in display of all application users.

A list of application users that matches your search criteria displays.

Step 10 In the list of search results, check the check box next to the application users that you want to add to this access control group. If the list comprises multiple pages, use the links at the bottom to see more results.

Note The list of search results does not display application users that already belong to the user group.

Step 11 Click **Add Selected**.
The Access Control Group Configuration window reappears with the application users that you added listed in the Users pane.

Note After you add an application user, you can view the roles by clicking the i icon in the Permission column for that user.

Step 12 To save your changes to this access control group, click **Save**.

Related Topics

Access Control Group Setup , on page 869
Find Access Control Group , on page 870

Delete Users from Access Control Groups

This section describes how to delete users from an access control group in Cisco Unified Communications Manager (Unified CM) Administration.

Procedure

Step 1 Choose **User Management** > **User Management** > **Access Control Group**.
The Find and List Access Control Groups window appears.

Step 2 Find the access control group from which you want to delete users.

Step 3 Click the name of the access control group that you want to update.
The access control group that you chose appears. The Users list shows the users that currently belong to the access control group.

Step 4 Check the check boxes next to the names of the users that you want to delete from this access control group.

Step 5 Click **Delete Selected**.
A confirmation message asks you to confirm the deletion.

Step 6 To delete the selected access control group members, click **OK** or **Cancel** to exit this window.
The Access Control Group Configuration reappears with the deleted users removed from the Users in Group pane.

Related Topics

Access Control Group Setup , on page 869
Find Access Control Group , on page 870

Assign Roles to Access Control Group

Users with full access can assign roles to access control groups. An access control group that has assigned roles has access to the resources that the role comprises.

This section describes assigning roles to an access group in Cisco Unified Communications Manager (Unified CM) Administration.

Note When an administrator assigns roles to an access control group, the administrator should assign the Standard Unified CM Admin Users role to the access control group. This role enables the users to log into Unified CM Administration.

Procedure

Step 1 Choose **User Management** > **User Settings** > **Access Control Group**.
The Find and List Access Control Groups windows appears.

Step 2 Find the access control group to which you want to assign roles.

Step 3 Click the name of the access control group for which you want to assign roles.
The access control group that you chose appears. The Users list shows the users that currently belong to the access control group.

Step 4 From the Related Links drop-down list box, choose Assign Role to Access Control Group, and then click **Go**.
The Access Control Group Configuration window changes to display the Role Assignment pane. For the access control group that you chose, the list of assigned roles appears. Choose one of the following options:

a) To assign roles to the access control group, go to step 5.
b) To delete roles from the user group, go to step 9.

Step 5 To assign additional roles to the access control group, click **Assign Role to Group**.
The Find and List Roles dialog box appears.

Step 6 If necessary, use the **Find Role** search criteria to narrow the list of roles.

Step 7 Choose the roles to assign to this access control group by checking the check boxes next to the role names.
To close the Find and List Roles dialog box without assigning roles to this access control group, click **Close**.

Step 8 Click **Add Selected**.
The Find and List Roles dialog box closes. The chosen roles get added to the Role Assignment pane for this access control group. If you do not want to delete any assigned roles for this access control group, skip to step 10.

Step 9 To delete an assigned role from the access control group, select a role in the Role Assignment pane, and then click **Delete Role Assignment**. Repeat this step for each role that you want to delete from this access control group.

Step 10 Click **Save**.
The system makes the added and deleted role assignments to the access control group in the database.

Related Topics

Access Control Group Setup , on page 869
Find Access Control Group , on page 870

View User Roles, Access Control Groups, and Permissions

This section describes how to view the roles, access control groups, and permissions that are assigned to a user who belongs to a specified access control group. Use the following procedure to view the roles, access control groups, and permissions that are assigned to a user in an access control group.

Note You can also view user roles by using **User Management** > **Application User** (for application users) or **User Management** > **End User** (for end users) to view a particular user, and then display the user roles.

Procedure

Step 1 Choose **User Management** > **User Settings** > **Access Control Group**.

The Find and List Access Control Groups window appears.

Step 2 Find the access control group that has the users for which you want to display assigned roles.

Step 3 Click the name of the access control group for which you want to view the roles that are assigned to the users. The Access Control Group Configuration window appears for the access control group that you chose. The Users pane shows the users that belong to the access control group.

Step 4 For a particular user, click the username.
The Application User Configuration window (for application users) or End User Configuration window (for end users) appears.

Step 5 From the Related Links drop-down list box, choose User Privilege Report, and then click **Go**.
For the user that you chose, the following information appears:

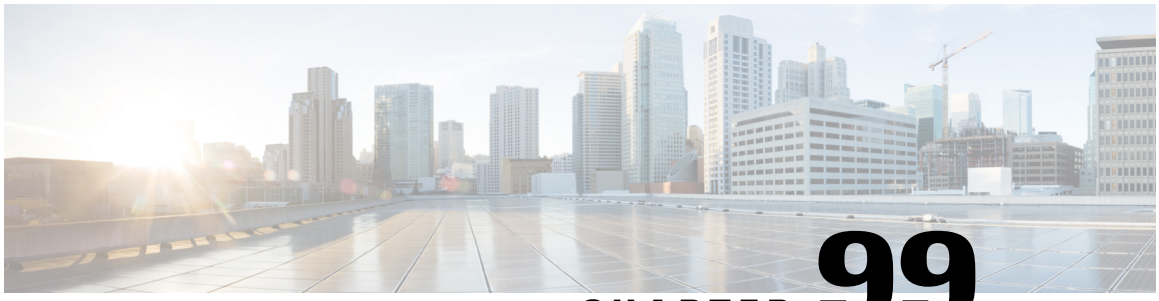
a) Access control groups to which the user belongs
b) Roles that are assigned to the user
c) Resources to which the user has access. For each resource, the following information appears:

- Application
- Resource
- Permission (read and/or update)

Step 6 To return to the user, choose **Back to User** or **Back to Application User** in the Related Links drop-down list box, and click **Go**.

Related Topics

Access Control Group Setup , on page 869
Find Access Control Group , on page 870



CHAPTER 99

End User Phone Addition

This chapter provides information about adding and configuring end users at the End User, Phone, DN, and LA Configuration window.

About End User Phone and Device Addition

In Cisco Unified Communications Manager Administration, use the **User Management** > **User/Phone Add** Add menu path to configure an end user, a phone, and a line appearance in a single addition.

The End User, Phone, DN, and LA Configuration window in Cisco Unified Communications Manager Administration provides a single window that allows you to perform the basic steps that are required to add a new user and assign the user to a new phone. While you add a new end user and associate the end user with a new phone, you can configure a new directory number (DN) and line appearance (LA) information for the new end phone.

The End User, Phone, DN, and LA Configuration window, which does not allow you to enter existing end users, phones, or directory numbers, adds records of the following types:

- End users
- Phones
- Directory numbers
- Device profiles
- Voicemail profile

Note You can modify end user information only if synchronization with an LDAP server is not enabled. To check whether synchronization with an LDAP server is enabled, choose the **System** > **LDAP** > **LDAP System** menu option. In the LDAP System window that displays, ensure that the Enable Synchronizing from LDAP Server check box is not checked. If synchronization is enabled, access to the End User, Phone, DN, and LA Configuration window is blocked.

Administrators can customize the End User, Phone, DN, and LA Configuration window. Fields in the window have the following check boxes next to them, which you can use to customize those fields:

- Default—Enter a value in the field, then check the Default check box to make that value the default value. Other users can edit the default value, unless the Read Only check box is checked.
- Hidden—Check the Hidden check box to hide the field.
- Read Only—Check the Read Only check box to make the field read only.

To save your customization changes, click the Save Settings button. The customizations are system-wide, so all other users will see customizations that you save.

To display all hidden fields in the window, click the Show Hidden Fields button.

User and Device Settings

The following table describes the end user and device settings.

Table 129: User and Device Settings

Field	Description
User Information	
User ID	Enter the end user identification name. Cisco Unified Communications Manager does not permit modifying the user ID after it is created. You may use the following special characters: =, +, <, >, #, ;, \, , “”, and blank spaces.
Password	Enter five or more alphanumeric or special characters for the end user password. You may use the following special characters: =, +, <, >, #, ;, \, , “”, and blank spaces.
Confirm Password	Enter the end user password again.
PIN	Enter five or more numeric characters for the Personal Identification Number.
Confirm PIN	Enter the PIN again.
Last Name	Enter the end user last name. You may use the following special characters: =, +, <, >, #, ;, \, , “”, and blank spaces.
Middle Name	Enter the end user middle name. You may use the following special characters: =, +, <, >, #, ;, \, , “”, and blank spaces.
First Name	Enter the end user first name. You may use the following special characters: =, +, <, >, #, ;, \, , “”, and blank spaces.
Device Associations	

Field	Description
Product Type	This list box displays the types of devices that are available for association with this end user. From the drop-down list box, choose the type of device to associate with this end user.
MAC Address	Enter a unique MAC address for the new device that you are associating with the new user. The MAC address comprises exactly 12 hexadecimal digits (0 to 9, A to F).
Calling Search Space DN	From the drop-down list box, choose the calling search space for the directory number that you are associating with this user and device.
Calling Search Space Phone	From the drop-down list box, choose the calling search space for the phone that you are associating with this user and device.
External Phone Number Mask	Specify the mask that is used to format caller ID information for external (outbound) calls that are made from the associated device. • The mask can contain up to 24 characters. Valid characters specify 0 to 9, *, #, and X. • Enter the literal digits that you want to appear in the caller ID information and use Xs to represent the directory number of the associated device. • See the following examples:If you specify a mask of 972813XXXX, an external call from extension 1234 displays a caller ID number of 9728131234 if the Use External Phone Number Mask option is checked on the route pattern that is used to make the external call.If you specify a mask of all literal digits, such as 9728135000 to represent a main attendant number, that literal number (9728135000) displays as the caller ID for an external call from any associated device.
Extension	This field represents the primary directory number for the end user. End users can have multiple lines on their phones. Enter an extension for the new user and phone. You may use the following characters: 0 to 9, ?, [,], +, -, *, ^, #, !.
Route Partition	From the drop-down list box, choose a partition for the directory number that you specified in the Extension field.
Voice Mail Profile	From the drop-down list box, choose a voice-mail profile for the directory number. Choose <None> to use the system default.
Enable Extension Mobility	Check this check box to enable extension mobility. After you have added the new user, you can use the **User Management** > **End User** menu option to choose an Extension Mobility profile.

Add and Associate End User and Phone

The following procedure provides instructions on adding an end user and phone and associating the user and phone with a directory number and device profile.

Procedure

Step 1 Choose **User Management** > **User/Phone Add** Add.
The End User, Phone, DN, and LA Configuration window displays.

Note If LDAP synchronization is enabled, access to this window is blocked.

Note Before you proceed, you can use the links in the Related Links drop-down list box at the top, right of the End User, Phone, DN, and LA Configuration window to determine whether an end user or phone already exists.

To find out which end users already exist, choose Back to Find List Users in the Related Links drop-down list box and click Go. Use the Find and List Users window that displays to search for the end user ID that you plan to add. If the end user ID already exists, you cannot use the User/Phone Add menu option to add this end user.

To find out which phones already exist, choose Back to Find List Phones in the Related Links drop-down list box and click Go. Use the Find and List Phones window that displays to search for the phone that you plan to add. If the phone already exists, you cannot use the User/Phone Add menu option to add this phone.

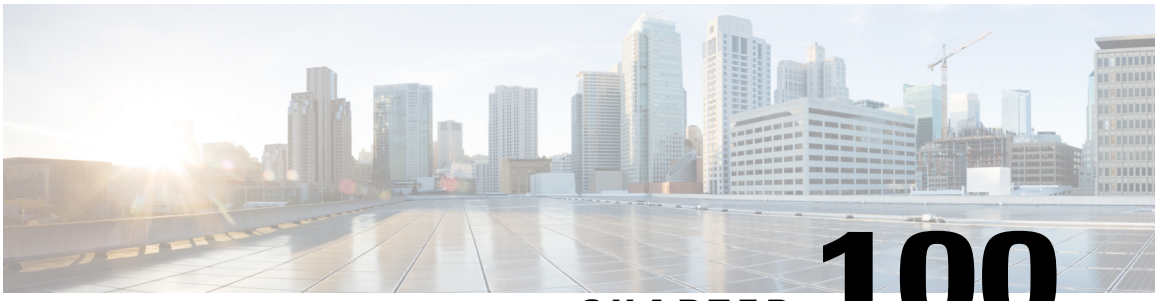
If you use either of the Related Links, repeat Step 1, on page 880 to return to the End User, Phone, DN, and LA Configuration window.

Step 2 Enter the appropriate settings as described in Table 129: User and Device Settings, on page 878.

Step 3 When you complete the end user configuration, click Save to add the end user and device.
The end user gets created in the Cisco Unified Communications Manager database.

Related Topics

LDAP System Setup , on page 107
End User Phone Addition , on page 877



CHAPTER 100

UC Service Setup

This chapter provides information to set up Unified Communications (UC) services.

About UC Service Setup

In Cisco Unified Communications Manager Administration, use the **User Management** > **User Settings** > **UC Service** to set up unified communications (UC) services such as voicemail, conferencing, CTI, and IM and Presence.

The UC Service window in Cisco Unified Communications Manager Administration allows you to add, search, display, and maintain information about UC services. You can group UC services into service profiles that you associated with end users. After end users have a service profile, their clients can download this profile for seamless integration with the configured UC services.

You can set up these UC services:

- Voicemail
- Mailstore
- Conferencing
- Directory
- IM and presence
- CTI

UC Service Setup Tips

- Port values for UC services must match the available port on the server. Change the port number only if it conflicts with other services.
- Cisco recommends that you use HTTPS as the voicemail transport protocol for Cisco Unity and Cisco Unity Connection

Add Voicemail Service

Procedure

Step 1 Select **User Management** > **User Settings** > **UC Service**.

Step 2 Select **Add New**.

Step 3 Select **Voicemail** from the **UC Service Type** drop-down list.

Step 4 Enter the voicemail settings in the following fields.

Table 130: Voicemail Settings

Field	Description
Product Type	Select a product type. Available options are Unity and Unity Connection. Default setting: Unity.
Name	Enter the name of the voicemail service. Ideally, the voicemail service name should be descriptive enough for you to instantly recognize it. Maximum characters: 50 (ASCII only).
Description	(Optional) Enter a description that helps you to distinguish between voicemail services. You can change the description if required. Maximum characters: 100.
Hostname/IP Address	Enter the address of the voicemail service in one of the following forms: • Hostname • IP address • Fully qualified domain name (FQDN) This field value must exactly match the hostname, IP address, or FQDN of the associated voicemail service. If the hostname or IP address of the voicemail service changes, change this field value accordingly.

Field	Description
Port	Enter the port to connect with the voicemail service. Default port: 443 This field value must match the available port on the voicemail service. Change the port number only if it conflicts with other services.
Protocol	Select the protocol to route voicemail messages securely. Available options: HTTP, HTTPS Default setting: HTTPS. **Tip** Cisco recommends that you use HTTPS as the voicemail transport protocol for Cisco Unity and Cisco Unity Connection servers. Only change to HTTP if your network configuration does not support HTTPS.

Step 5 Select **Save**.
The Add Successful message appears and the voicemail service is created in the Unified CM Database.

What to Do Next

Add Mailstore Service , on page 883

Related Topics

Feature Group Template Setup , on page 953

Add Mailstore Service

Cisco Jabber clients use the mailstore service for visual voicemail functionality.

Procedure

Step 1 Select **User Management** > **User Settings** > **UC Service**.
Step 2 Select **Add New**.
Step 3 Select **Mailstore** from the **UC Service Type** drop-down list.
Step 4 Enter the mailstore settings in the following fields.

Table 131: Mailstore Settings

Field	Description
UC Service Type	Specifies the UC service type as Mailstore.
Product Type	Specifies the product type as Exchange.
Name	Enter the name of the mailstore service. Ideally the mailstore service name should be descriptive enough for you to instantly recognize it. Maximum characters: 50 (ASCII only).
Description	(Optional) Enter a description that helps you to distinguish between mailstore services. You can change the description if required.
Hostname/IP Address	Enter the address of the mailstore service in one of the following forms: • Hostname • IP address • FQDN This field value must exactly match the hostname, IP address, or FQDN of the associated mailstore service. If the address of the mailstore service changes, change this field value accordingly. **Note** Cisco Unity creates subscriber mailboxes for message storage on the Microsoft Exchange server. **Note** Cisco Unity Connection usually provides a mailstore service, and hosts the mailstore service on the same server.
Port	Specify the port number configured for the service. Default Port: 143 Allowed Values: 1 - 65535 **Note** For secure voice messaging with Cisco Unity Connection, use port 7993. **Note** This value must match the available port on the mailstore service. Change the port number only if it conflicts with other services.

Field	Description
Protocol	Select the corresponding protocol to use when Cisco Jabber clients contact this service. Available Options: TCP, SSL, TLS, UDP Default Setting: TCP, which is the most commonly used network configuration. Change this setting to suit your deployment, Unified CM settings, and security needs. **Note** For secure voice messaging with Cisco Unity Connection, use TLS.

Step 5 Select **Save**.
The Add Successful message appears and the mailstore service is created in the Unified CM database.

What to Do Next

Add more UC services.

Add a service profile.

Associate UC services in a service profile to an end user.

Related Topics

Feature Group Template Setup , on page 953

Add Conferencing Service

Procedure

Step 1 Select **User Management** > **User Settings** > **UC Service**.
Step 2 Select **Add New**.
Step 3 Select **Conferencing** from the **UC Service Type** drop-down list box.
Step 4 Enter the conferencing settings in the following fields.

Field	Description
UC Service Type	Specifies conferencing as the UC service type.
Product Type	Select a product type that applies to your network configuration. Available Options: MeetingPlace Classic, MeetingPlace Express, WebEx
Name	Enter the name of the coferencing service. Ideally the service name should be descriptive enough for you to instantly recognize it. Maximum characters: 50 (ASCII only).

Field	Description
Description	(Optional) Enter a description that helps you to distinguish between directory services. You can change the description if required.
Hostname/IP Address	Enter the address of the conferencing service in one of the following forms: • Hostname • IP address • FQDN This field must exactly match the hostname, IP address, or FQDN of the associated directory service. If the address of the directory service changes, change this field value accordingly. Allowed values: Alphanumeric (a-zA-Z0-9), period (.), backslash (\), dash (-), and underscore (_).
Port	Enter the port for the conferencing service so that users can contact the service when they sign in to web conferences. Default Port: 80 Allowed Values: 1- 65535 **Note** Use port 80 for HTTP and port 443 for HTTPS communications. **Note** This value must match the available port on the conferencing service. Change the port number only if it conflicts with other services.
Protocol	Select the protocol to route web conference communications. Available Options: HTTP, HTTPS Default Setting: HTTP. Change this setting to suit your network configuration, IM and Presence settings and security needs as follows: **HTTP** Selects Hypertext Transfer Protocol as the standard method for transferring data between the server, Cisco Jabber, and the browser. Select this option if the Cisco Unified MeetingPlace or the Cisco Unified MeetingPlace Express server does not have SSL enabled. **HTTPS** Selects Hypertext Transfer Protocol over SSL as the method for securely transferring data between the server, Cisco Jabber, and the browser. Select this option if the Unified MeetingPlace or the Unified MeetingPlace Express server has SSL enabled.

Step 5 Select **Save**.
The Add Successful message appears and the conferencing service is created in the Unified CM database.

What to Do Next

Add more UC services.

Add a service profile.

Associate UC services in a service profile to an end user.

Related Topics

Feature Group Template Setup , on page 953

Add Directory Service

Procedure

Step 1 Select **User Management** > **User Settings** > **UC Service**.
Step 2 Select **Add New**.
Step 3 Select **Directory** from the **UC Service Type** drop-down list box.
Step 4 Enter the directory settings in the following fields.

Field	Description
UC Service Type	Specifies directory as the UC service type.
Product Type	Select a supported directory product type from this list that applies to your network configuration. Available Options: Directory, Enhanced Directory Default Setting: Directory
Name	Enter the name of the directory service. Ideally the directory service name should be descriptive enough for you to instantly recognize it. Maximum characters: 50 (ASCII only). Allowed values: All characters allowed except quotes ("), angle brackets (< >), backslash (\), ampersand (&), and percent (%).
Description	(Optional) Enter a description that helps you to distinguish between directory services. You can change the description if required. Allowed values: All characters allowed except quotes ("), angle brackets (< >), backslash (\), ampersand (&), and percent (%).

