Cisco Unified Communications Manager Administration Guide

Release 7.1(2)

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-18611-01

Cisco Unified Communications Manager Administration Guide

CONTENTS

PART 10 **Appendixes**

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 documentation by accessing Cisco's product documentation page at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

The preface covers these topics:

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	"Voice Mail Configuration" Contains information on how to configure voice mail and messaging in Cisco Unified Communications Manager Administration.
Part 6	"Device Configuration" Contains information on how to configure devices in Cisco Unified Communications Manager Administration.
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

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

- *Installing Cisco Unified Communications Manager Release 7.1(2)*
- *Upgrading Cisco Unified Communications Manager Release 7.1(2)*
- *Cisco Unified Communications Manager Documentation Guide*
- *Release Notes for Cisco Unified Communications Manager Release 7.1(2)*
- *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.
⟶	This pointer highlights an important line of text in an example.

Convention	Description
^	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.**

Obtaining Documentation and Submitting a 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 1

Cisco Unified Communications Manager

CHAPTER 1

Introduction

Cisco Unified Communications Manager (formerly Cisco Unified CallManager) serves as the software-based call-processing component of the Cisco Unified Communications family of products. A wide range of Cisco Media Convergence Servers provides high-availability server platforms for Cisco Unified Communications Manager call processing, services, and applications.

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), and Cisco Unified Communications Manager Attendant Console

Additional Information

See the "Related Topics" section on page 1-11.

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).

Additional Information

See the “Related Topics” section on page 1-11.

Browsing to Cisco Unified Communications Manager Administration

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. See the “Web Browsers” section on page 1-2 for more information on browsing to the server.

Additional Information

See the “Related Topics” section on page 1-11.

Web Browsers

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

- Microsoft Internet Explorer (IE) 6
- Microsoft Internet Explorer (IE) 7
- Netscape 7.1

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 logon 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.

Cisco Unified Communications Manager Administration Logon

Use the following procedure to log on 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.

Procedure

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

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**.

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

Additional Information

See the "Related Topics" section on page 1-11.

Cisco Unified Communications Manager Administration Log Off

Procedure

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

Step 1 From the main Cisco Unified Communications Manager Administration window, click the **Logout** button that is in the upper, right corner.

Step 2 The window redisplays with the log in fields.

Additional Information

See the "Related Topics" section on page 1-11.

Hypertext Transfer Protocol Over Secure Sockets Layer (HTTPS)

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, the Cisco Unified CM User Options, Trace Collection Tool, the Real-Time Monitoring Tool (RTMT), and 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).

Using Internet Explorer 6 and HTTPS with Cisco Unified Communications Manager Administration

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 **View 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 **View Certificate** > **Install Certificate** option.

Note The address that you use to access Cisco Unified Communications Manager must match the name on the certificate or a message will display 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.

Perform the following procedure to save the HTTPS certificate in the trusted folder in the browser client. For other tasks that you can perform in the Security Alert dialog box, refer to the *Cisco Unified Communications Manager Security Guide*.

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 **View Certificate**.

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

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.

Additional Information

See the "Related Topics" section on page 1-11.

Using Internet Explorer 7 and HTTPS with Cisco Unified Communications Manager Administration

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 Internet Explorer 7, which is a Windows Vista feature, also runs on Windows XP Service Pack 2 (SP2), Windows XP Professional x64 Edition, and Windows Server 2003 Service Pack 1 (SP1). Ensure that Java Runtime Environment (JRE) is present to provide Java-related browser support for IE.

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.

Additional Information

See the "Related Topics" section on page 1-11.

Using Netscape and HTTPS with Cisco Unified Communications Manager Administration

When you use HTTPS with Netscape, you can view the certificate credentials, trust the certificate for one session, trust the certificate until it expires, or not trust the certificate at all.

Tip If you trust the certificate for one session only, you must repeat the following procedure each time that you access the HTTPS-supported application. If you do not trust the certificate, you cannot access the application.

Note The address that you use to access Cisco Unified Communications Manager must match the name on the certificate or a message will display by default. If you access the web application by using the 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.

Perform the following procedure to save the certificate to the trusted folder:

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 certificate authority dialog box displays.

Step 2 Click one of the following radio buttons:

- Accept this certificate for this session
- Do not accept this certificate and do not connect
- Accept this certificate forever (until it expires)

Note If you choose Do not accept, the application does not display.

Note To view the certificate credentials before you continue, click **Examine Certificate**. Review the credentials, and click **Close**.

Step 3 Click **OK**.

The Security Warning dialog box displays.

Step 4 Click **OK**.

Additional Information

See the "Related Topics" section on page 1-11.

Navigating the Cisco Unified Communications Manager Administration Application

After you log on, 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.

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

- Cisco Unified Communications Manager Administration—Shows the 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 main Cisco Unified OS Administration window, so you can configure and administer the Cisco Unified Communications Manager platform. You must log off 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 off from any other application before you can log in to this application.

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** button 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 Presence Server Link

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.

Additional Information

See the "Related Topics" section on page 1-11.

Link to Cisco Unified Presence Server

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.

Additional Information

See the "Related Topics" section on page 1-11.

Customized Log-on Message

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

For more information and the procedure for uploading your customized log-on message, refer to the *Cisco Unified