Field	Description
Hostname/IP Address	Enter the address of the directory service in one of the following forms: • Hostname • IP address • FQDN This field must exactly match the hostname, IP address, or FQDN of the associated directory service. If the address of the directory service changes, change this field value accordingly. Allowed values: Allowed characters include alphanumeric (a-zA-Z0-9), period (.), backslash (\), dash (-), and underscore (_).
Port	Enter the port for the directory service. Default Port: 389 Allowed Values: 1- 65535 **Note** This value must match the available port on the directory service. Change the port number only if it conflicts with other services.
Protocol	Select the protocol to route communications between the directory service and Cisco Jabber clients. Available Options: TCP, UDP, TLS Default Setting: TCP. This is the most commonly used network configuration. Change this setting to suit your network configuration, Unified CM settings, and security needs.

Step 5 Select **Save**.
The Add Successful message appears and the directory service is created in the Unified CM database.

What to Do Next

Add more UC services.

Add a service profile.

Associate UC services in a service profile to an end user.

Related Topics

Feature Group Template Setup , on page 953

Add IM and Presence Service

Procedure

Step 1 Select **User Management** > **User Settings** > **UC Service**.

Step 2 Select **Add New**.

Step 3 Select **IM and Presence** from the UC Service Type drop-down list.

Step 4 Enter the IM and Presence settings in the following fields.

Table 132: IM and Presence Settings

Field	Description
UC Service Type	Specifies IM and Presence as the UC service type.
Product Type	Select a supported IM and Presence product type from this list that applies to your network configuration. Available options: Unified CM (IM and Presence), WebEx (IM and Presence) Default setting: Unified CM (IM and Presence)
Name	Enter the name of the IM and Presence service. Ideally the IM and Presence service name should be descriptive enough for you to recognize it instantly. Maximum characters: 50 (ASCII only).
Description	(Optional) Enter a description that helps you to distinguish between IM and Presence services. You can change the description if required.
Hostname/IP Address	Enter the address of the IM and Presence service in one of the following forms: • Hostname • IP address • DNS SRV Allowed values: Allowed characters include alphanumeric (a-zA-Z0-9), period (.), backslash (\), dash (-), and underscore (_). **Note** This field value must exactly match the host name, IP address, or DNS SRV of the associated IM and Presence service. If the address of the IM and Presence service changes, change this field value accordingly. **Tip** Cisco recommends DNS SRV to help the client find the correct IM and Presence service for the user.

Step 5 Select **Save**.
The Add Successful message appears and the IM and Presence service is created in the Unified CM database.

What to Do Next

Add more UC services.

Add a service profile.

Associate UC services in a service profile to an end user.

Related Topics

Feature Group Template Setup , on page 953

Add CTI Service

Soft clients use the CTI service for deskphone control

Procedure

Step 1 Select **User Management** > **User Settings** > **UC Service**.
Step 2 Select **Add New**.
Step 3 Select **CTI** from the **UC Service Type** drop-down list box.
Step 4 Enter the computer telephone integration (CTI) settings in the following fields.

Field	Description
UC Service Type	Specifies CTI as the UC service type.
Product Type	Specifies CTI as the product type.
Name	Enter the name of the CTI service. Ideally the CTI service name should be descriptive enough for you to instantly recognize it. Maximum characters: 50 (ASCII only).
Description	(Optional) Enter a description that helps you to distinguish between CTI services when you have more than one configured. You can change the description if required.

Field	Description
Hostname/IP Address	Enter the address of the CTI service in one of the following forms: • Hostname • IP address • FQDN This field must exactly match the, hostname, IP address, or FQDN of the associated CTI service. If the address of the CTI service changes, change this field value accordingly.
Port	Enter the port for the CTI service. Default port: 2748 Allowed ports: 1-65535 **Note** This value must match the available port on the CTI service. Change the port number only if it conflicts with other services.
Protocol	Specifies TCP as the default protocol.

Step 5 Select **Save**.
The Add Successful message appears and the CTI service is created in the Unified CM database.

What to Do Next

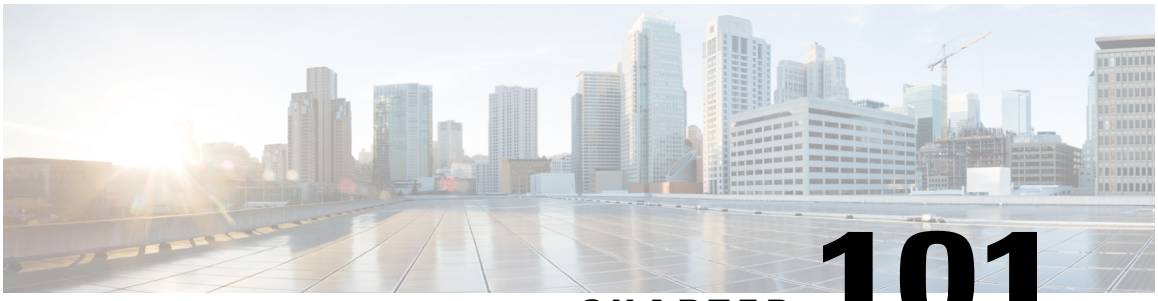
Add more UC services.

Add a service profile.

Associate UC services in a service profile to an end user.

Related Topics

Feature Group Template Setup , on page 953



CHAPTER 101

Service Profile Setup

This chapter contains information to set up service profiles.

About Service Profile Setup

In Cisco Unified Communications Manager (Unified CM) Administration, use the **User Management** > **User Settings** > **Service Profile** menu path to set up service profiles from existing unified communications (UC) services.

The Service Profile window in Unified CM allows you to add, search, display, and maintain information about service profiles that you can assign to end users.

Note If you want a listing of the users associated with a service profile, you can select Dependency Records from the Related Links drop-down list box in the upper right corner.

Service Profile Setup Tips

- Before you create service profiles, you must configure unified communications (UC) services.
- If you upgrade the system from a pre-9.0 Cisco Unified Presence installation, the existing service profiles are migrated from Cisco Unified Presence to Unified CM. You do not lose your service profile settings after you upgrade.
- Migrated service profiles have auto-generated names. You can change them at a later point.
- Prior to Cisco Unified CM IM and Presence Service Release 9.0(1), service profile data used to be editable from Cisco Unified Presence Administration under the **Application** > **CUPC/Cisco Jabber** menu.
- When you configure the IM and Presence UC service, you cannot mix and match product types for the primary, secondary, and tertiary servers. However, you can mix and match the other services.

- If your primary voicemail server is Cisco Unity, you must configure the primary voicemail and primary mailstore servers.
- If your primary voicemail server is Cisco Unity Connection, you do not need to configure a primary voicemail server but you must select a primary mailstore server.
- The primary, secondary, and tertiary server drop-down lists contain the UC services that you previously configured on the UC Services window. Change the servers to suit your network configuration.
- When you use an IM-only client, you cannot set up the service profiles with CTI on Cisco Unified Communications Manager or CCMIP on IM and Presence as it causes high CPU activity on the Cisco Unified Communications Manager and IM an Presence servers.

Service Profile Settings

The following table lists and describes the service profile field settings.

Table 133: Service Profile Settings

Field	Description
Service Profile Information	
Name	Enter the name of the service profile. Ideally the service profile name should be descriptive enough for you to instantly recognize it. This name is visible on the End User settings window. Maximum characters: 50 (ASCII only). Allowed Values: All characters allowed except quotes ("), angle brackets (< >), backslash (\), ampersand (&), and percent (%).
Description	(Optional) Enter a description that helps you to distinguish between service profiles when you have more than one configured. You can change the description if required. Allowed Values: All characters allowed except quotes ("), angle brackets (< >), backslash (\), ampersand (&), and percent (%)
Make this the default service profile for the system	Check this check box to make this service profile the default option for the system. **Note** If you specify a default service profile, end users that do not have an associated service profile automatically inherit the default service profile settings.
Voicemail Profile	
Primary	Select the primary voicemail server with which you want to associate this service profile. This drop-down list contains the voicemail servers that you previously configured on the UC Services window.
Secondary	Select a secondary voicemail server, if applicable.
Tertiary	Select a tertiary voicemail server, if applicable.

Field	Description
Mailstore Profile	
Primary	Select a primary mailstore server. This drop-down list contains the mailstore servers that you previously configured on the UC Services window.
Secondary	Select a secondary mailstore server, if applicable.
Tertiary	Select a tertiary mailstore server, if applicable.
Conferencing Profile	
Primary	Select a primary conferencing server. This drop-down list contains the conferencing servers that you previously configured on the UC Services window.
Secondary	Select a secondary conferencing server, if applicable.
Tertiary	Select a tertiary conferencing server, if applicable.
Server Certificate Verification	Default: Any Specify how the conferencing server associated with this profile supports TLS connections. This setting is for TLS verification of the conferencing servers listed for this conferencing profile. Select from the following options: **Any Certificate** Cisco Jabber accepts all valid certificates. **Self Signed or Keystore** Cisco Jabber accepts the certificate if the certificate is self-signed, or the signing Certificate Authority certificate is in the local trust store. **Note** A keystore is a file that stores authentication and encryption keys. **Keystore Only** Cisco Jabber accepts only certificates that are defined in the keystore. You must import the certificate or its Certificate Authority signing certificate into the local trust store.
Directory Profile	

Field	Description
Primary	Select a primary directory server. This drop-down list contains the directory servers that you previously configured on the UC Services window. **Note** If you select User Data Service (UDS) for directory integration, then you can use UDS for directory searches without selecting any primary, secondary, or tertiary servers. Clients connect to UDS using DNS/SRV. **Tip** Instead of or in addition to UDS, you can specify primary, secondary, tertiary basic or advanced LDAP UC services, because some clients that use these may not support UDS.
Secondary	Select a secondary directory server, if applicable. If you do not set up any backup directory servers, you cannot perform directory searches for Cisco Jabber clients if the first server fails.
Tertiary	Select a tertiary directory server, if applicable. If you do not configure any backup directory servers, you cannot perform directory searches for Cisco Jabber clients if the first server fails.
IM and Presence Profile	
Primary	Select a primary IM and Presence server. This drop-down list contains the IM and Presence servers that you previously configured on the UC Services window. **Note** An IM and Presence profile cannot mix the IM and Presence server and Webex Presence server.
Secondary	Select a secondary IM and Presence server, if applicable.
Tertiary	Select a tertiary IM and Presence server, if applicable.
CTI Profile	
Primary	Select a primary CTI server. This drop-down list contains the CTI servers that you previously configured on the UC Services window.
Secondary	Select a secondary CTI server, if applicable.
Tertiary	Select a tertiary CTI server, if applicable.

Related Topics

Add Service Profile , on page 897

Add Service Profile

Procedure

Step 1 In Unified CM Administration, select **User Management** > **User Settings** > **Service Profile**
The **Find and List** window appears.

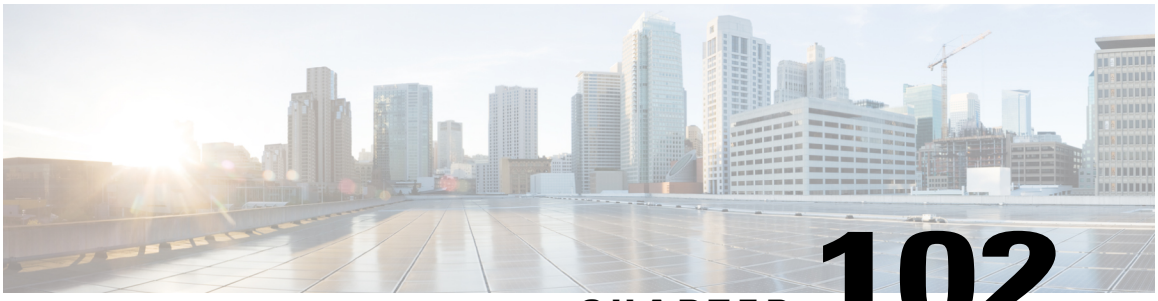
Step 2 Select **Add New**.

Step 3 Enter settings for the service profile fields. See About Service Profile Setup , on page 893.

Step 4 Select **Save**.
The **Add Successful** message appears and the service profile gets created in the Cisco Unified CM database.

Related Topics

About UC Service Setup, on page 881
About Service Profile Setup , on page 893



CHAPTER 102

Universal Template Setup

This chapter contains information about page layout preferences, Universal Device Templates (UDTs), and Universal Line Templates (ULTs).

Page Layout Preferences

In Cisco Unified Communications Manager Administration, use the **User Management** > **User/Phone Add** > **Page Layout Preference** menu path to customize the layout of the **Universal Device Template** and **Universal Line Template** windows.

The **Page Layout Preference Window** allows you to specify and save a custom window layout by rearranging sections, which contain the fields that you configure when you create device or line templates.

With Page Layout Preferences, you can perform the following actions:

- Use arrows to rearrange the order of sections
- Expand, collapse, and hide individual sections
- Expand, collapse, or hide all sections with the push of a button
- Reset to the default view
- Save your page layouts

Note You cannot hide sections that contain mandatory settings for template configuration, such as Required and Frequently Entered Settings.

Modify Page Layout

Procedure

Step 1 From Cisco Unified Communications Manager Administration, select **User Management** > **User/Phone Add** > **Page Layout Preference**

Step 2 Select one of the following window names:

- **Universal Device Template**
- **Universal Line Template**

The section list appears.

Step 3 Rearrange the sections as required.

Note Select **Set To Default** to reset to the default sections order.

Step 4 Select **Save**

The page layout is saved.

What to Do Next

Verify your page layout on the GUI window that you selected.

Universal Device Template Setup

In Cisco Unified Communications Manager Administration, use the **User Management** > **Quick User/Phone Add** > **Universal Device Template** menu path to set up universal device templates (UDTs) that you can apply to any device, such as a phone, RDP, or EM Profile, that you create later.

UDTs are templates that you create to apply to any device. Administrators can view all device-related settings in one simple interface and apply these settings to any device. UDTs use tokens, which are variables in specific fields that fill in information (such as an employee name) automatically. These templates ease administrative tasks that relate to setting up users and devices and keep a range of device settings on one central, customizable interface.

Universal Device Template Settings

Note The UDT sections in this window may appear in a different order than the following table indicates. To change the order of these settings, use the **User Management** > **Quick User/Phone Add** > **Universal Device Templates Display Preference** menu.

Note To make the window easier to view, the template sections are collapsed by default. Expand sections that you need as you review the template setup process. Select the **Expand All** button on the bottom of the window to expand all sections. To customize the **Universal Device Templates window**, see "Universal device template display preference setup"

.

Note The UDT sections in this window may appear in a different order than the following table indicates. To change the order of these settings, use the **User Management** > **User/Phone Add** > **Page Layout Preference** menu.

Note To make the window easier to view, the template sections are collapsed by default. Expand sections that you need as you review the template setup process. Select the **Expand All** button on the bottom of the window to expand all sections. To customize the **Universal Device Template window**, see "Page layout preferences setup"

.

This table describes the available settings in the Universal Device Template window.

Table 134: Universal Device Template Settings

Field	Description
Template Information	
Name	Enter a name to identify this UDT.
Required and Frequently Entered Settings	
Description	Enter the purpose of the UDT. You can enter the functional rule of a group of users or the key features enabled in the template. . **Tip** You can click the pencil icon to place tokens in the description. Tokens are variables that are replaced with actual values, after you create this UDT. You can select the available elements from the list (such as User First Name). For example, the token "#Lastname#s desk phone" becomes "Smith's desk phone" for a user with the last name "Smith." **Note** When you insert the device with this template, the element in the description is propagated based on the actual device or user information.
Device Pool	Select the device pool for the UDT. The device pool defines sets of common characteristics for this UDT, such as region, date/time group, softkey template, and MLPP information.

Field	Description
Device Security Profile	Choose the device security profile for the UDT. The security profile for the UDT is model and protocol independent. **Note** You can only select a model-independent security profile for a UDT. To identify the settings that the profile contains, see the **System** > **Security Profile** > **Phone Security Profile** menu. **Note** If you enable the security feature for a template, the security setting is applied to the phone inserted with this template only when the phone supports all of the following security features. **1** Security Authentication **2** Security Encryption **3** File Encrypt Otherwise you insert the phone with the default non-secure security profile with the same model and device protocol of the inserted phone. For more information about how CAPF settings that you update in the phone configuration window affect security profile CAPF settings, see the *Cisco Unified Communications Manager Security Guide*.
SIP Profile	Select the default SIP profile or a specific profile that was previously created. SIP profiles provide specific SIP information such as registration and keepalive timers, media ports, and Do Not Disturb control.
Phone Button Template	Select the appropriate phone button template for the UDT. The phone button template determines the behavior of buttons, and identifies which feature (such as line and speed dial) is used for each button. **Note** You must select a phone button template before you can expand the Phone Button Configuration field. **Note** You can only assign universal phone button templates to a UDT.
Phone Buttons Configuration	
Use this section to view and change the settings for the universal phone button template. This section lists the configurable buttons for the phone button template that you select in the Phone Button Template field. You can update a universal phone button template to add or remove features; add or remove lines and speed dials; or assign features, lines, and speed dials to different buttons on the phone that you add after you create the UDT. You can change the button labels in the default phone button templates, but you cannot change the function of the buttons in the default templates. **Note** If you update a phone template, be sure to inform affected users of the changes.	

Field	Description
Line Appearance	
Directory Number	Select a directory number (DN) from the drop-down list box. After you create a device with this UDT, the DN will exist on the newly created device automatically.
Line Label	If left blank, this defaults to the line number. If you desire a different label for the line on the phone, you can enter it here. **Tip** You can use tokens (pencil icon) to enter the line label.
Display (Caller ID)	Leave this field blank to have the system display the extension. Use a maximum of 30 alphanumeric characters. Typically, use the username or the directory number (if using the directory number, the person receiving the call may not see the proper identity of the caller). **Tip** You can use tokens (pencil icon) to enter the display.
Ring Setting When Phone is Idle *	Use this field to set up the ring setting for this UDT for the line appearance when an incoming call is received and no other active calls exist on that device. Select one of the following options: • Use system default • Disable • Flash only • Ring once • Ring
Ring Setting When Phone is in Use	From the drop-down list box, select the ring setting that is used for this UDT when it has an active call on a different line. Select one of the following options: • Use system default • Disable • Flash only • Ring once • Ring • Beep only

Field	Description
Visual Message Waiting Indicator Policy *	Enter the external phone number (or mask) that is used to send Caller ID information for this UDT. You can enter a maximum of 24 number, the international escape character +, and "X" characters. The Xs represent the directory number and must appear at the end of the pattern. For example, if you specify a mask of 972813XXXX, an external call from extension 1234 displays a caller ID number of 9728131234.
Audible Message Waiting Indicator Policy *	Use this field to configure the ring setting for the line appearance when an incoming call is received and no other active calls exist on that device. Select one of the following options: • Use system default • Disable • Flash only • Ring once • Ring

Field	Description
Recording Options *	This field determines the recording option on the line appearance of an agent. The default recording option is Call Recording Disabled. Select one of the following options: **Call Recording Disabled** You cannot record call that you make on this line appearance. **Selective Call Recording Enabled** You can record calls that you make on this line appearance by using a softkey or programmable line key that is assigned to the device, a CTI-enabled application, or both interchangeably. Selective recording supports two modes: **Silent recording** Call recording status is not reflected on the Cisco IP device display. Silent recording is typically used in a call center environment to allow a supervisor to record an agent call. A CTI-enabled application running on the supervisor desktop is generally used to start and stop the recording for an agent-customer call. **User recording** User recording-Call recording status is reflected on the Cisco IP device display. You can start or stop a recording by using using a softkey, programmable line key, or CTI-enabled application running on the user desktop. To enable user recording, add the Record softkey or programmable line key to the UDT. Do not add the Record softkey if you only want silent recording. When the recording option is set to either Automatic Call Recording Enabled or Selective Call Recording Enabled, you can associate the line appearance with a recording profile. When automatic recording is enabled, start- and stop-recording requests using a softkey, programmable line key, or CTI-enabled application are rejected.

Field	Description
Recording Profile	This field determines the recording profile on the line appearance of an agent. Choose an existing recording profile from the drop-down list box. To create a recording profile, use the **Device** > **Device Settings** > **Recording Profile** menu option. The default value specifies None.
Call Pickup Group Audio Alert Setting (Phone Active)	This field determines the type of notification an incoming call sends to members of a call pickup group. If the called phone does not answer, the phones in the call pickup group that are busy will either hear a beep (beep beep) or hear nothing (disabled). **Use System Default** The setting of the Cisco CallManager service parameter Call Pickup Group Audio Alert Setting of Busy Station determine the value of this field. **Disable** No alert is sent to member of the call pickup group. **Beep Only** A beep beep is sent to members of the call pickup group.
Call Pickup Group Audio Alert Setting (Phone Idle)	This field determines the type of notification an incoming call sends to members of a call pickup group. If the called phone does not answer, the phones in the call pickup group that are idle will either hear a short ring (ring once) or hear nothing (disabled). **Use System Default** The setting of the Cisco CallManager service parameter Call Pickup Group Audio Alert Setting of Idle Station determines the value of this field. **Disable** No alert is sent to members of the call pickup group. **Ring Once** A short ring is sent to members of the call pickup group.

Field	Description
Monitoring Calling Search Space	The monitoring calling search space of the supervisor line appearance must include the agent line or device partition to allow monitoring the agent. Set the monitoring calling search space on the supervisor line appearance window. Choose an existing calling search space from the drop-down list box. The default value specifies None.
SpeedDial	
(number from 1 to 199 in the left column)	This column identifies the speed-dial button (for example, 1, 2, 3, or 4) or the abbreviated-dial index for abbreviated dial.
Number	Enter the number that you want the system to dial when the user presses the speed-dial button. You can enter digits 0 through 9, *, #, and +, which is the international escape character. For a Pause in Speed Dial, you can enter comma (,) which can act as a delimiter as well as other pause before sending DTMF digits.
Label	Enter the text that you want to display for the speed-dial button or abbreviated-dial number. **Note** If you are configuring a Pause in Speed Dial, you must add a label so that FAC, CMC, and DTMF digits are not displayed on the phone screen.
BLF SpeedDial With the BLF Presence feature, a watcher can monitor the status of the presence entity (also called presentity). When you configure BLF/SpeedDial buttons, the presence entity appears as a speed dial on the device of the watcher. The following section describes the settings that you configure for BLF/SpeedDial buttons.	

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 CM directory numbers as BLF/SpeedDial buttons, enter the directory number in this field. For this field, enter only numerals, asterisks (*), and pound signs (#). **Note** If you configure the Destination field, do not select an option from the Directory Number drop-down list box. If you select an option from the Directory Number drop-down list box after you configure the Destination, Unified CM deletes the Destination configuration.
Directory Number	The Directory Number drop-down list box displays a list of directory numbers that exist in the Unified CM database. Configure this setting only if you did not configure the Destination field. For a UDT that runs either SCCP or SIP, select 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.
BLF Directed Call Park	
Directory Number	The Directory Number drop-down list box displays a list of directory numbers that exist in the Unified CM database. For a UDT that runs either SCCP or SIP, select the number (and corresponding partition, if it appears) that you want the system to dial when the user presses the speed-dial button; for example, 6002 in 3. Directory numbers that appear without specific partitions belong to the default partition.

Field	Description
Label	Enter the text that you want to appear for the BLF/Directed Call Park button. This field supports internationalization. If your phone does not support internationalization, the system uses the text that appears in the Label ASCII field.
Service URL	
Button Service	Enter the name of the service. If the service is not marked as an enterprise subscription, the service name appears in areas where you can subscribe to a service; for example, under Cisco Unified Communications Self Care Portal. Enter up to 32 characters for the service name.
Label	Enter the text that you want to appear for the Service URL button.
Device Settings	
Device Name	Enter a name to identify the device that uses this UDT. For device names that are not based on a MAC address, as a general rule, you can enter 1 to 15 characters comprised of alphanumeric characters (a-z, A-D, 0-9). In most cases, you can also enter dot (.), dash (-), and underscore (_).
Owner User ID	From the drop-down list box, select the User ID that you want to assign as the device owner for devices that use this UDT. By default, this field is set to the **Current Device Owner's User ID**. If this option is configured, when you use this UDT to create a device in the Quick User/Phone Add menu, the user ID under which you create the device is assigned as the device owner. In addition, if self provisioning is enabled for a user, when that user logs into the device for the first time, the device is created automatically with that user's user ID as the device owner. You may also select a specific user ID as the device owner for all devices that use this UDT. If you choose this option, when you use this UDT to create a device in the Quick User/Phone Add menu, regardless of which user you use to create the device, Cisco Unified Communications Manager assigns the user ID in the UDT Owner User ID drop-down list box as the device owner.
Mobility User ID	From the drop-down list box, select the user ID of the assigned mobility user. You can either select a user ID to own all devices created using this UDT, or select **Current Device Owner's User Id** to have the user who the devices are created for (using this UDT) as the owner of the device. **Tip** Assign the element that represents the user ID to the UDT to associate the UDT to the user or owner ID.

Field	Description
Join Across Lines	From the drop-down list box, enable or disable the Join Across Lines feature or select Default to use the service parameter setting. **Off** This setting disables the Join Across Lines feature. **On** This setting enables the Join Across Lines feature. **Default** This setting uses the Join Across Lines setting that is in the service parameter.
Always Use Prime Line	From the drop-down list box, choose one of the following options: **Off** When a device is idle and receives a call on any line, a user answers the call from the line on which the call is received. **On** When a device is idle (off hook) and receives a call on any line, the primary line is chosen for the call. Calls on other lines continue to ring, and the user must select those other lines to answer these calls. **Default** Unified CM uses the configuration from the Always Use Prime Line service parameter, which supports the Cisco CallManager service.

Field	Description
Always Use Prime Line for Voice Message	From the drop-down list box, choose one of the following options: **On** If a device is idle, the primary line becomes the active line for retrieving voice messages when a user presses the Messages button. **Off** If a device is idle, pressing the Messages button automatically dials the voice-messaging system from the line that has a voice message. Unified CM always selects the first line that has a voice message. If no line has a voice message, the primary line gets used when a user presses the Messages button. **Default** Unified CM uses the configuration from the Always Use Prime Line for Voice Message service parameter, which supports the Cisco CallManager service.
Single Button Barge	From the drop-down list box, enable or disable the Single Button Barge/cBarge feature for this UDT or choose Default to use the service parameter setting. **Off** This setting disables the Single Button Barge/cBarge feature; however, the regular Barge or cBarge features still work. **Barge** This setting enables the Single Button Barge feature. **CBarge** This setting enables the Single Button cBarge feature. **Default** Uses the Single Button Barge/cBarge setting that is in the service parameter. For more information, see “Barge and Privacy” in the *Cisco Unified Communications Manager Features and Services Guide*.

Field	Description
Privacy	For privacy on this UDT, select **On** in the Privacy drop-down list box. For more configuration information, see "Barge and Privacy" in the *Cisco Unified Communications Manager Features and Services Guide*.
Built in Bridge	Enables or disables the built-in conference bridge for the barge feature (select **On**, **Off**, or **Default**). For more information, see "Barge and Privacy" in the *Cisco Unified Communications Manager Features and Services Guide* and the *Cisco Unified Communications Manager Security Guide*.
Allow Control of Device from CTI	Check this check box to allow CTI to control and monitor this UDT. If the associated directory number specifies a shared line, you should check the check box as long as at least one associated device specifies a combination of device type and protocol that CTI supports.
Hotline Device	Check this check box to enable Hotline device for this UDT. Hotline devices can only connect to other Hotline devices. This feature is an extension of PLAR, which configures a device 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.
Logged into Hunt Group	This check box indicates that this UDT is currently signed in to a hunt list (group). When this UDT is added to a hunt list, the administrator can sign the user in or out by checking or unchecking this check box. Users use the softkey on a device to sign in or out of the hunt list.

Field	Description
Retry Video Call as Audio	This check box applies only to video endpoints that receive a call. If devices using this UDT receive a call that does not connect as video, the call tries to connect as an audio call. By default, the system checks this check box to specify that devices on this UDT should immediately retry a video call as an audio call (if it cannot connect as a video call) prior to sending the call to call control for rerouting. If you uncheck this check box, a video call that fails to connect as video does not try to establish as an audio call. The call then fails to call control, and call control routes the call via Automatic Alternate Routing (AAR), route list, or hunt list.
Ignore Presentation Indicators (internal calls only)	Check this check box to configure call display restrictions on a call-by-call basis. When this check box is checked, Unified CM ignores any presentation restriction that is received for internal calls. 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 connected line display information for each call. For more information about call display restrictions, see the "Call Display Restrictions" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
Enable Extension Mobility	Check this check box if to allow this UDT to support extension mobility.
Require Off-Premise Location	Check this check box if the device inserted with this template requires off-premise location update upon the registration. Off-premise location update is required when the device location cannot be detected automatically by Cisco Emergency Responder. Check this check box only for the template that remote or mobile devices use, which have frequent location change.
Device Routing	
SIP Dial Rules	If required, select the appropriate SIP dial rule. SIP dial rules provide local dial plans for this UDT, so users do not have to press a key or wait for a timer before the call is processed. Leave the SIP Dial Rules field set to **None** if you do not want dial rules to apply to this UDT. This means that the user must use the dial softkey or wait for the timer to expire before the call gets processed.

Field	Description
Calling Search Space	From the drop-down list box, select the appropriate calling search space (CSS). A CSS comprises a collection of partitions that are searched to determine how a dialed number should be routed. The calling search space for this UDT and the calling search space for the directory number are used together. The directory number CSS takes precedence over the device CSS. For more information, see "Partitions and Calling Search Spaces" in the *Cisco Unified Communications Manager System Guide*.
Calling Party Transformation CSS for Inbound Calls	This setting allows you to localize the calling party number on this UDT for inbound calls. Make sure that the Calling Party Transformation CSS that you select contains the calling party transformation pattern that you want to assign to this UDT. **Tip** Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the Calling Party Transformation CSS for Inbound Calls as None, the transformation does not match and is not applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.
Calling Party Transformation CSS for Outbound Calls	This setting allows you to localize the calling party number on this UDT for outbound calls. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this UDT. **Tip** Before the call occurs, the UDT must apply the transformation by using digit analysis. If you configure the Calling Party Transformation CSS for Outbound Calls as None, the transformation does not match and is not applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.
Rerouting Calling Search Space	From the drop-down list box, select a calling search space to use for rerouting. The rerouting calling search space of the referrer is used to find the route to the refer-to target. When the Refer fails due to the rerouting calling search space, the Refer Primitive rejects the request with the `405 Method Not Allowed` message. The redirection (3xx) primitive and transfer feature also uses the rerouting calling search space to find the redirect-to or transfer-to target.

Field	Description
SUBSCRIBE Calling Search Space	Supported with the BLF Presence feature, the SUBSCRIBE calling search space determines how Unified CM routes BLF presence requests that come from this UDT. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the UDT. From the drop-down list box, select the SUBSCRIBE calling search space to use for BLF presence requests for this UDT. All calling search spaces that you configure in Unified CM Administration appear in the SUBSCRIBE Calling Search Space drop-down list box. If you do not select a different calling search space for the end user from the drop-down list, the SUBSCRIBE calling search space defaults to None.
Use Device Pool Calling Party Transformation CSS for Inbound Calls	To use the Calling Party Transformation CSS that is configured in the device pool that is assigned to this UDT, check this check box. If you do not check this check box, this UDT uses the Calling Party Transformation CSS setting for inbound calls.
Use Device Pool Calling Party Transformation CSS for Outbound Calls	To use the Calling Party Transformation CSS that is configured in the device pool that is assigned to this UDT, select this check box. If you do not select this check box, the UDT uses the Calling Party Transformation CSS for outbound calls that you selected in the Phone Configuration window.
Phone Settings	
Common Profile	From the drop-down list box, select a common phone profile from the list of available common phone profiles. Select View Details for specific details about each common phone profile.
Common Device Configuration	From the drop-down list box, you can select a common device configuration that was configured in the Common Device Configuration window. Select View Details for specific details about each common device configuration.
Softkey Template	From the drop-down list box, select a softkey template. Leave the softkey template set to <None> to use the softkey template configured in the assigned Common Phone Profile.

Field	Description
Feature Control Policy	From the drop-down list box, select a feature control policy that has already been configured in the Feature Control Policy configuration window (**Device** > **Device Settings** > **Feature Control Policy** Leave the softkey template set to <None> to use the feature control policy configured in assigned Common Phone Profile.
Phone Personalization	The Phone Personalization setting allows you to enable this UDT so that it works with Phone Designer. Phone designer is a Cisco Unified Communications widget that allows a user to customize the wallpaper and ring tones on a device. From the Phone Personalization drop-down list box, select one of the following options: **Disabled** The user cannot customize this UDT by using Phone Designer. **Enabled** The user can use Phone Designer to customize this UDT. **Default** This UDT uses the configuration from the Phone Personalization enterprise parameter. **Note** You must install and configure Phone Designer, so a user can customize the device.
Protocol Settings	
MTP Preferred Originating Codec	From the drop-down list box, select the codec to use if a media termination point is required for SIP calls.
Digest User	Select an end user that you want to associate with this UDT for this setting that is used with digest authentication (SIP security). **Note** Ensure that you configured digest credentials for the user that you choose, as specified in the End User setting window. After you save the UDT and apply the setup update to the device, the digest credentials for the user is added to the phone configuration file. For more information about digest authentication, see the *Cisco Unified Communications Manager Security Guide*.

Field	Description
Outbound Call Rollover	Use this setting if you are creating this UDT for a Cisco Unified IP Phone 7931. **No Rollover** Conference and transfer do not work in this mode. If a user attempts to use either of these features, the phone status displays as Error Pass Limit. **Note** Choose this setting only if you need to support CTI applications. **Rollover Within Same DN** Conferences and call transfers complete by using the same directory number (on different lines). For example, consider a phone that has directory number 1506 that is assigned to both Line 6 and 7. The user has an active call on Line 6 and decides to transfer the call. When the user presses the Transfer button, the call on Line 6 gets placed on hold, and a new call initiates on Line 7 to complete the transfer. **Rollover to any line** Conferences and call transfers complete by using a different directory number and line than the original call. For example, consider a phone that has directory number 1507 assigned to Line 8 and directory number 1508 assigned to Line 9. The user has an active call on Line 8 and decides to transfer the call. When the user presses the Transfer button, the call on Line 8 is placed on hold, and a new call initiates on Line 9 to complete the transfer.
Media Termination Point Required	Check this check box if you want to use an MTP to implement features that H.323 does not support (such as hold and transfer). Uncheck this check box if you do not want to use an MTP to implement features. **Note** Check this check box only for H.323 clients and those H.323 devices that do not support the H.245 empty capabilities set or if you want media streaming to terminate through a single source. If you check this check box to require an MTP and a device becomes the endpoint of a video call, the call will be audio only.
Unattended Port	Check this check box to indicate an unattended port on this UDT.

Field	Description
Require DTMF Reception	Check this check box to require DTMF reception for this UDT. **Note** In configuring Cisco Unified Mobility features, when using intercluster DNs as remote destinations for an IP phone via SIP trunk (either intercluster trunk [ICT] or gateway), check this check box so that DTMF digits can be received out of band, which is crucial for Enterprise Feature Access midcall features.
IP Phone Services Subscription	
Select the **Subscribe** button and select the service. If the service is not marked as an enterprise subscription, the service name appears in areas where you can subscribe to a service. Enter up to 128 characters for the service name. For Java MIDlet services, the service name must exactly match the name that is defined in the Java Application Descriptor (JAD) file. **Note** You must configure IP Phone services and save them before you can configure Service URL Buttons. **Note** Unified CM allows you to create two or more IP phone services with identical names. Cisco recommends that you do not do so unless most or all phone users are advanced, or unless an administrator always configures the IP phone services. Be aware that if AXL or any third-party tool accesses the list of IP phone services for configuration, you must use unique names for IP phone services.	
Security Settings	
General Security Settings	

Field	Description
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Unified CM inserts a trusted relay point (TRP) device with this media endpoint. Select one of the following values: **Default** If you select this value, the UDT uses the Use Trusted Relay Point setting from the common device configuration. **Off** Select this value to disable the use of a TRP with this UDT. This setting overrides the Use Trusted Relay Point setting in the common device configuration. **On** Select this value to enable the use of a TRP with this UDT. This setting overrides the Use Trusted Relay Point setting in the common device configuration. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Unified CM places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVPAgent). If both TRP and MTP are required for the endpoint, TRP is used as the required MTP. For information about call behavior, see "TRP Insertion in Cisco Unified Communications Manager" in the *Cisco Unified Communications Manager System Guide*. If both TRP and RSVPAgent are needed for the endpoint, Unified CM 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 CM first tries to find a transcoder that is also designated as a TRP. For more information about network virtualization and trusted relay points, see the Trusted Relay Point section and its subtopics in the "Media Resource Management" chapter of the *Cisco Unified Communications Manager System Guide*.

Field	Description
Protected Device	Check this check box to designate this UDT as protected, which enables a device to play a 2-second tone to notify the user when a call is encrypted and both devices are configured as protected. The tone plays for both parties when the call is answered. The tone does not play unless both devices are protected and the call occurs over encrypted media. This setting represents only one of several configuration requirements for the secure indication tone to play. For more information about the secure indication tone feature and the configuration requirements, see the *Cisco Unified Communications Manager Security Guide*. **Note** If you check this check box and the system determines that the call is not encrypted, a device plays an indication tone to alert the user that the call is not protected.
Certificate Authority Proxy Function (CAPF) Settings	

Field	Description
Authentication Mode	This field allows you to choose the authentication method that this UDT uses during the CAPF certificate operation. From the drop-down list box, select one of the following options: **By Authentication String** Installs/upgrades, deletes, or troubleshoots a locally significant certificate only when the user enters the CAPF authentication string on the UDT. **By Null String** Installs/upgrades, deletes, or troubleshoots a locally significant certificate without user intervention. **Note** This option provides no security; Cisco strongly recommends that you choose this option only for closed, secure environments. **By Existing Certificate (Precedence to LSC)** Installs/upgrades, deletes, or troubleshoots a locally significant certificate if a manufacture-installed certificate (MIC) or locally significant certificate (LSC) exists in the UDT. If a LSC exists in the UDT, authentication occurs via the LSC, regardless of whether a MIC exists in the UDT. If a MIC and LSC exist in the UDT, authentication occurs via the LSC. If a LSC does not exist in the UDT, but a MIC does exist, authentication occurs via the MIC. At any time, the UDT uses only one certificate to authenticate to CAPF even though a MIC and LSC can exist in the UDT at the same time. If the primary certificate, which takes precedence, becomes compromised for any reason, or, if you want to authenticate via the other certificate, you must update the authentication mode. **By Existing Certificate (Precedence to MIC)** Installs, upgrades, deletes, or troubleshoots a locally significant certificate if a LSC or MIC exists in the UDT. If a MIC exists in the UDT, authentication occurs via the MIC, regardless of whether a LSC exists in the UDT. If a LSC exists in the UDT, but a MIC does not exist, authentication occurs via the LSC. **Note** The CAPF settings that are configured in the Phone Security Profile window interact with the CAPF parameters that are configured in the Phone Configuration window.

Field	Description
Authentication String	If you select the By Authentication String option in the Authentication Mode drop-down list box, this field applies. Manually enter a string or select the **Generate String** button to generate a string. **Note** Ensure that the string contains 4 to 10 digits. To install, upgrade, delete, or troubleshoot a locally significant certificate, a user or administrator must enter the authentication string on a device.
Key Size (Bits)	For this setting that is used for CAPF, select the key size for the certificate from the drop-down list box. The default setting equals 1024. Other options include 512 and 2048. **Note** If you select a higher key size than the default setting, the UDT takes longer to generate the entropy that is required to generate the keys. Key generation, which is set at low priority, allows the UDT to function while the action occurs. Key generation takes up to 30 or more minutes to complete. **Note** The CAPF settings that are configured in the Phone Security Profile window interact with the CAPF parameters that are configured in the Phone Configuration window.
Service Configuration Settings	
Information	Enter the location (URL) of the help text for the information button. Leave this field blank to accept the default setting.
Directory	Enter the server from which the UDT obtains directory information. Leave this field blank to accept the default setting.
Messages	Leave this field blank (not used by Unified CM).
Services	Enter the location (URL) for IP phone services.
Authentication Server	Enter the URL that the UDT uses to validate requests that are made to the web server. If you do not provide an authentication URL, the advanced features for UDT that require authentication do not function. By default, this URL accesses a Cisco Unified Communications Self Care Portal window that was configured during installation. Leave this field blank to accept the default setting.

Field	Description
Proxy Server	Enter the host and port (for example, proxy.cisco.com:80) that are used to proxy HTTP requests for access to non-local host addresses from the HTTP client. The rule contains two parts for when to use the proxy server parameter: • The hostname contains a "." • The hostname specifies an IP address in any form. If you do not configure this URL, the UDT attempts to connect directly to the URL. To accept the default setting, leave this field blank.
Idle	Enter the URL that appears on the display when the UDT device is not used for the time that is specified in Idle Timer field. For example, you can display a logo on the LCD when the UDT device is not used for 5 minutes. To accept the default setting, leave this field blank.
Idle Timer (seconds)	Enter the time (in seconds) that you want to elapse before the URL that is specified in the Idle field appears. To accept the value of the Idle URL Timer enterprise parameter, leave this field blank.
Secure Authentication URL	Enter the secure URL that the UDT device uses to validate requests that are made to the web server. **Note** If you do not provide a Secure Authentication URL, a device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, a device chooses the appropriate URL, based on its capabilities. By default, this URL accesses a Cisco Unified Communications Self Care Portal window that was configured during installation. Leave this field blank to accept the default setting. Maximum length: 255
Secure Directory URL	Enter the secure URL for the server from which the UDT obtains directory information. This parameter specifies the URL that this UDT uses when you press the Directory button. **Note** If you do not provide a Secure Directory URL, a device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, a device chooses the appropriate URL, based on its capabilities. Leave this field blank to accept the default setting. Maximum length: 255

Field	Description
Secure Idle URL	Enter the secure URL for the information that appears on the display when this UDT is idle, as specified in Idle Timer field. For example, you can display a logo on the LCD when the UDT is not used for 5 minutes. **Note** If you do not provide a Secure Idle URL, a device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, a device chooses the appropriate URL, based on its capabilities. To accept the default setting, leave this field blank. Maximum length: 255
Secure Information URL	Enter the secure URL for the server location where the UDT can find help text information. This information appears when the user presses the information (I) button or the question mark (?) button. **Note** If you do not provide a Secure Information URL, this UDT uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, this UDT selects the appropriate URL, based on its capabilities. To accept the default setting, leave this field blank. Maximum length: 255
Secure Messages URL	Enter the secure URL for the messages server. This UDT contacts this URL when the user presses the Messages button. **Note** If you do not provide a Secure Messages URL, a device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, a device chooses the appropriate URL, based on its capabilities. To accept the default setting, leave this field blank. Maximum length: 255
Secure Services URL	Enter the secure URL for Cisco Unified IP Phone services. The Secure Services URL is the location that the UDT contacts when the user presses the Services button. **Note** If you do not provide a Secure Services URL, a device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, a device chooses the appropriate URL, based on its capabilities. To accept the default setting, leave this field blank. Maximum length: 255

Field	Description
Services Provisioning	From the drop-down list box, select how the UDT supports the services: **Internal** The UDT uses the phone configuration file to support the service. Select this option or Both for Cisco-provided default services where the Service URL was not updated; that is, the service URL indicates Application:Cisco/<name of service>; for example, Application:Cisco/CorporateDirectory. Select Internal or Both for Cisco-signed Java MIDlets because Cisco-signed Java MIDlets are provisioned in the configuration file. **External URL** Selecting External URL indicates that the UDT ignores the services in the phone configuration file and retrieves the services from a Service URL. If you configure a custom Service URL for a service, including a Cisco-provided default service, you must choose either External URL or Both; if you choose Internal in this case, the services that are associated with the custom URLs do not work on the UDT. **Both** Selecting Both indicates that the UDT supports both the services that are defined in the configuration file and external applications that are retrieved from service URLs.
Troubleshooting Settings	

Field	Description
Packet Capture Mode	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. Choose one of the following options from the drop-down list box: **None** This option, which serves as the default setting, indicates that no packet capturing is occurring. After you complete packet capturing, configure this setting. **Batch Processing Mode** Unified CM writes the decrypted or nonencrypted messages to a file, and the system encrypts each file. The system creates a new file daily with a new encryption key. Unified CM, which stores the file for seven days, also stores the keys that encrypt the file in a secure location. Unified CM stores the file in the PktCap virtual directory. A single file contains the time stamp, source IP address, source IP port, destination IP address, packet protocol, message length, and the message. The TAC debugging tool uses HTTPS, administrator username and password, and the specified day to request a single encrypted file that contains the captured packets. Likewise, the tool requests the key information to decrypt the encrypted file. For more information about packet capturing, see the *Troubleshooting Guide for Cisco Unified Communications Manager*.
Packet Capture Duration	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. This field specifies the maximum number of minutes that is allotted for one session of packet capturing. The default setting equals 0, although the range exists from 0 to 300 minutes. To initiate packet capturing, enter a value other than 0 in the field. After packet capturing completes, the value, 0, appears. For more information about packet capturing, see the *Cisco Unified Communications Manager Troubleshooting Guide*.

Field	Description
Secure Shell User	Enter a user ID for the secure shell user. You can enter any alphanumeric or special characters up to 50 characters. Invalid characters include ", %, &, <, >, and \. This field appears when the UDT supports SSH access. Cisco Technical Assistance Center (TAC) uses secure shell for troubleshooting and debugging. Contact TAC for further assistance. For more information about how to configure encrypted phone configuration files to ensure that the Unified CM does not send unencrypted SSH credentials to the UDT device, see the *Cisco Unified Communications Manager Security Guide*.
Secure Shell Password	Enter the password for a secure shell user. You can enter any alphanumeric or special characters up to 200 characters. Invalid characters include ", %, &, <, >, and \. Contact TAC for further assistance. For more information about configuring encrypted phone files to ensure that Unified CM does not send unencrypted SSH passwords to the UDT device, see the *Cisco Unified Communications Manager Security Guide*.
Locale Settings	
User Locale	From the drop-down list box, select the locale that is associated with the UDT. The user locale identifies a set of detailed information to support users, including language and font. **Note** If no user locale is specified, Unified CM uses the user locale that is associated with the device pool. **Note** If the users require that information appear in any language other than English, verify that the locale installer is installed before you configure the user locale. See the Unified CM Locale Installer documentation.
Network Locale	From the drop-down list box, select the locale that is associated with the UDT. The network locale contains a definition of the tones and cadences that the UDT in a specific geographic area uses. **Note** If no network locale is specified, Unified CM uses the network locale that is associated with the device pool. **Note** If users require that country-specific tones be played, verify that the locale is installed before ypu configure the network locale. See the Unified CM Locale Installer documentation.
Multilevel Precedence Preemption (MLPP) Settings	

Field	Description
MLPP Domain	Select an MLPP domain from the drop-down list box for the MLPP domain that is associated with this UDT. If you leave the **None** value, devices with this UDT inherit the MLPP domain from the value that was set for the device pool. If the device pool does not have an MLPP domain setting, this UDT inherits its MLPP domain from the value that was set for the MLPP Domain Identifier enterprise parameter.
MLPP Indication	If available, this setting specifies whether a device that can play precedence tones uses the capability when it places an MLPP precedence call. From the drop-down list box, select a setting to assign to this UDT from the following options: **Default** This UDT inherits its MLPP indication setting from its device pool. **Off** This UDT does not handle nor process indication of an MLPP precedence call. **On** This UDT does handle and process indication of an MLPP precedence call. **Note** Do not configure a UDT with the following combination of settings: MLPP Indication is set to **Off** or **Default** (when default is **Off**) while MLPP Preemption is set to **Forceful**. **Note** Turning on MLPP Indication (at the enterprise parameter, device pool, or device level) disables normal Ring Setting behavior for the lines on a device, unless MLPP Indication is turned off (overridden) for the UDT.

Field	Description
MLPP Preemption	If available, this setting specifies whether this UDT that can preempt calls in progress uses the capability when it places an MLPP precedence call. From the drop-down list box, select a setting to assign to this UDT from the following options: **Default** This UDT inherits its MLPP preemption setting from its device pool. **Disabled** This UDT does not allow preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. **Forceful** This UDT allows preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. **Note** Do not configure a UDT with the following combination of settings: MLPP Indication is set to **Off** or **Default** (when default is **Off**) while MLPP Preemption is set to **Forceful**.
Do Not Disturb (DND) Settings	
Do Not Disturb	Check this check box to enable Do Not Disturb (DND) for this UDT.

Field	Description
DND Option	When you enable DND on the UDT, this parameter allows you to specify how the DND features handle incoming calls: **Call Reject** This option specifies that no incoming call information is presented to the user. Depending on how you configure the DND Incoming Call Alert parameter, the UDT 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 UDT, so the user can accept the call. **Use Common Phone Profile Setting** This option specifies that the device on the UDT uses the DND Option setting from the Common Phone Profile window. **Note** For 7940 and 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 is presented to the device.

Field	Description
DND Incoming Call Alert	When you enable the DND Ringer Off or Call Reject option, this parameter specifies how a call appears on a device. From the drop-down list, select one of the following options: **None** This option specifies that this UDT uses the DND Incoming Call Alert setting from the Common Phone Profile window. **Disable** This option disables both beep and flash notification of a call, but, for the DND Ringer Off option, incoming call information still appears. For the DND Call Reject option, no call alerts appear, and no information is sent to the UDT. **Beep Only** For an incoming call, this option causes the associated device to play a beep tone only. **Flash Only** For an incoming call, this option causes the associated device to display a flash alert.
Automatic Alternate Routing (AAR) Settings	
AAR Group	Select the automated alternate routing (AAR) group for this UDT. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. If no AAR group is specified, Unified CM uses the AAR group that is associated with Device Pool or Line.
AAR Calling Search Space	Select the appropriate calling search space for this UDT to use when it performs automated alternate routing (AAR). 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.
Busy Lamp Field Settings	

Field	Description
BLF Presence Group	Configure this field with the BLF Presence feature. From the drop-down list box, select a BLF presence group for this UDT. The selected group specifies the devices, end users, and application users that can monitor this directory number. The default value for BLF Presence Group specifies Standard Presence group, configured with installation. BLF presence groups that are configured in Unified CM Administration also appear in the drop-down list box. Presence authorization works with BLF presence groups to allow or block presence requests between groups. For more information about how to configure permissions between groups and how presence works with Cisco Extension Mobility, see the "BLF Presence" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
BLF Audible Alert Setting (Phone Idle)	This setting determines the busy lamp field (BLF) audible alert setting when no current call exists on the BLF DN: **On** An audible alert sounds. **Off** No audible alert sounds. **Default** The configuration in the Service Parameters Configuration window determines the alert option.
BLF Audible Alert Setting (Phone Busy)	This setting determines the BLF audible alert setting when at least one active call exists on the BLF DN, but no call pickup alerts exist: **On** An audible alert sounds. **Off** No audible alert sounds. **Default** The configuration in the Service Parameters Configuration window determines the alert option.
Music on Hold Settings	

Field	Description
User Hold MOH Audio Source	To specify the audio source that plays when a user initiates a hold action, select an audio source from the drop-down list box. If you do not select an audio source, Unified CM uses the audio source that is defined in the device pool or the system default if the device pool does not specify an audio source ID. **Note** You define audio sources in the Music On Hold Audio Source Configuration window. For access, select **Media Resources** > **Music on Hold Audio Source**.
Network Hold MOH Audio Source	To specify the audio source that plays when the network initiates a hold action, select an audio source from the drop-down list box. If you do not choose an audio source, Unified CM uses the audio source that is defined in the device pool or the system default if the device pool does not specify an audio source ID. **Note** You define audio sources in the Music On Hold Audio Source Configuration window. For access, select **Media Resources** > **Music on Hold Audio Source**.
Location Settings	
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 box, select the appropriate location for this UDT. A location setting of **Hub_None** means that the locations feature does not keep track of bandwidth. A location setting of **Phantom** specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the **System** > **Location Info** > **Location** menu option. For more information about location-based CAC across intercluster trunks, see "Location-Based Call Admission Control Over Intercluster Trunk" in the *Cisco Unified Communications Manager System Guide*.
Geolocation	From the drop-down list box, select a geolocation. You can select the **Unspecified** geolocation, which designates that this UDT does not associate with a geolocation. You can also select a geolocation that is configured with the **System** > **Geolocation Configuration** menu option.

Field	Description
Device Mobility Mode	From the drop-down list box, turn the device mobility mode on or off for this UDT or select **Default** to use the default device mobility mode. The default setting uses the value for the Device Mobility Mode service parameter. Click **View Current Device Mobility Settings** to display the current values of these device mobility parameters: • Cisco Unified Communications Manager Group • Roaming Device Pool • Location • Region • Network Locale • AAR Group • AAR Calling Search Space • Device Calling Search Space • Media Resource Group List • SRST For more information, see "Device Mobility" in the *Cisco Unified Communications Manager Features and Services Guide*.
Media Resource Group List	Select the appropriate Media Resource Group List. A Media Resource Group List comprises a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from the available media resources according to the priority order that is defined in a Media Resource Group List. If you choose **None**, Unified CM uses the Media Resource Group List that is defined in the device pool. For more information, see the "Media Resource Management" section in the *Cisco Unified Communications Manager System Guide*.

Field	Description
Remote Device	If you are experiencing delayed connect times over SCCP pipes to remote sites, check the Remote Device check box. Checking this check box tells Unified CM to allocate a buffer for the UDT when it registers and to bundle SCCP messages. **Tip** Because this feature consumes resources, be sure to check this check box only when you are experiencing signaling delays for phones that are running SCCP. Most users do not require this option. Unified CM sends the bundled messages to the UDT when the station buffer is full, as soon as it receives a media-related message, or when the Bundle Outbound SCCP Messages timer expires. **Note** To specify a setting other than the default setting (100 msec) for the Bundle Outbound SCCP Messages timer, set up a new value in the Service Parameters Configuration window for the Cisco CallManager service. Although 100 msec specifies the recommended setting, you may enter 15 msec to 500 msec.

Related Topics

About Universal Device Template Display Preference Setup

About Universal Line Template Setup

The Universal Line Template (ULT) feature allows you to create templates with settings that you would normally apply to a directory number. You can create one or more ULTs to reflect your most common directory number configurations, and apply the templates when adding a new directory number on the **Quick User/Phone Add** window.

Tip To make the window easier to view, the template sections are collapsed by default. Expand sections that you need as you walk through the template setup process. Select the **Expand All** button to expand all sections.

Note The ULT sections in this window may appear in a different order than the settings table indicates. To change the order of these settings, use the **User Management** > **User/Phone Add** > **Page Layout Preference** menu.

Universal Line Template Settings

The following table provides descriptions of all possible fields that display when you add or update a Universal Line Template (ULT).

Table 135: Universal Line Template Settings

Field	Description
Template Information	
Name	Enter a unique name for the ULT.
Urgent priority	If the dial plan contains overlapping patterns, Cisco Unified Communications Manager (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 Unified Communications Manager must route a call immediately.
Required and Frequently Entered Settings	
Line Description	Enter a description for the ULT. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand ('), or angle brackets (<>). **Tip** Select the pencil icon to place tokens in the description. Tokens are variables that are replaced with actual values, after you create this ULT. For example, the token “#Lastname#s desk phone” becomes “Smith's desk phone” for a user with the last name “Smith.”
Route Partition	Select a route partition to which the directory number belongs. **Note** The directory number can appear in more than one partition.
Voice Mail Profile	Select this parameter to make the pilot number the same as the directory number for this line. This action proves useful if you do not have a voice-messaging server that is configured for devices on this ULT.
Calling Search Space	Choose partitions that are searched for numbers that are called from this directory number. **Note** Changes cause an update of Pickup Group Names that are listed in the **Call Pickup Group** field. The setting applies to all devices that use this ULT.
Alerting Name	This name represents the name that displays during an alert to a shared directory number. For non-shared directory numbers, during alerts, the system uses the name that is entered in the **Display** field. **Tip** Select the pencil icon to place tokens in the description. Tokens are variables that are replaced with actual values, after you create this ULT. For example, the token “#Lastname#s desk phone” becomes “Smith's desk phone” for a user with the last name “Smith.” **Note** Do not use the word Voicemail anywhere in your Alerting Name. Use of the word Voicemail can cause Cisco Unity Connection to process the call as a direct call rather than as a forwarded call.
Directory Number Settings	

Field	Description
BLF Presence Group	Used with the BLF Presence feature, the directory number serves as the presence entity; that is, watchers request the status of the directory number, so the real-time status of the directory number displays on the device. If you want the phone to receive the status of the presence entity, make sure that the BLF Presence group of the watcher is allowed to view the status of the BLF Presence group that is applied to the directory number, as indicated in the **Presence Group Configuration** window. For information about the BLF Presence feature, refer to the *Cisco Unified Communications Manager Features and Services Guide*.
Call Pickup Group	This field determines the type of notification an incoming call sends to members of a call pickup group. If the called device does not answer, the devices in the call pickup group hear a short ring (ring once) or hear nothing (disabled). **Use System Default** The value of this field gets determined by the setting of the Cisco CallManager service parameter Call Pickup Group Audio Alert Setting of Idle Station. **Disable** No alert is sent to members of the call pickup group. **Ring Once** A short ring is sent to members of the call pickup group.

Field	Description
Party Entrance Tone	From the Party Entrance Tone drop-down list box, select one of the following options: **Default** Use the value that you configured in the Party Entrance Tone service parameter. **On** A tone plays on the phone when a basic call changes to a multiparty call, that is, a barge call, cBarge call, ad hoc conference, meet-me conference, or a joined call. In addition, a different tone plays when a party leaves the multi-party call. • If the originator of the multiparty call has a built-in bridge, the tone is played to all parties if you select On for the controlling device. • When the controlling device leaves the call, Unified Communications Manager identifies whether another device on the call can play the tone. • If another device on the call can play the tone, Unified Communications Manager plays the tone. • If the controlling device cannot play the tone, Unified Communications Manager does not play the tone even if you enable the party entrance tone feature. **Off** A tone does not play on the phone when a basic call changes to a multiparty call.
Auto Answer	Select one of the following options to activate the Auto Answer feature for this ULT: • Auto Answer Off <Default> • 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. Do not configure Auto Answer for devices that have shared lines.
Reject anonymous calls	Check this check box to reject all anonymous calls for the DN. Anonymous calls are calls with no caller ID or that have caller ID blocked.
Music on Hold (MoH) Settings	

Field	Description
User Hold MoH Audio Source	Select the music on hold audio source to be played when the user presses HOLD to place a call on hold.
Network Hold MoH Audio Source	Select the music on hold audio source to be played when the system places a call on hold while the user transfers a call or initiates a conference or call park.
Automatic Alternate Route (AAR) Settings	
AAR Destination Mask	The settings in this field specify treatment of calls for which insufficient bandwidth exists to reach the destination. Automated alternate routing (AAR) handles calls that are routed to the AAR Destination Mask or Voice Mail. Configure the following value: **Voice Mail** Select this option to use settings in the Voice Mail Profile Configuration window.
AAR Group	Select the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. Set AAR Group to <None> to prevent rerouting blocked calls.
Retain this destination in the call forwarding history	Checking this check box allows the AAR leg of the call to be present in the Call History. By default, the directory number configuration retains the AAR leg of the call in the call history, which ensures that the AAR forward to voice-message system prompts the user to leave a voice message.
Call Forward Settings: Call Forward All	

Field	Description
Forward Destination For All Calls	The settings in this row of fields specify how calls forwarded to this directory number behave if the directory number is set to forward all calls. The CSS field is used to validate the Forward All destination that is entered when the user activates Call Forward All from the phone. This field also is used to redirect the call to the Call Forward All destination. Select one of the following options in the drop-down list box: **Voice Mail** Select this option to use settings in the **Voice Mail Profile Configuration** window. **Destination** This setting indicates the directory number to which all calls are forwarded. Enter any dialable phone number, including an outside destination. **Calling Search Space** This setting applies to all devices that use this directory number.
Primary Calling Search Space For Forwarding All Calls	Because call forwarding is a line-based feature, in cases where the device CSS is unknown, the system uses only the line CSS to forward the call. If the line CSS is restrictive and not routable, the forward attempt fails. Addition of a secondary CSS for Call Forward All provides a solution to enable forwarding. The primary CSS for Call Forward All and secondary CSS for Call Forward All are linked together (Primary CFA CSS + Secondary CFA CSS). Unified Communications Manager uses this combination to validate the CFA destination and to forward the call. See the description for the CSS field for information about how the combination of Primary and Secondary CFA CSSes works
Secondary Calling Search Space For Forwarding All Calls	Because call forwarding is a line-based feature, in cases where the device CSS is unknown, the system uses only the line CSS to forward the call. If the line CSS is restrictive and not routable, the forward attempt fails. A secondary CSS for Call Forward All provides a solution to enable forwarding. The primary CSS for Call Forward All and secondary CSS for Call Forward All get concatenated (Primary CFA CSS + Secondary CFA CSS). Unified Communications Manager uses this combination to validate the CFA destination and to forward the call. See the description for the CSS field for information about how the combination of Primary and Secondary CFA CSSes works.

Field	Description
Calling Search Space Activation Policy	

Field	Description
	Three values exist for this option: • Use System Default • With Configured CSS • With Activating Device/Line CSS **Use System Default** If you configure the CSS Activation Policy to use the System Default, then the CFA CSS Activation Policy cluster-wide service parameter determines which Forward All CSS is used. If the CFA CSS Activation Policy service parameter is set to With Configured CSS, then Forward All CSS and Secondary CSS for Forward All is used for Call Forwarding. If CFA CSS Activation Policy service parameter is set to With Activating Device/Line CSS, then Forward All CSS and Secondary CSS for Forward All is automatically populated with the Directory Number CSS and Device CSS for the activating device. **CFA Calling Search Space Activation Policy Service Parameter** Ensure the CFA CSS Activation Policy service parameter that displays in the Cluster-wide Parameters (Feature - Forward) section of the Service Parameter Configuration window is set correctly for call forward all to work as intended. The parameter specifies the following values: • With Configured CSS (default) • With Activating Device/Line CSS When the CSS Activation Policy is set to Use System Default, the value of the CFA CSS Activation Policy service parameter is used to determine the Call Forward All CSS. When the option With Configured CSS is selected, the primary and secondary CFA CSS is used. When the option With Activating Device/Line CSS is selected, the primary and secondary CFA CSS get updated with primary line CSS and activating Device CSS. **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.

Field	Description
	• 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. **With Configured Calling Search Space** If you select the With Configured CSS option, the Forward All CSS that is explicitly configured in the Directory Number Configuration window controls the forward all activation and call forwarding. If the Forward All CSS is set to None, no CSS is configured for Forward All. A forward all activation attempt to any directory number with a partition fails. No change in the Forward All CSS and Secondary CSS for Forward All occurs when forward all is activated. **With Activating Device/Line Calling Search Space** If you prefer to use the combination of the Directory Number CSS and Device CSS without configuring a Forward All CSS, select With Activating Device/Line CSS for the CSS Activation Policy. With this option, when Forward All is activated from the phone, the Forward All CSS and Secondary CSS for Forward All automatically is populated with the Directory Number CSS and Device CSS for the activating device. With this configuration (CSS Activation Policy set to With Activating Device/Line), if the Forward All CSS is set to None, when forward all is activated through the phone, the combination of Directory Number CSS and activating Device CSS is used to verify the forward all attempt.
Call Forward Settings: Call Forward Other: Forward	
Destination and Calling Search Space	In these fields, you can enter a destination and CSS to use with the **Apply To** options below. Use **Apply To** to quickly apply the same destination and CSS to Internal, External or all forwarding types below.

Field	Description
Busy - Internal Calls	The settings in this row of fields specify the forwarding treatment for internal calls to this directory number if the directory number is busy. See the description for the Busy Trigger field for information about when a line is considered busy. The call forward destination and CSS field get used to redirect the call to the forward destination. Select one of the following options in the drop-down list box: **Voice Mail** Select this option to use settings in the **Voice Mail Profile Configuration** window. **Destination** This setting indicates the directory number to which all calls are forwarded. Enter any dialable phone number, including an outside destination. **Calling Search Space** This setting applies to all devices that use this directory number.
Busy - External Calls	The settings in this row of fields specify the forwarding treatment for external calls to this directory number if the directory number is busy. See the description for the Busy Trigger field for information on when a line is considered busy. The call forward destination and CSS field get used to redirect the call to the forward destination. Select one of the following options in the drop-down list box: **Voice Mail** Select this option to use settings in the **Voice Mail Profile Configuration** window. **Destination** This setting indicates the directory number to which all calls are forwarded. Enter any dialable phone number, including an outside destination. **Calling Search Space** This setting applies to all devices that use this directory number.

Field	Description
No Answer - Internal Calls	The settings in this row of fields specify the forwarding treatment for internal calls to this directory number if the directory number does not answer. The call forward destination and CSS field get used to redirect the call to the forward destination. Select one of the following options in the drop-down list box: **Voice Mail** Select this option to use settings in the **Voice Mail Profile Configuration** window. **Destination** This setting indicates the directory number to which all calls are forwarded. Enter any dialable phone number, including an outside destination. **Calling Search Space** This setting applies to all devices that use this directory number.
No Answer - External Calls	The settings in this row of fields specify the forwarding treatment for external calls to this directory number if the directory number does not answer. The call forward destination and CSS field get used to redirect the call to the forward destination. Select one of the following options in the drop-down list box: **Voice Mail** Select this option to use settings in the **Voice Mail Profile Configuration** window. **Destination** This setting indicates the directory number to which all calls are forwarded. Enter any dialable phone number, including an outside destination. **Calling Search Space** This setting applies to all devices that use this directory number.

Field	Description
No Coverage - Internal Calls	For information about Call Coverage, see the *Cisco Unified Communications Manager System Guide*. The call forward destination and CSS field get used to redirect the call to the forward destination. Select one of the following options in the drop-down list box: **Voice Mail** Select this option to use settings in the **Voice Mail Profile Configuration** window. **Destination** This setting indicates the directory number to which all calls are forwarded. Enter any dialable phone number, including an outside destination. **Calling Search Space** This setting applies to all devices that use this directory number.
No Coverage - External Calls	For information about Call Coverage, see the *Cisco Unified Communications Manager System Guide*. The call forward destination and CSS field get used to redirect the call to the forward destination. Select one of the following options in the drop-down list box: **Voice Mail** Select this option to use settings in the **Voice Mail Profile Configuration** window. **Destination** This setting indicates the directory number to which all calls are forwarded. Enter any dialable phone number, including an outside destination. **Calling Search Space** This setting applies to all devices that use this directory number.
Unregistered - Internal Calls	This field applies to unregistered internal DN calls. The calls are rerouted to a specified Destination Number or Voice Mail. **Note** You must also specify the maximum number of forwards in the Service Parameters Configuration window for a Directory Number.

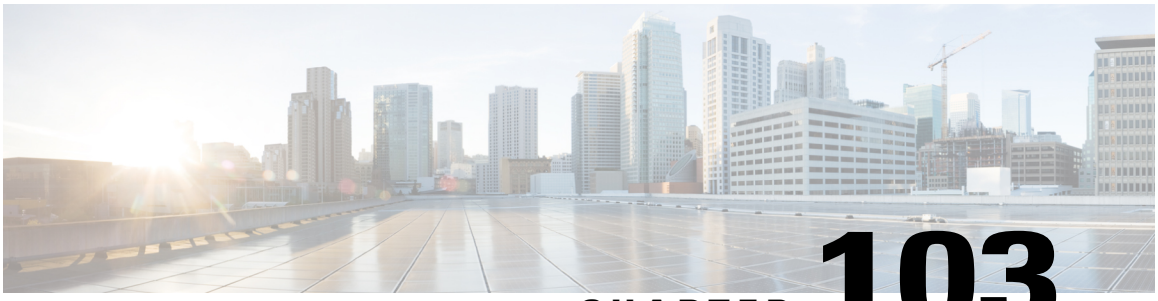
Field	Description
Unregistered - External Calls	This field applies to unregistered external DN calls. The calls are rerouted to a specified Destination Number or Voice Mail. **Note** You must also specify the maximum number of forwards in the Service Parameters Configuration window for a Directory Number.
CTI Failure	This field applies only to CTI route points and CTI ports. The settings in this row specify the forwarding treatment for external calls to this CTI route point or CTI port if the CTI route point or CTI port fails. Select one of the following options in the drop-down list box: **Voice Mail** Select this option to use settings in the **Voice Mail Profile Configuration** window. **Destination** This setting indicates the directory number to which all calls are forwarded. Enter any dialable phone number, including an outside destination. **Calling Search Space** This setting applies to all devices that use this directory number.
No Answer Ring Duration (seconds)	Used in conjunction with Call Forward No Answer Destination, this field sets the timer for how long the phone rings before it is forwarded. Leave this setting blank to use the value that is set in the Cisco CallManager service parameter Forward No Answer Timer. **Caution** By default, Unified Communications Manager makes the time for the T301 timer (specifies a timer for receiving the Alerting message) longer than the No Answer Ring Duration time; if the set time for the T301 timer expires before the set time for the No Answer Ring Duration expires, the call ends, and no call forwarding can occur. If you select to do so, you can configure the time for the No Answer Ring Duration to be greater than the time for the T301 timer. For information about the T301 timer, select **System** > **Service Parameters**; select the server, the Cisco CallManager service, and then select the parameter in the window that displays.
Park Monitoring Settings	

Field	Description
Forward Destination for External Calls When Not Retrieved	When the person whose call is parked is an external party, the call is forwarded to the specified destination in this field. If this field value is empty, the person whose call is parked is redirected to the line of the person who parked the call. Specify the following values: **Voice Mail** Select this option to use settings in the Voice Mail Profile Configuration window.
Calling Search Space for Forwarding External Calls When Not Retrieved	This setting specifies the directory number to which a parked call (from an external party) is forwarded when the service parameter Park Monitoring Forward No Retrieve Timer expires. Use any dialable phone number, including an outside destination. A CSS comprises an ordered list of route partitions that are typically assigned to devices. Calling search spaces determine the partitions that calling devices search when they are attempting to complete a call.
Forward Destination for Internal Calls When Not Retrieved	When the person whose call is parked is an internal party, the call is forwarded to the specified destination in this field. If this field value is empty, the person whose call is parked is redirected to the line of the person who parked the call. Specify the following values: **Voice Mail** Select this option to use settings in the Voice Mail Profile Configuration window.
Calling Search Space for Forwarding Internal Calls When Not Retrieved	This setting specifies the directory number to which a parked call (from an internal party) is forwarded when the service parameter Park Monitoring Forward No Retrieve Timer expires. Use any dialable phone number, including an outside destination. A CSS comprises an ordered list of route partitions that are typically assigned to devices. Calling search spaces determine the partitions that calling devices search when they attempt to complete a call.
Park Monitor Reversion Timer (seconds)	This parameter determines the number of seconds that Unified Communications Manager waits before prompting the user to retrieve a call that the user parked. This timer starts when the user presses the Park softkey on the phone, and a reminder is issued when the timer expires. The default is 60 seconds. **Note** If you configure a nonzero value, this value overrides the value of this parameter set in the Service Parameters window. However, if you configure a value of 0 here, then the value in the Service Parameters window is used.
Multilevel Precedence Preemption (MLPP) Alternate Party Settings	

Field	Description
Target (Destination)	Enter the number to which MLPP precedence calls should be diverted if this directory number receives a precedence call and neither this number nor its call forward destination answers the precedence call. Values can include numeric characters, octothorpe (#), and asterisk (*).
MLPP Calling Search Space	From the drop-down list box, select the CSS to associate with the MLPP alternate party target (destination) number.
MLPP No Answer Ring Duration (seconds)	Enter the number of seconds (between 1 and 60) after which an MLPP precedence call will be directed to this directory number alternate party if this directory number and its call-forwarding destination do not answer the precedence call. Leave this setting blank to use the value that is set in the Unified Communications Manager enterprise parameter Precedence Alternate Party Timeout.
Hold Reversion Settings	
Disable Hold Reversion	To disable hold reversion for a line when the system setting is enabled, check this checkbox. If you leave the checkbox unchecked, Unified Communications Manager uses the timer setting.
Hold Reversion Ring Duration (seconds)	Enter a number from 0 to 1200 (inclusive) to specify the wait time in seconds before issuing a reverted call alert to the holding party phone. If you enter a value of 0, Unified Communications Manager does not invoke the reverted call feature for a held call. At installation, this field remains blank. If you leave this setting blank, the Hold Reversion Duration timer setting for the cluster applies.
Hold Reversion Notification Interval (seconds)	Enter a number from 0 to 1200 (inclusive) to specify the interval time in seconds for sending periodic reminder alerts to the holding party phone. If you enter a value of 0, Unified Communications Manager does not send reminder alerts. At installation, this field remains blank. If you leave this setting blank, the Hold Reversion Notification Interval timer setting for the cluster applies.
Enterprise Alternate Number and +E.164 Alternate Number **Note** The following fields apply to both the Enterprise Alternate Number and the +E.164 Alternate Number sections as the fields are identical for each section.	
Add Alternate Number	Select **Add Enterprise Alternate Number** to add an enterprise alternate number and associate it to this directory number. Select **Add +E.164 Alternate Number** to add an +E.164 alternate number and associate it to this directory number.

Field	Description
Number Mask	In the text box, enter a number mask for the enterprise alternate number or +E.164 alternate number. This field can contain only digits 0-9, X and the plus sign (+). If the Number Mask contains a plus sign, the plus sign must be the first character in the mask. Refer to the Alternate Number field below to see how the alternate number appears after the mask has been applied. Unified Communications Manager applies the mask to the directory number and creates an enterprise alternate number or +E.164 alternate number that acts as an alias for the directory number. Other phones can dial this directory number by dialing the enterprise number. **Enterprise Alternate Number Example** If you apply a number mask of 8XXXX to directory number 2000, Unified Communications Manager creates an enterprise alternate number 82000 as an alias of directory number 2000. If the dialed digits of an incoming call are 82000, Unified Communications Manager routes the call to the user that is registered to directory number 2000. **+E.164 Alternate Number Example** If you apply a number mask of 1972515XXXX to directory number 2000, Unified Communications Manager creates an +E.164 alternate number 19725152000 as an alias of directory number 2000. If the dialed digits of an incoming call are 19725152000, Unified Communications Manager routes the call to the user that is registered to directory number 2000.
Alternate Number	
Add to Local Partition	Check this check box to assign this alternate number to a local route partition. Leave the check box unchecked if you do not want to restrict access to this alternate number. **Note** For users in the local cluster to be able to dial this alternate number, the partition to which you assign the alternate number must be in a local calling search space.
PSTN Failover for Enterprise Alternate Number, +E.164 Alternate Number, and URI Dialing	

Field	Description
Advertised Failover Number	If the local cluster is part of an ILS network, and Global Dial Plan Replication is enabled, the local cluster advertises the PSTN failover to remote clusters in the ILS network. If a remote cluster is unable to route a call via a SIP trunk to one of the advertised directory URIs or alternate numbers that are associated with this directory number (DN), the remote cluster can reroute the call to the advertised PSTN failover number and send the call to a PSTN gateway. From the drop-down list box, select one of the following options: **<None>** ILS does not advertise a PSTN failover option. **Enterprise Number (<number>)** ILS advertises the enterprise alternate number as the PSTN failover for all the alternate numbers and directory URIs that are associated to this DN. **+E.164 Number (<number>)** ILS advertises the +E.164 alternate number as the PSTN failover for all the alternate numbers and directory URIs that are associated to this DN. **Note** If Global Dial Plan Replication is enabled, ILS advertises the PSTN failover setting to the ILS network, regardless of whether the Advertise Globally via ILS check box is checked for the alternate number that you select.



CHAPTER 103

Feature Group Template Setup

This chapter contains information to set up feature group templates.

Feature Group Template Setup

In Cisco Unified Communications Manager Administration, use the **User Management** > **User/Phone Add** > **Feature Group Templates** menu path to set up a feature template that includes features such as mobility and IM and Presence. You can also assign a pre-configured service profile and universal device templates to a user.

Note You set up feature group templates that you use when you add a user or device from the **Quick User/Phone Add** window. Changes to the template do not affect users and devices that are already added.

This table lists and describes the field settings on the **Feature Group template** window.

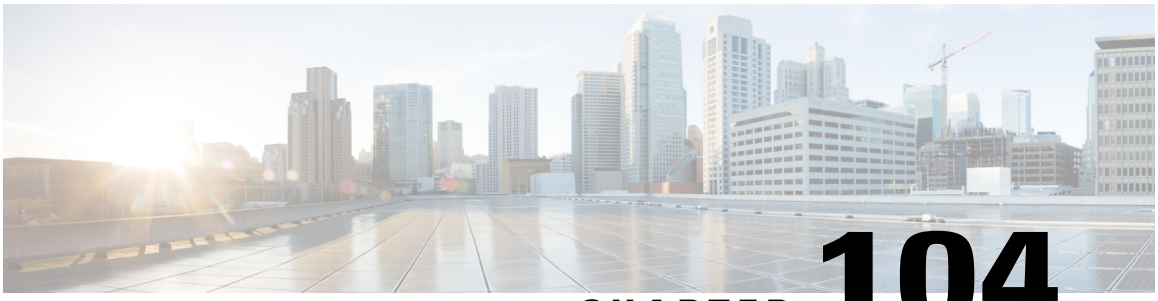
Table 136: Feature Group Template Settings

Field	Description
Feature Group Templates	
Name	Enter the feature group template identification name.
Description	Enter a description for the feature group template. The description can be up to 100 characters in any language, and most punctuation is allowed.
Features	

Field	Description
Home Cluster	Check this check box if the end user is homed to this cluster. The end user should only be homed to one cluster within the enterprise. **Note** IM and Presence does not function properly if an end user is assigned to more than one cluster. **Note** After an upgrade to Unified Communications Manager Release 10.0(1), when new users are synced from LDAP, the home cluster is not enabled. You must modify your existing LDAP synchronization agreement and add a Feature Group Template which has the home cluster enabled.
Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)	Check this check box to enable the end user (on the home cluster) for IM and Presence. Configure IM and Presence in the associated service profile. **Note** You must install a Cisco Unified Communications Manager IM and Presence Service node along with Cisco Unified Communications Manager. Use the **User Management** > **User Settings** > **UC Services** menu to configure the settings for the IM and Presence Service.
Include meeting information in Presence	Check this checkbox to enable the end user to include meeting and calendar information in IM and Presence Service. Before making this selection, the end user must be on the home cluster and have IM and Presence enabled. Also ensure that an Exchange Presence Gateway is configured on the Cisco Unified Communications Manager IM and Presence Service server. You can also enable the inclusion of end user meeting and calendar information in IM and Presence Service using the End User Configuration window or the Bulk Administration Tool. For information about using the Bulk Administration Tool to enable the inclusion of meeting and calendar information, see topics related to configuring an end user template in the *Cisco Unified Communications Manager Bulk Administration Guide*.
Service Profile	Select a service profile from the drop-down list box. To view the settings for each service profile, select the **More Details** link. **Note** You can create new service profiles from the **User Management** > **User Settings** > **Service Profile** menu.
User Profile	Select a user profile from the drop-down list box. To view the settings for each service profile, select the **More Details** link. **Note** You can create new user profiles from the **User Management** > **User Settings** > **User Profile** menu.

Field	Description
Allow Control of Device from CTI	If you check this check box, the AllowCTIControlFlag device property becomes active, which allows control of the device from computer telephony integration (CTI) applications. This setting takes effect when the user signs in to a device or the device is in the user CTI control device list. **Note** If the user does not sign into a device or no device exists in the user CTI control device list, this setting has no effect. The Allow Control of Device from CTI setting in the end user configuration overrides the AllowCTIControlFlag device property of the device to which the user signs in.
Enable Extension Mobility Cross Cluster	Check this check box to enable this end user to use the Cisco Extension Mobility Cross Cluster feature.
Enable Mobility	Check this check box to activate Cisco Unified Mobility, which allows the user to manage calls through a single phone number and to pick up in-progress calls on the desk phone and mobile phone.
Enable Mobile Voice Access	Check this check box to allow the user to access the Mobile Voice Access integrated voice response (IVR) system to initiate Cisco Unified Mobility calls and activate or deactivate Cisco Unified Mobility capabilities.
Maximum Wait Time for Desk Pickup *	Enter the maximum time in milliseconds that is permitted to pass before the user must pick up a call that is transferred from the mobile phone to desktop phone. Default: 10000
Remote Destination Limit *	Enter the maximum number of phones to which the user is permitted to transfer calls from the desktop phone. Default: 4
BLF Presence Group *	Use this field to configure the BLF Presence feature. From the drop-down list box, choose a BLF presence group for the end user. The selected group specifies the destinations that the end user can monitor. The default value for BLF Presence Group specifies Standard Presence group, configured with installation. BLF presence groups that are configured in Cisco Unified CM Administration also appear in the drop-down list box. BLF presence authorization works with BLF presence groups to allow or block presence requests between groups. For more information about how to configure permissions between groups and how BLF presence works with extension mobility, see the *Cisco Unified Communications Manager Features and Services Guide*.

Field	Description
SUBSCRIBE Calling Search	Supported with the BLF presence feature, the SUBSCRIBE calling search space determines how Unified Communications Manager routes presence requests that come from the end user. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the end user. From the drop-down list box, choose the SUBSCRIBE calling search space to use for presence requests for the end user. All calling search spaces that you configure in Cisco Unified CM Administration appear in the SUBSCRIBE Calling Search Space drop-down list box. If you do not select a different calling search space for the end user from the drop-down list, the SUBSCRIBE calling search space defaults to None. To configure a SUBSCRIBE calling search space specifically for this purpose, you configure a calling search space as you do all calling search spaces.
User Locale	From the drop-down list box, choose the locale that is associated with the end user. The user locale identifies a set of detailed information to support end users, which includes language and font. Unified Communications Manager uses this locale for extension mobility and the Cisco Unified Communications Self Care Portal. For Cisco Extension Mobility login, the locale that is specified here takes precedence over the device and device profile settings. For Cisco Extension Mobility logout, Unified Communications Manager uses the end user locale that the default device profile specifies. **Note** If you do not choose an end user locale, the locale that is specified in the Cisco CallManager service parameters as Default User Locale applies.
Desk Phones	From the drop-down list box, select a universal device template for desk phones that are associated to this user.



CHAPTER 104

Quick User and Phone Addition

This chapters contains information to quickly add users and phones to Cisco Unified Communications Manager (Unified CM).

Quick User and Phone Addition Configuration and Settings

In Cisco Unified Communications Manager (Unified CM) Administration, use the **User Management** > **User/Phone Add** > **Quick User/Phone Add** menu path to configure a user, a phone, and a line appearance in a single, easy addition.

The Quick User/Phone Add window in Unified CM provides a single window that allows you to perform basic steps to add a new user and assign the phones to the user.

Before you add a user and phone from this window, ensure that you have performed the following prerequisites:

- Set up a line (directory number)
- Set up a universal device template
- Set up a feature group template

Quick User and Phone Addition Settings

The following table lists the quick user and phone addition settings.

Table 137: Quick User and Phone Addition Settings

Field	Description
User Information	
First Name	Enter the end user first name.

Field	Description
Middle Name	Enter the end user middle name.
Last Name	Enter the end user last name.
User ID	Enter the end user identification name. Unified CM does not permit modifying the user ID after you create it.
Access Control Group Membership	
User is a member of	Select the plus sign (+) next to this drop-down list box to list the access control groups (ACGs). You can assign this user as an ACG member. ACGs allow users with full access to configure different levels of access for Unified CM administrators. Full-access users configure the access of other users to Unified CM. **Tip** Select the plus sign (+) again to add more ACGs for the user.
Device Creation	
Feature Group Template	This drop-down list box lists the feature group templates to which you can assign this user. You can assign one template. After you create the user and assign a feature group template, the **Manage Devices** button appears. **Note** You have to add at least one extension before the **Manage Devices** button appears.
Credentials	
Use default credential	Use this setting to select the default credential, so you do not have to type credentials into a field. When you select this setting, the default credential defined in the system default credential policy is used automatically during the user insertion. The password and PIN input and confirm text box is disabled. **Note** This setting is not supported for the update user operation.
Password	Enter five or more alphanumeric or special characters for the user password. You may use the following special characters: =, +, <, >, #, ;, \, , "", and blank spaces.
Confirm Password	Enter the user password again.
PIN	Enter five or more numeric characters for the personal identification number (PIN).
Confirm PIN	Enter the PIN again.
Extensions	

Field	Description
Extension	This field represents the extensions for the user. Extensions represent the lines that are added to a phone. These extensions are based on the available lines in the template. After you assign the first (primary) extension, the secondary extensions drop-down list box lists the available extensions. To assist the administrator, the drop-down list box shows extensions as either "Available" or "Used." **Note** You cannot add devices until you specify an extension. **Note** You can add multiple extensions for the user. When you select the green plus sign (+) under Action, you can add more extensions and change their order of appearance.
Personal	
Directory URI	Enter the directory uniform resource identifier (URI) for this user. A directory URI looks like an email address and follows the user@host format. It allows for others to find a user in a directory easily.
Number Displayed in Directory	Enter the user telephone number. This number shows up when you hit the company (local) directory button on your phone.
Email	Enter the user e-mail address.
Manager User Id	Enter the user ID of the manager. **Note** The manager user ID that you enter does not have to exist in the same cluster as the user; therefore, Unified CM does not require that you enter a user ID that already exists in the database.
Department	Enter the user department information (for example, the department number or name).

Related Topics

Feature Group Template Setup , on page 953
Universal Device Template Setup, on page 900

Add New User and Device

Procedure

Step 1 Select **Add New**.
The Quick User/Phone Add window is displayed.

Step 2 Enter the appropriate settings.
See topics related to quick user and phone addition for details.

Step 3 Select **Save**.

Step 4 Select **Manage Devices**.

Step 5 Select **Add New Phone**.

Step 6 Set the following fields:

- Product Type
- Device Protocol
- Device Name
- Universal Device Template
- Number of Expansion Modules

  This field appears only for devices that support expansion modules. When you enter the number of expansion modules, you can also select the expansion module type if the device supports more than one type. The expansion module type you select is applied to all expansion modules on the device. Devices that support only one type of expansion module display the supported expansion module type by default. The maximum number of expansion modules you can enter for a device is determined by the number the expansion modules the device supports.

  When you check the Is Extension Mobility Template Checkbox, the No. of Expansion Modules field and Expansion module field are disabled

  Note Cisco Unified Communications Manager uses three universal device templates to define the characteristics of a device: Desk Phones, Mobile Devices, and Profiles. Set the device templates in the **Feature Group Template** window.

- Is Extension Mobility Template

Step 7 Select **Save**.
The phone is added to the user.

Related Topics

Quick User and Phone Addition Configuration and Settings , on page 957

Add New User and Existing Device

Note Unified CM uses the three universal device templates that you defined on the **Feature Group Template** window to define the characteristics of devices.

Procedure

Step 1 Select **Add New**.

The **Quick User/Phone Add** window appears.

Step 2 Enter the appropriate settings as described in Quick User and Phone Addition Configuration and Settings , on page 957.

Step 3 Select **Save**.
The user is added to the Unified CM database.

Step 4 Select **Manage Devices**.

Step 5 Select **Find a Phone to Move to This User**.

Step 6 Select the phone you want to associate to the user.

Note You can set search filters on the phone listing.

Step 7 Select **Move Selected**.
The phone is added to the user.

Related Topics

Quick User and Phone Addition Configuration and Settings , on page 957

Move Device to a User

Note Be aware that when a device is moved to the user, that device is disassociated from the previous user.

Procedure

Step 1 In Unified CM Administration, select **User Management** > **User/Phone Add** > **Quick User/Phone Add**
The Find and List window appears. Records from an active (prior) query may also appear in the window.

Step 2 From the first drop-down list box, select a search parameter.

Example:
Select **First Name** to search by the user first name.

Step 3 From the second drop-down list box, select a search pattern.

Step 4 Specify the appropriate search text, if applicable.

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

Step 5 Select **Find**.
All matching records appear. You can change the number of items that appear on each page by choosing a different value from the Rows per Page drop-down list box.

Step 6 Select the user to which you wish to move an existing device.

The user profile appears.

Step 7 Select the **Manage Devices** button.

Step 8 Select the **Find a Phone to Move to This User** button.

Step 9 Select the phone you want to associate to the user.

Note You can set search filters on the phone listing.

Step 10 Select **Move Selected**.
The phone is added to the user profile.

Related Topics

Quick User and Phone Addition Configuration and Settings , on page 957

CHAPTER 105

Self-Provisioning

Self-Provisioning

Self-Provisioning for End Users and Administrators

The Self-Provisioning feature allows an end user or administrator to add an unprovisioned phone to a Cisco Unified Communications Manager system with minimal administrative effort. A phone can be added by plugging it into the network and following a few prompts to identify the user.

This feature enhances the out-of-box experience for end users by allowing them to directly add their desk phone or soft client without contacting the administrator. It simplifies administrator deployments by allowing them to add desk phones on behalf of an end user. The feature lets administrators and users deploy a large number of devices without interacting directly with the Cisco Unified Communications Manager Administration GUI, but from the device itself. The feature relies on the administrator preconfiguring a number of templates and profiles, so that when the phone attempts to self-provision, the necessary information is available in the system for it to create a new device.

Note Self-provisioning is not supported for secured endpoints.

There are two levels of configuration for Self-Provisioning:

- The system level
- The user level

You can set up this feature at the system level from Cisco Unified Communications Manager Administration under the **User Management** > **Self-Provisioning** menu.

To set up this feature, you can select one of the following modes:

- **Secure Mode**
  - Administrators can provision devices on behalf of end users
  - End users can provision devices with their credentials
- **Non-Secure Mode**
  - End users/administrators can enter Self-Service ID for the device that is being provisioned.

With appropriately configured User Profiles, end users can provision their own devices. These User Profiles may be shared by a group of users that share the same characteristics. The User Profile contains the following settings:

- Universal Device Templates
- Universal Line Template
- End user Self-Provisioning settings

Note The administrator can set any User Profile as the system default.

In order to allow a user to provision a new device using Self-Provisioning, the user must meet the following criteria:

If you do not configure a UDT in the User Profile, user assignment fails and plays the following error message on the phone: `This device could not be associated to your account. Please contact the System administrator to complete provisioning.`

- Self-Provisioning must be enabled for the end user.

  Note Self-Provisioning must be enabled even if the administrator performs device self-provisioning on behalf of the user.

- The user must have a primary extension.
- The user must have the appropriate universal device template linked to the User Profile.
- The total number of owned devices must be less than the Self-Provisioning limit that is specified on the associated User Profile.

Self-Provisioning IVR Service

The Self-Provisioning feature introduces a new service called Self-Provisioning IVR service. When you dial the CTI RP DN that is configured on the Self-Provisioning page, from an extension of a user that uses the

IVR service, the phone connects to the Self-Provisioning IVR application and prompts you to provide the Self-Service credentials. Based on the validation of the Self-Service credentials that you provide, the IVR service assigns the autoregistered IP phones to the users.

You can configure self-provisioning even if the service is deactivated, but the administrator cannot assign IP phones to users using the IVR service. By default, this service is deactivated.

Note When you upgrade a previous release Cisco Unified Communications Manager to Release 10.0, the Cisco Unified Communications Manager will create a Universal Device Template and a Universal Line Template which will retain the previous configurations for Auto-Registration settings. After the upgrade, the values of **Partition** and **External Phone Number Mask** will be populated in the new Universal Line Template by Cisco Unified Communications Manager and in the Line field of the Universal Device Template respectively. And also, the Cisco Unified Communications Manager populates the Cisco Unified Communications Manager name for the Universal Device Template and a Universal Line Template and configures the same values for Auto-Registration settings.

Self-Provisioning Settings

The following table lists and describes the Self-Provisioning settings.

Table 138: Self-Provisioning Settings

Name	Description
Status	
Status	Displays the success or failure messages for Self-Provisioning save and Self-Provisioning IVR service restart actions. Displays **Ready** message when the following features are turned on: • Auto-Registration • Self-Provisioning IVR service When either feature is turned off, the status displays the name of the feature that is turned off. When both Auto-Registration and Self-Provisioning IVR service are turned off, you can still save the configuration.
Authentication Mode	

Name	Description
Require Authentication	Requires authentication for self-provisioning. Select one of the following authentication options: **Allow authentication for users only (via Password/PIN)** Allows users to use their password or PIN to authenticate and provision devices based on the permissions in their User Profile. **Allow authentication for users (via Password/PIN) and Administrators (via Authentication Code)** Allows users and administrators to provision on behalf of an end user through an authentication code. The authentication code must be an integer ranging from 0 to 20 digits but cannot be empty (null). **Note** Self-Provisioning from the phone interface uses the user password instead of a PIN. A PIN is used for Self-Provisioning through the IVR interface. By default, **Require Authentication mode** is selected with the **Allow Authentication for users only (via Password/PIN)** radio button checked and the **Authentication Code** text box disabled.
No Authentication Required	**Note** This mode is not recommended for day-to-day operation. Users and administrators do not require authentication. In this open mode, authentication is disabled when a device is self-provisioned. The administrator or end user can enter a user ID or self-provisioning ID into an endpoint and the endpoint is associated to the user account.
IVR Settings	
Language Preference	Displays the available and selected language based on the language pack that is installed on the Cisco Unified Communications Manager. You can select the priority of the language for the IVR to play by using the up and down arrows. English, United States is the default language in the **Selected Language** list if no other language pack is installed. You can have a maximum of nine languages in the **Selected Language** list depending on the language pack that is installed on the Cisco Unified Communications Manager. If you try to remove the only language from the **Selected Language** list, a warning message appears as follows: `Selected Language should contain at least one language.`

Name	Description
CTI Route Point	Select a CTI Route Point from the drop-down list. The selected CTI Route Point can have one or multiple DNs associated to it. The DNs are autopopulated when you select a route point. For the selected route point, the corresponding DN appears with the following message: `Dial 2000 from the phone to assign an extension.` If no DN is assigned to the selected route point, the following message appears: `No DN is assigned to the Route Point. Please assign a DN to the Route Point.` The default value is Not Selected. The CTI RP supports the following codecs: • G711 u-law 64K • G711 a-law 64K • G729 • L16 256K When you dial the CTI Route point to associate a phone to the user, the IVR prompts play. When this process is still in progress and you click on any softkey (for example, hold, transfer, conference, and so on), the CTI Route Point IVR call disconnects and 20 seconds later, the phone display shows that the call is disconnected. **Note** • Self Provisioning IVR supports a maximum of 100 ports (calls to the CTI Route Point). When a new CTI Route Point is created, the default Max Calls for the Route Point is 5000. • The number of CTI Route Point ports can be further reduced below 100 (for example, to 50 or 20) based on the size of the Unified Communications Manager cluster and the number of users. Reduce the max calls to reduce the virtual memory footprint of a process Plug-and-Play Launcher.

Name	Description
Application User	Select an Application User from the drop-down list. For the selected application user, if *Standard CTI Enabled* role is not assigned, the following warning message appears: `Standard CTI Enabled role is not assigned for this application user. Self-Provisioning IVR service will not work.` You must select an Application User for the Self-Provisioning IVR to work. If the selected application user does not have valid credentials set (for example, password), the following warning message appears:`Valid credentials not set for this application User. Self-Provisioning IVR service will not work.` The default value specifies Not Selected.

Name	Description
Save	Saves the Self-Provisioning configuration. If you modified the CTI Route Point or the Application User, a popup message appears: `Changing the CTI Route Point Selection requires the Self-Provisioning service to restart. Any active Self-Provisioning sessions will be terminated. If you do not restart now, you will have to manually restart Self-Provisioning through the Cisco Unified Communications Serviceability interface.` The popup message provides the following three options and, based on what you select, it displays the appropriate status message in the **Status** field: • **Save and Restart Now:** Saves the configuration and restarts Self-Provisioning IVR service automatically, which displays the message: `Save successful. Self-Provisioning IVR service restarted successfully.` **Note** There is a delay of 30 seconds between Self-Provisioning IVR service restart and call establishment with CTI RP. During this delay time, you will hear a reorder tone until the CTI RP gets registered and the IVR service gets activated again. **Note** When the Self-Provisioning IVR service goes down during a call in-progress, the call disconnects immediately. **Note** When you select **Save and Restart Now**, it saves the configuration but fails to restart the Self-Provisioning IVR service, and the following status message appears: `Save successful. Failed to restart Self-Provisioning IVR service.` • **Save Without Restarting:** Saves the configuration but does not restart Self-Provisioning IVR service, which displays the message: `Save successful`. • **Cancel:** Closes the popup message and displays the new changes configured for Self-Provisioning without saving. If you want to retain the old configuration, refresh the page. Changes to the Self-Provisioning configuration do not take effect until you restart the Self-Provisioning IVR service. For information about restarting a service, see the *Cisco Unified Serviceability Administration Guide*.

User Profile Settings

The following table lists the User Profile settings.

Table 139: User Profile Settings

Name	Description
User Profile	
Name	Enter a name to identify the User Profile.
Description	(Optional) Enter a description for the User Profile.
Make this the default User Profile for the system	Check this check box to specify this User Profile as the default for the system.
Universal Device Template **Note** These templates are used to create new phones or move phones for the users that are associated with this feature group template. **Note** If you do not configure a UDT in the User Profile, user assignment fails and plays the following error message on the phone: `This device could not be associated to your account. Please contact the System administrator to complete provisioning.`	
Desk Phones	From the drop-down list box, select a universal device template for desk phones that are associated to this user.
Mobile and Desktop Devices	From the drop-down list box, select a universal device template for mobile devices that are associated to this user.
Remote Destination/Device Profiles	From the drop-down list box, select a universal device template for profiles that are associated to this user.
Universal Line Template	
Universal Line Template	From the drop-down list box, select a universal line template to associate to this feature group template. **Note** You can create universal line templates from **User Management** > **User/Phone Add** > **Universal Line Template**. **Note** A universal line template is not required for the Self-Provisioning feature.
Self-Provisioning	

Name	Description
Allow end user to provision their own phones	Check this check box to enable user self-provisioning, which provides end users with permission to provision their phones.
Limit Provisioning once End User has this many phones	Specify a limit to the number of provisions an end user can perform. The maximum is 20 and the default is 10.

Set Up Self-Provisioning for New User

Note A newly self-provisioned device may not immediately appear as Registered in Cisco Unified Communications Manager.

Procedure

Step 1 Select **User Management** > **Self Provisioning**.

Step 2 Select one of the following options:

- Requires Authentication: Allow authentication for users only
- Requires Authentication: Allow authentication for users and administrators

  Note For administrator authentication, specify the authentication code. The authentication code must be an integer ranging from 0 to 20 digits but cannot be empty (null).

Step 3 Select **User Management** > **User Settings** > **User Profile**.

Step 4 Create or choose an existing user profile.

Note Make sure the proper universal device template is associated with the user profile and self-provisioning is configured properly.

Step 5 Check the **Allow end user to provision their own phones** check box.

Step 6 Create or choose an existing Feature Group Template. Make sure the proper User Profile is associated.

Step 7 Create a user from **User Management** > **User/Phone Add** > **Quick User/Phone Add**.

Step 8 Select a Feature Group Template.

Step 9 Specify a line extension.

Step 10 Select **Save**.

The new user is now able to perform self-provisioning on the device.

Set Up Self-Provisioning for Existing User

Note A newly self-provisioned device may not immediately appear as Registered in Cisco Unified Communications Manager.

Procedure

Step 1 Select **User Management** > **Self Provisioning**.

Step 2 Select one of the following options:

- Requires Authentication: Allow authentication for users only
- Requires Authentication: Allow authentication for users and administrators

  Note For administrator authentication, specify the authentication code. The authentication code must be an integer ranging from 0 to 20 digits but cannot be empty (null).

Step 3 Find an existing user in the Unified Communications Manager database.

Step 4 Find the User Profile that is associated with the user.

Step 5 Open the User Profile.

Step 6 Check the **Allow end user to provision their own phones** check box.

Step 7 Select **Save**.
The user is now able to perform self-provisioning on the device.

Set Up Cisco Unified Communications Manager to Support Self-Provisioning

Before You Begin

The administrator must first either add the end user using the Bulk Administration Tool or synchronize the end user from LDAP to add the end users to the Cisco Unified Communications Manager.

Procedure

Step 1 Select **User Management** > **User Phone/Add** > **Universal Device Template** and **User Management** > **User Phone/Add** > **Universal Line Template**. Create a Universal Device Template (UDT) and a Universal Line Template (ULT) for the end user.
For information about UDT and ULT settings, see Universal Device Template Settings, on page 900 and Universal Line Template Settings, on page 935.

Step 2 Select **User Management** > **User Settings** > **User Profile**. Create a User Profile and assign the created UDT and ULT to the end user. Ensure that you check the **Allow End User to Provision Their Own Phones** check box.
For information about User Profile settings, see User Profile Settings, on page 970.

The end user is now associated with a UDT and ULT.

Step 3 Select **User Management** > **User Phone/Add** > **Feature Group Template**. Create a Feature Group Template (FGT) and select the user profile in the **User Profile** drop-down list that you created in the preceding step.
For information about FGT, see Feature Group Template Setup , on page 953.

Step 4 Select **System** > **LDAP** > **LDAP Directory**. Select the FGT from the **Feature Group Template** drop-down list and synchronize the end user.
For information about LDAP directory page, see LDAP Directory Settings, on page 112.

Note The first four steps show how to add users, how to configure User Profile and associate the UDT and ULT, how to create a FGT, and how to synchronize LDAP users. If you are adding users manually or using BAT, perform steps 1 and 2 where you must create a User Profile with appropriate UDT and ULT and associate the User Profiles to particular users.

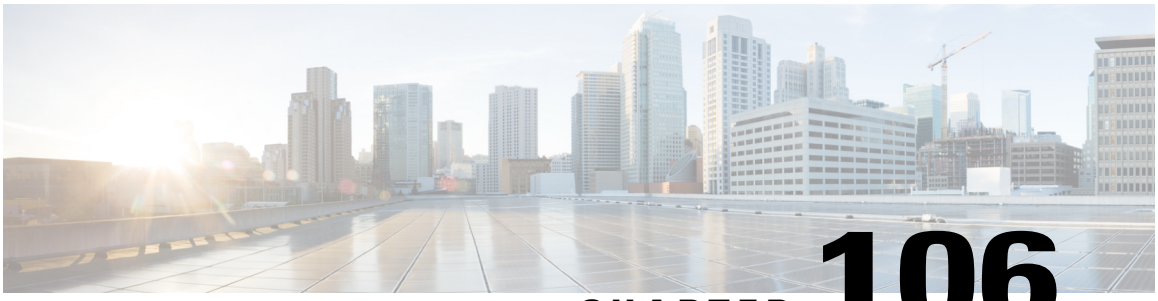
Step 5 Select **Device** > **CTI Route Point**. Create a CTI Route Point and an Application User and associate the CTI Route Point with the Application User. You must have the *Standard CTI Enabled* role enabled for the Application User.
For information about CTI Route Point and Application User, see CTI Route Point Settings , on page 455 and Application User Settings , on page 831.

Step 6 Select **System** > **Cisco Unified CM** and configure the **Auto-Registration Information**.
For information about autoregistration, see Autoregistration Settings , on page 159.

Step 7 Select **User Management** > **Self-Provisioning** and configure the authentication mode, IVR settings, and CTI Route point.
For information about Self-Provisioning, see Self-Provisioning Settings , on page 965.

Step 8 Autoregister the phone to the Cisco Unified Communications Manager.

Step 9 Dial the CTI Route Point from the autoregistered IP phone to associate the device to an end user.
When you dial the CTI Route Point, the phone connects to the Self-Provisioning IVR application and plays the IVR prompts. Based on the validation of the Self-Service credentials that you provide, the IVR service assigns the autoregistered IP phone to the user.



CHAPTER 106

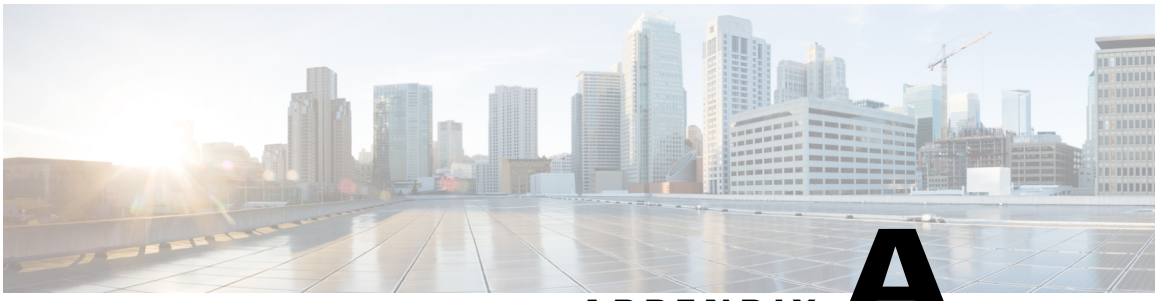
Other User Management Menu Options

Other user management menu options

This chapter provides brief descriptions of selected User Management menu options that other documents describe in greater detail. A pointer to the document that contains more details is provided for each User Management menu option.

PART IX

Cisco Unified Communications Manager Bulk Administration



APPENDIX A

Bulk Administration Tool (BAT)

Bulk Administration Tool (BAT)

In Cisco Unified Communications Manager Administration, use the Bulk Administration menu and the submenu options to configure entities in Cisco Unified Communications Manager through use of the Bulk Administration Tool.

The Cisco Unified Communications Manager Bulk Administration Tool (BAT), a web-based application, performs bulk transactions to the Cisco Unified Communications Manager database. BAT lets you add, update, or delete a large number of similar phones, users, or ports at the same time. When you use Cisco Unified Communications Manager Administration, each database transaction requires an individual manual operation, while BAT automates the process and achieves faster add, update, and delete operations.

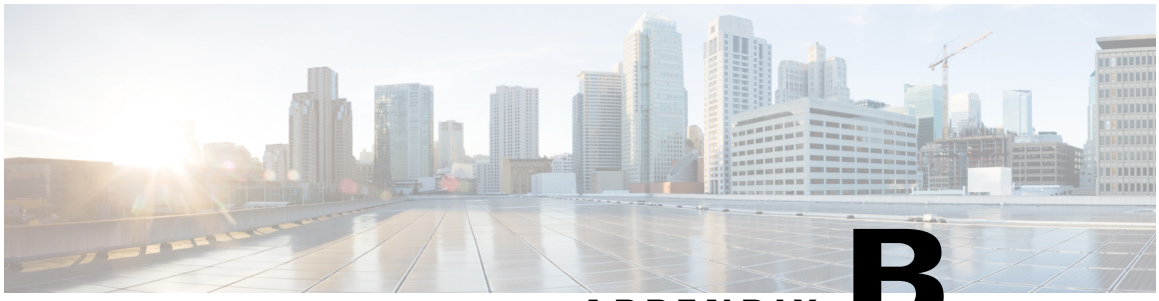
You can use BAT to work with the following types of devices and records:

- Add, update, and delete Cisco Unified IP Phones including voice gateway (VGC) phones, computer telephony interface (CTI) ports, and H.323 clients
- Add, update, and delete users
- Add, update, and delete User Device Profiles
- Add, update, and delete Cisco Unified Communications Manager Assistant managers and assistants
- Add, update, and delete ports on a Cisco Catalyst 6000 FXS Analog Interface Module
- Add or delete Cisco VG200 and Cisco VG224 analog gateways and ports
- Add or delete Forced Authorization Codes
- Add or delete Client Matter Codes
- Add or delete Call Pickup Groups
- Update or export CUP/CUPC users
- Populate or depopulate the Region Matrix
- Insert, delete, or export the Access List
- Export or import configuration

- Insert, delete, or export Remote Destination and Remote Destination Profile

You can also work with these devices in combination with the user information. For example, when you add CTI ports and users, BAT allows you to "Enable CTI Application Use." This saves time when you are adding users who have applications that require a CTI port, such as Cisco IP Softphone.

An optional component of BAT, the Cisco Unified Communications Manager Auto-Register Phone Tool (TAPS), further reduces the manual labor that is involved in administering a large system. When you need to add a large block of new phones, you can use BAT to add the devices with dummy media access control (MAC) addresses instead of entering each MAC address in the data input file. After the phones are installed, the phone users or the administrator can call the TAPS directory number, follow the voice prompts, and download the correct user device profiles for their phones.



APPENDIX B

Dependency Records

This appendix provides information about the dependency record windows in Cisco Unified Communications Manager Administration. These windows help you to determine which records in the database use other records. For example, you can determine which devices (such as CTI route points or phones) use a particular calling search space.

If you need to delete a record from Cisco Unified Communications Manager, you can use dependency records to show which records are associated with the record that you want to delete. You can then reconfigure those records, so they are associated with a different record.

Enable Dependency Records

To access dependency records, you must first enable them. The system disables dependency records by default. To enable the dependency records, perform the following procedure.

Caution Enabling the dependency records functionality causes high CPU usage. This task executes at below-normal priority and may take time to complete due to dial plan size and complexity, CPU speed, and the CPU requirements of other applications.

Procedure

Step 1 Choose **System** > **Enterprise Parameters**

Step 2 Scroll to the CCMAdmin Parameters area of the window.

Step 3 From the Enable Dependency Records drop-down list box, choose True.
A dialog box displays with a message about the consequences of enabling the dependency records. Read the information carefully before clicking OK.

Step 4 Click OK.
The field displays True.

Step 5 Click Save.

Disable Dependency Records

If you have dependency records enabled and your system is experiencing CPU usage issues, you can disable dependency records. (The system disables dependency records by default.) To disable the dependency records, perform the following procedure.

Procedure

Step 1 Choose **System** > **Enterprise Parameters**.

Step 2 Scroll to the CCMAdmin Parameters area of the window.

Step 3 From the Enable Dependency Records drop-down list box, choose False.
A dialog box displays with a message about dependency records. Read the information carefully before clicking OK.

Step 4 Click OK.
The field displays False.

Step 5 Click Save.

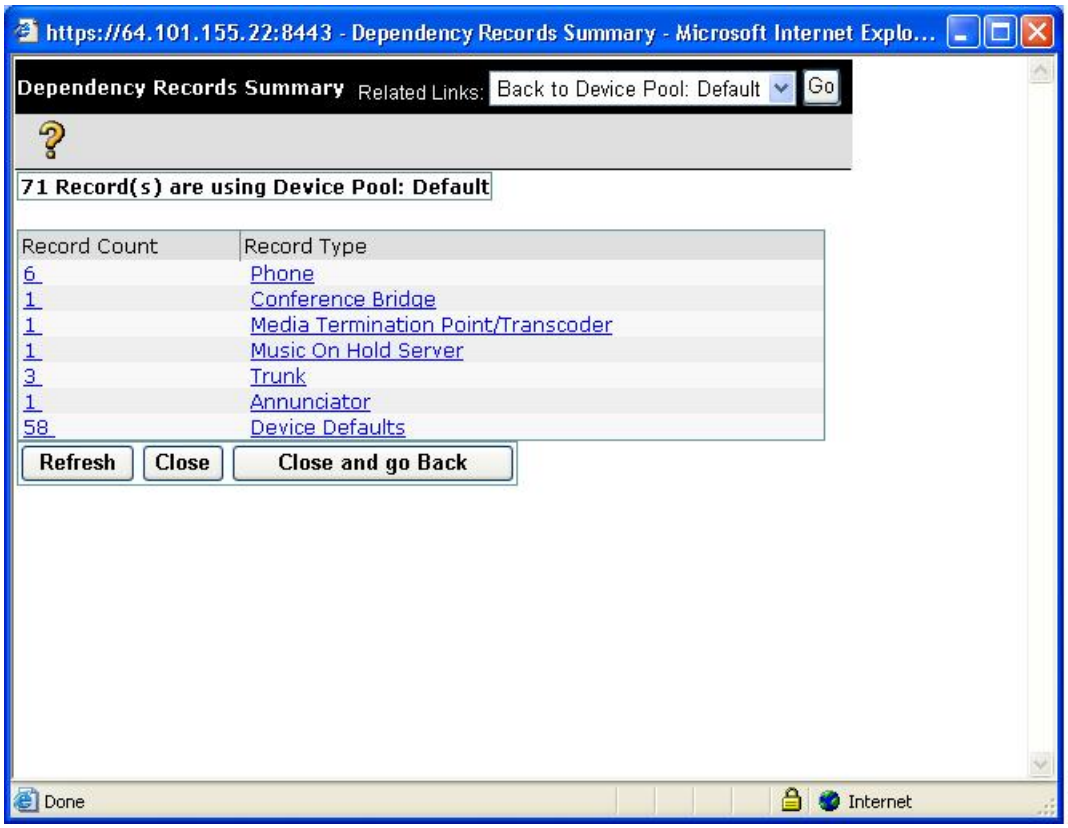
Access Dependency Records

To access dependency records from Cisco Unified Communications Manager configuration windows, choose Dependency Records from the Related Links box and click Go. The Dependency Records—Summary window displays. This window displays the number and type of records that use the record that is shown in the Cisco Unified Communications Manager configuration window.

Note If the dependency records are not enabled, the Dependency Records—Summary window displays a message, not the information about the record.

For example, if you display a the Default device pool in the Device Pool Configuration window and click the Dependency Records link, the Dependency Records Summary window displays all the records that use that device pool, as shown in the following figure.

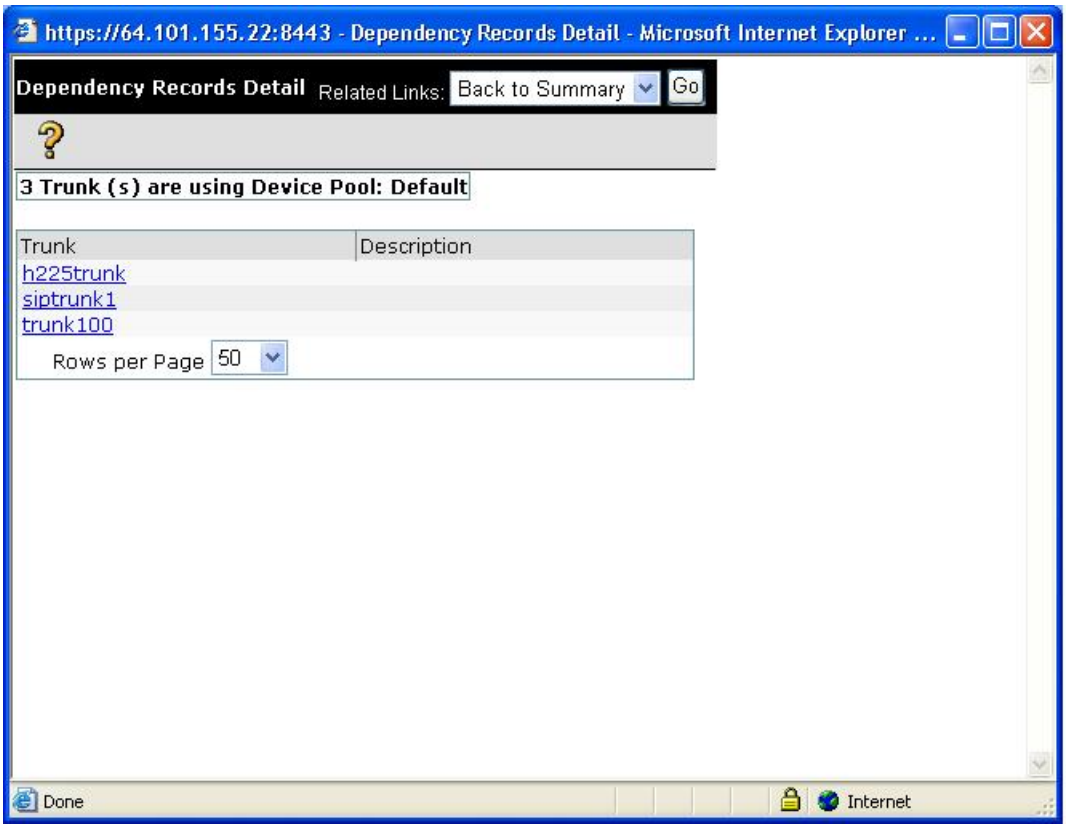
Figure 1: Dependency Records—Summary Example



To display detailed dependency records information, click the record about which you want more information; for example, click the trunk record. The Dependency Records Detail window displays, as shown in the following figure. If you want to return to the original configuration window, choose Back to Summary from

the Related List Box and click Go; then, choose Back to <configuration window name> and click Go, or click the Close and go Back button.

Figure 2: Dependency Records—Detail Example



To display the configuration window of the record that is displayed in the Dependency Records Detail window, click the record. The configuration window for that record displays. For example, if you click the h225trunk record that is shown in the Dependency Record figure, the Trunk Configuration window displays with information about the h225trunk.

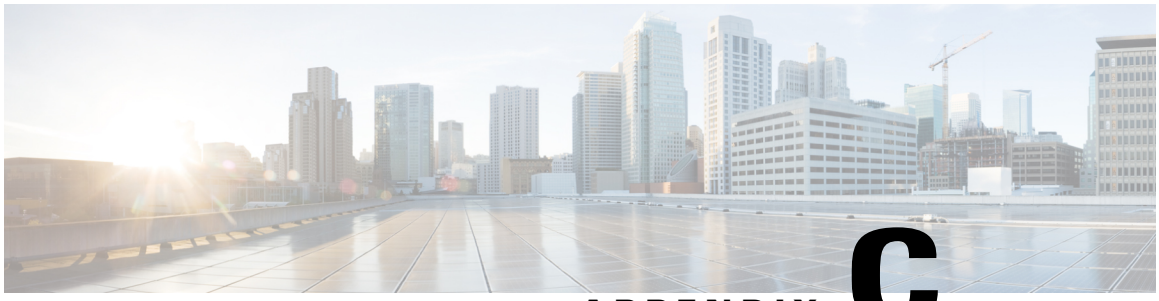
Related Topics

Enable Dependency Records , on page 981

Dependency Record Buttons

Three buttons display in the Dependency Records Summary window:

- Refresh—Updates the window with current information.
- Close—Closes the window but does not return to the Cisco Unified Communications Manager configuration window in which you clicked the Dependency Records link.
- Close and Go Back—Closes the window and returns to the Cisco Unified Communications Manager configuration window in which you clicked the Dependency Records link.



APPENDIX C

Non-Cisco SIP Phones Setup

This appendix provides information about Configuring Non-Cisco Phones That Are Running SIP.

About Non-Cisco SIP Phone Setup

Cisco Unified Communications Manager supports Cisco Unified IP Phones with SIP as well as RFC3261-compliant phones that are running SIP from third-party companies. This appendix describes how to configure the third-party phones that are running SIP by using Cisco Unified Communications Manager Administration.

Third-Party SIP Phone Setup Process

Cisco Unified Communications Manager supports Cisco Unified IP Phones with SIP as well as RFC3261-compliant phones that are running SIP from third-party companies. You can manually configure a third-party phone that is running SIP by using Cisco Unified Communications Manager Administration.

Note Cisco Unified Communications Manager does not support third party SIP phone registration using the same IP unless the combination of the IP address and the port number in the contact header are unique.

Procedure

Step 1 Gather the information about the phone.

- MAC address
- Physical location of the phone

- Cisco Unified Communications Manager user to associate with the phone
- Partition, calling search space, and location information, if used
- Number of lines and associated DNs to assign to the phone

Step 2 Determine whether sufficient Device License Units are available. If not, purchase and install additional Device License Units. Third-Party SIP Devices (Basic) and (Advanced) consume three and six Device License Units each, respectively.
See topics related to calculating the number of required licenses and obtaining a license in the *Cisco Unified Communications Manager Features and Services Guide*.

Step 3 Configure the end user that will be the Digest User.

Note If the third-party phone that is running SIP does not support an authorization ID (digest user), create a user with a user ID that matches the DN of the third-party phone. For example, create an end user named 1000 and create a DN of 1000 for the phone. Assign this user to the phone (see Step 9, on page 986).

Step 4 Configure the SIP Profile or use the default profile. The SIP Profile gets added to the phone that is running SIP by using the Phone Configuration window.

Note Third-party phones that are running SIP use only the SIP Profile Information section of the SIP Profile Configuration window.

Step 5 Configure the Phone Security Profile. To use digest authentication, you must configure a new phone security profile. If you use one of the standard, nonsecure SIP profiles that are provided for auto-registration, you cannot enable digest authentication.

Step 6 Add and configure the third-party phone that is running SIP by choosing Third-party SIP Device (Advanced) or (Basic) from the Add a New Phone Configuration window.

Note Third-party SIP Device (Basic) supports one line and consumes three license units, and Third-party SIP Device (Advanced) supports up to eight lines and video and consumes six license units.

Step 7 Add and configure lines (DNs) on the phone.

Step 8 In the End User Configuration window, associate the third-party phone that is running SIP with the user by using Device Association and choosing the phone that is running SIP.

Step 9 In the Digest User field of the Phone Configuration window, choose the end user that you created in Step 3, on page 986.

Step 10 Provide power, install, verify network connectivity, and configure network settings for the third-party phone that is running SIP.
See the administration guide that was provided with your phone that is running SIP.

Step 11 Make calls with the third-party phone that is running SIP.
See the user guide that came with your third-party phone that is running SIP.

Related Topics

Phone Security Profile Setup , on page 167
Directory Number Setup , on page 289
Set Up Cisco Unified IP Phone , on page 620
Set Up Speed-dial Buttons or Abbreviated Dialing , on page 625
About SIP Profile Setup , on page 745
About End User Setup , on page 841

Associate Devices to End User , on page 856
Enable Digest Authentication for Third-Party SIP Phones , on page 988

Different Setups for SIP Phones

The following table provides a comparison overview of the configuration differences between Cisco Unified IP Phones and third-party phones that are running SIP.

Table 140: Model Configuration Comparison for Phones That Are Running SIP

Phone That Is Running SIP	Integrated with Centralized TFTP	Sends MAC Address	Downloads Softkey File	Downloads Dial Plan File	Supports Cisco Unified Communications Manager Failover and Fallback	Supports Reset and Restart
Cisco Unified IP Phone 7911, 7941, 7961, 7970, 7971	Yes	Yes	Yes	Yes	Yes	Yes
Cisco Unified IP Phone 7940, 7960	Yes	Yes	No	Yes	Yes	Yes
Cisco Unified IP Phone 7905, 7912	Yes	Yes	No	No	Yes	Yes
Third-party phone that is running SIP	No	No	No	No	No	No

Use Cisco Unified Communications Manager Administration to configure third-party phones that are running SIP. The administrator must also perform configuration steps on the third-party phone that is running SIP; see following examples:

- Ensure proxy address in the phone is the IP or Fully Qualified Domain Name (FQDN) of Cisco Unified Communications Manager.
- Ensure directory number(s) in the phone match the directory number(s) that are configured for the device in Cisco Unified Communications Manager Administration.
- Ensure digest user ID (sometimes referred to as Authorization ID) in the phone matches the Digest User ID in Cisco Unified Communications Manager Administration.

Consult the documentation that came with the third-party phone that is running SIP for more information.

Related Topics

Where to Find More Information , on page 990

How Cisco Unified Communications Manager Identifies Third-Party Phones

Because third-party phones that are running SIP do not send a MAC address, they must identify themselves by using username.

The REGISTER message includes the following header:

```
Authorization: Digest username="swhite", realm="ccmsipline",
nonce="GBauADss2qoWr6k9y3hGGVDAqnLfoLk5", uri="sip:172.18.197.224", algorithm=MD5,
response="126c0643a4923359ab59d4f53494552e"
```

The username, swhite, must match an end user that is configured in the End User Configuration window of Cisco Unified Communications Manager Administration. The administrator configures the SIP third-party phone with the user; for example, swhite, in the Digest User field of Phone Configuration window.

Note You can assign each end user ID to only one third-party phone (in the Digest User field of the Phone Configuration window). If the same end user ID is assigned as the Digest User for multiple phones, the third-party phones to which they are assigned will not successfully register.

Related Topics

Set Up Cisco Unified IP Phone , on page 620
About End User Setup , on page 841

Third-Party Phones Running SIP and TFTP

Third-party phones that are running SIP do not get configured by using the Cisco Unified Communications Manager TFTP server. The customer configures them by using the native phone configuration mechanism (usually a web page or tftp file). The customer must keep the device and line configuration in the Cisco Unified Communications Manager database synchronized with the native phone configuration (for example, extension 1002 on the phone and 1002 in Cisco Unified Communications Manager). Additionally, if the directory number of a line is changed, ensure that it gets changed in both Cisco Unified Communications Manager Administration and in the native phone configuration mechanism.

Enable Digest Authentication for Third-Party SIP Phones

To enable digest authentication for third-party phones that are running SIP, the administrator must create a Phone Security Profile. See the *Cisco Unified Communications Manager Security Guide* for details. On the Phone Security Profile Configuration window, check the Enable Digest Authentication check box. After the security profile is configured, the administrator must assign that security profile to the phone that is running SIP by using the Phone Configuration window. If this check box is not checked, Cisco Unified Communications Manager will use digest authentication for purposes of identifying the phone by the end user ID, and it will not verify the digest password. If the check box is checked, Cisco Unified Communications Manager will verify the password.

Note Cisco Unified Communications Manager does not support Transport Layer Security (TLS) from third-party phones that are running SIP.

Related Topics

Phone Security Profile Setup , on page 167

DTMF Reception

To require DTMF reception, check the Require DTMF Reception check box that displays on the Phone Configuration window in Cisco Unified Communications Manager Administration.

Licensing Third-Party SIP Phones

Licensing of third-party phones that are running SIP enforces the following limitations:

- Third-party SIP Device (Basic)—Video calls do not get supported. Video enforcement occurs as part of the offer/answer process. If video-related media is provided as part of an offer or answer from a SIP device that is not permitted to negotiate video, only the non-video-related parts of the call get extended to the destination party. Similarly, a SIP endpoint that is not permitted to negotiate media will not receive any video-related media in the SDP that is sent from Cisco Unified Communications Manager.
- Third-party SIP Device (Advanced) and (Basic)—Cisco-specific SIP extensions do not get supported. Some Cisco-specific SIP extensions that are not supported include service URIs, header extensions, dialog subscriptions, and remote call control proprietary mime types. Cisco Unified Communications Manager will reject any request from a phone that is running SIP that is not permitted to use an advanced feature that uses a service request URI (such as Call Pickup URI, Meet Me Service URI). The SIP profile specifies service URIs. The profile gets assigned to SIP devices. Cisco Unified Communications Manager will block features that require the use of Cisco-specific SIP extensions.

Note Ensure that any wireless third-party SIP client or device is configured as a Third-Party SIP Device (Advanced) in conformance with Cisco Unified Communications Manager licensing policy.

For more information about Cisco SIP Extensions, contact your Cisco representative.

In Cisco Unified Communications Manager, Release 5.1(1) and above, certain characteristics for Basic and Advanced Third-Party phones that are running SIP changed. These characteristics include changes to the Maximum Number of Calls per Device, Default Maximum number of calls per DN, and Default Busy Trigger per DN fields that display on the Directory Number Configuration window in Cisco Unified Communications Manager Administration. The following tables provide more information.

Table 141: Directory Number Migration Changes for Basic Third-Party Phones That Are Running SIP

Field Name	Old Value	New Value
Maximum Number of Calls Per Device	8	2

Field Name	Old Value	New Value
Default Maximum Number of Calls per DN	4	2
Default Busy Trigger per DN	2	2

Table 142: Directory Number Migration Changes for Advanced Third-Party Phones That Are Running SIP

Field Name	Old Value	New Value
Maximum Number of Calls Per Device	64	16
Default Maximum Number of Calls per DN	4	2
Default Busy Trigger per DN	2	2

For users that have third-party phones that are running SIP that are configured on any version of release 5.0 that are migrating/upgrading to release 6.0(1) or above, be aware that, after the upgrade, these devices retain their release 5.0 configured values. However, if users need to make changes to DN configuration values, users must change Maximum Number of Calls and Default Busy Trigger values on each DN.

For basic third-party phones that are running SIP, only one line value needs to be modified. However, for advanced third-party phones that are running SIP, users potentially must disassociate lines on the device before they can make any DN-related configuration changes. This situation potentially can happen if more than four lines are configured. An example scenario follows:

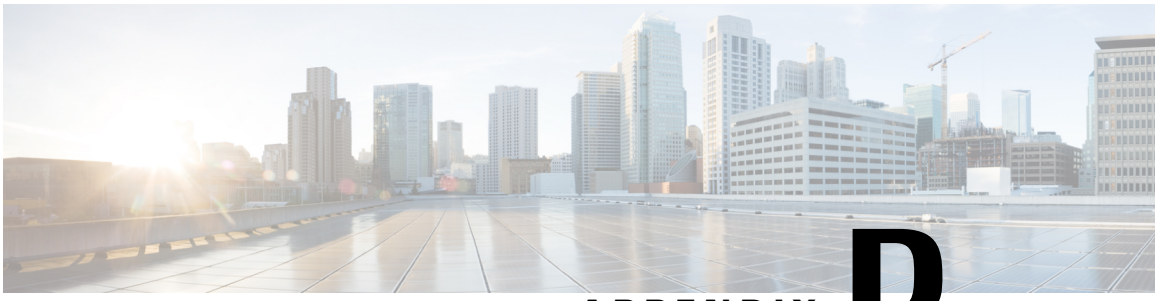
- Advanced phone configured with 6 lines with Maximum number of calls = 4 and Busy Trigger = 2 for each line.
- After upgrade to release 6.1, ensure maximum number of calls on the device is reduced to 16 or below before any DN changes. The current value on this phone equals 24 (6 lines * 4). The device essentially exists in a negative zone (16-24).
- User would disassociate two lines from the device.
- After the user disassociates those lines from the device, you can modify the DN characteristics for the remaining four lines by setting Maximum Number of Calls and Busy Trigger to an appropriate value.
- User reassociates the disassociated lines.

Where to Find More Information

Related Topics

Directory Number Setup , on page 289
Cisco Unified IP Phone Setup , on page 579
SIP Profile Setup , on page 745

End User Setup , on page 841
Third-Party SIP Phone Setup Process , on page 985



APPENDIX D

AS-SIP Configuration

Assured Services SIP (AS-SIP) endpoints are SIP endpoints compliant with MLPP, DSCP, TLS/SRTP, and IPv6 requirements. AS-SIP provides for multiple endpoint interfaces on the Unified Communications Manager. The Third-Party AS-SIP Endpoint device type allows a third-party AS-SIP-compliant generic endpoint to be configured and used with the Unified CM.

The Cisco-proprietary RoundTable (RT) 8961, 9951 and 9971 SIP phones, and their corresponding Unified CM interfaces, are enhanced to provide AS-SIP features. The RT MLPP behavior maintains feature parity with SCCP MLPP implementation. The SIP signaling interface between Unified CM and RT phones is different from the interface between Unified CM and Third-Party AS-SIP Endpoint. The Unified CM sends new configuration parameters to the RT endpoint as part of the extended mark-up language (XML) configuration file. These parameters enable and disable the AS-SIP features and also govern how the RT endpoint operates when using this functionality. The RT endpoint also parses, processes, and sends new headers indicating resource priority for a given call. The RoundTable enhancements focus on TFTP configuration and SIP call processing exchanges between the RT endpoint and the Unified CM.

AS-SIP Capabilities

The following capabilities are implemented or made available for the Third-Party AS-SIP Endpoint interface in compliance with LSC and AS-SIP Line requirements:

- MLPP
- TLS
- SRTP
- DSCP for precedence levels
- Error responses
- V.150.1 MER
- Conference Factory flow support
- MLPP Authentication and Authorization
- AS-SIP Line Early Offer

Note With the exception of AS-SIP Line Early Offer, these capabilities were also implemented, made available, or already existed for the RT 8961, 9951 and 9971 phones and corresponding Unified CM interfaces, in compliance with LSC and SIP EI requirements.

Set Up AS-SIP Line Endpoints

Unified CM supports Cisco Unified IP Phones with SIP as well as RFC3261-compliant phones that are running SIP from third-party companies. This procedure lists the tasks used to manually configure a third-party phone that is running SIP. Use Cisco Unified Communications Manager Administration to configure third party phones.

Procedure

Step 1 Gather the following information about the phone:

- Physical location of the phone Unified Communications Manager user to associate with the phone
- Partition, calling search space, and location information, if used
- Number of lines and associated DNs to assign to the phone

Step 2 Determine whether sufficient Device License Units are available.
All licensing for Unified CM and Unity Connection is centralized and held on the Enterprise License Manager. For more information, refer to the *Enterprise License Manager User Guide*.

Step 3 Configure the end user that will be the Digest User.
See topics related to End User configuration settings for field descriptions.

Note MLPP authentication (optional) requires the phone to send in an MLPP username and password. The end user specifies the highest MLPP precedence level allowed for that user. MLPP credentials are tied to the user while the need to use them is tied to the device (via the MLPP Authorization checkbox in the SIP Profile used by the device).

Step 4 Configure the SIP Profile or use the default profile. The SIP Profile gets added to the phone that is running SIP by using the **Phone Configuration** window.
Third-party AS-SIP phones use the SIP Profile Information section of the **SIP Configuration** window along with the following fields from the phone specific parameters section:

- Resource Priority Namespace
- MLPP User Authorization

Note The phone specific parameters are not downloaded to a third-party AS-SIP phone. They are only used by the Unified CM. Third party phones must locally configure the same settings.

See topics related to SIP profile configuration settings and configuring Cisco Unified IP Phones for more information.

Step 5 Configure the phone security profile.
To use digest authentication, you must configure a new phone security profile. If you use one of the standard, nonsecure SIP profiles that are provided for auto-registration, you cannot enable digest authentication. See topics related to phone security profile configuration and the *Cisco Unified Communications Manager Security Guide* for more information.

The phone security profile must be configured for TLS. See “TLS” section for details.

Step 6 Add and configure the third-party phone that is running SIP by choosing Third-party AS-SIP Endpoint from the **Add a New Phone Configuration** window.
See topics related to configuring Cisco Unified IP Phones for more information.

Step 7 Add and configure lines (DNs) on the phone.
See topics related to directory number configuration for more information.

Step 8 In the **End User Configuration** window, associate the third-party phone that is running SIP with the user by using Device Association and choosing the phone that is running SIP.
See topics related to associating devices to an end user for more information.

Step 9 In the Digest User field of the **Phone Configuration** window, choose the end user that you created in Step 3.

Step 10 Provide power, install, verify network connectivity, and configure network settings for the third-party phone that is running SIP.
See the administration guide that was provided with your phone that is running SIP.

Step 11 Make calls with the third-party phone that is running AS-SIP.
See the user guide that came with your third-party phone that is running SIP.

Configuration Differences for Phones Running AS-SIP

The following table provides a comparison overview of the configuration differences between Cisco Unified IP Phones and third-party phones that are running AS-SIP.

Phone Running AS-SIP	Integrated with Centralized TFTP	Sends MAC Address	Downloads Softkey File	Downloads Dial Plan File	Supports Unified Communications Manager Failover and Fallback	Supports Reset and Restart
Cisco Unified IP Phone 8961, 9951, 9971	Yes	Yes	Yes	Yes	Yes	Yes
Third-party AS-SIP device	No	No	No	No	No	No

Use Unified CM Administration to configure third-party phones that are running SIP (see the "SIP Profile Configuration Settings" section). The administrator must also perform configuration steps on the third-party phone that is running SIP; see following examples:

- Ensure proxy address in the phone is the IP or Fully Qualified Domain Name (FQDN) of Unified Communications Manager.
- Ensure directory number(s) in the phone match the directory number(s) that are configured for the device in Unified CM Administration.
- Ensure digest user ID (sometimes referred to as Authorization ID) in the phone matches the Digest User ID in Unified CM Administration.

Consult the documentation that came with the third-party phone that is running SIP for more information.

AS-SIP Conferencing

MOH is applied to its target (a held party, transferee just prior to transfer, or conferee just prior to joining the conference), if the feature invoker (holder, transferor, or conference initiator) supports Cisco-proprietary feature signaling. If the feature invoker does not support Cisco-proprietary feature signaling then MOH is not applied to its target. Also, if an endpoint explicitly signals that it is a conference mixer, then MOH will not be played to the target. There are two forms of AS-SIP Conferencing:

- Local mixing
- Conference factory

Local mixing

To the Unified CM, the conference initiator simply appears to have established simultaneously active calls, one to each of the other conference attendees. The conference is hosted locally by the initiator and the voices are mixed there. The calls from the conference initiator have special signaling that prevent it from being connected to an MOH source.

Conference factory

The conference initiator calls a Conference Factory Server located off of a SIP trunk. Through IVR signaling, the conference initiator instructs the Conference Factory to reserve a conference bridge. The Conference Factory gives the numeric address (a routable DN) to the conference initiator, who then establishes a subscription with the bridge to receive conference list information to keep track of participants. The Conference factory sends special signaling that will prevent it from being connected to an MOH Source.

Unified Communications Manager Identification of Third-Party Phones

Because third-party phones that are running SIP do not send a MAC address, they must identify themselves by using username.

The REGISTER message includes the following header:

Authorization: Digest
username=”swhite”,realm=”ccmsipline”,nonce=”GBauADss2qoWr6k9y3hGGVDAqnLfoLk5”,uri
=”sip:172.18.197.224”,algorithm=MD5,response=”126c0643a4923359ab59d4f53494552e”

The username, swhite, must match an end user that is configured in the End User Configuration window of Unified CM Administration (see End User Configuration Settings). The administrator configures the SIP third-party phone with the user; for example, swhite, in the Digest User field of Phone Configuration window (see Configuring Cisco Unified IP Phones).

Note You can assign each end user ID to only one third-party phone (in the Digest User field of the Phone Configuration window). If the same end user ID is assigned as the Digest User for multiple phones, the third-party phones to which they are assigned will not successfully register.

Third-Party Phones Running AS-SIP

Third-party phones that are running AS-SIP do not get configured by using the Unified Communications Manager TFTP server. The customer configures them by using the native phone configuration mechanism (usually a web page or tftp file). The customer must keep the device and line configuration in the Unified Communications Manager database synchronized with the native phone configuration (for example, extension 1002 on the phone and 1002 in Unified Communications Manager). Additionally, if the directory number of a line is changed, ensure that it gets changed in both Unified CM Administration and in the native phone configuration mechanism.

End User Configuration Settings

The End User Configuration window in Unified CM Administration allows the administrator to add, search, display, and maintain information about Unified Communications Manager end users. End users can control phones after you associate a phone in the End User Configuration window. If MLPP Authorization is enabled for AS-SIP, MLPP Authorization must also be configured on the End User administration page. This MLPP Authentication requires a user identification number and a password. The MLPP User Identification number must be composed of 6 - 20 numeric characters and the MLPP Password must be composed of 4 - 20 numeric

characters. The Precedence Authorization level can be set to any standard precedence level from Routine to Executive Override.

Note Extension Mobility is not supported for third-party AS-SIP devices.

Note Third-party AS-SIP does not support CAPF.

SIP Profile Configuration Settings

The SIP profile configuration settings contains an 'Is Assured SIP Service Enabled' checkbox. This should be checked for third-party AS-SIP endpoints, as well as AS-SIP trunks. This setting provides specific Assured Service behavior that affects services such as Conference factory and SRTP.

Enable Digest Authentication for Third-Party Phones Running SIP

To enable digest authentication for third-party phones that are running SIP, the administrator must create a Phone Security Profile. (See the “Phone Security Profile Configuration” section a general description and the Unified Communications Manager Security Guide for details.) On the Phone Security Profile Configuration window, check the Enable Digest Authentication check box. After the security profile is configured, the administrator must assign that security profile to the phone that is running SIP by using the Phone Configuration window. If this check box is not checked, Unified CM will use digest authentication for purposes of identifying the phone by the end user ID, and it will not verify the digest password. If the check box is checked, Unified CM will verify the password.

DTMF Reception

To require DTMF reception, check the Require DTMF Reception check box that displays on the Phone Configuration window in Unified CM Administration.

Phone Security Profile Configuration

In Unified CM Administration, use the **System > Security > Phone Security Profile** menu path to configure phone security profiles.

The Phone Security Profile window includes security-related settings such as device security mode, CAPF settings, digest authentication settings (only for phones that are running SIP), and encrypted configuration file settings. You must apply a security profile to all phones that are configured in Unified CM Administration.

Require DTMF Reception

Set Up Phone Security Profile Settings

Set Up TLS

For TLS for third-party AS-SIP devices, configure your call manager correctly using the procedures found in the Security chapter in the Unified Communications Operating System Administration Guide.

You will also need to follow your local procedures for generating certificates.

For information on configuring and applying a phone security profile, see the Unified Communications Manager Security Guide.

Add and Configure Third-Party Phones

Adding and configuring AS-SIP devices is virtually identical to existing third-party device types. There are, however, a few differences. The AS-SIP device type:

- Can be configured for MLPP
- Includes an optional Device Security Mode in the security profile
- For Third-party AS-SIP devices, the preemption setting is not available on the Unified CM. It is completely controlled by the third-party phone.
- Supports Early Offer for voice and video calls

Note Early Offer support for voice and video calls sends an SDP offer in the initial INVITE to the called party.

If Early Offer is enabled for a device, and the Unified CM expects to receive delayed offer calls, a Media Resource Group List must be configured in order to prevent the insertion of MTPs.

Use the following procedure to configure a media resource group list.

Procedure

Step 1 In CUCM Administration, choose **Media Resources > Media Resource Group**.

Step 2 Click the **Add New** button to add a new Media Resource Group List.

Step 3 In the Media Resource Group List, add only the Unified CM-based software MTPs to the Media Resource Group (MRG). Unified CM software resources are typically named MTP_# where # is a number (for example, "MTP_2").

Step 4 This media resource group, which should now contain all the software MTP resources from Unified CM, should not be applied to any media resource group list (MRGL). By placing the MTP resources in an MRG,

but not in an MRGL, these MTP resources are not be available to any of the devices on the system— which is the desired behavior.

Note If the system also has configured hardware MTP resources (which it does not by default), these must also be made unavailable using the same procedure.

For more information on adding and configuring third party phones, see Cisco Unified IP Phone Configuration, CUCM Administration Guide.

INDEX

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W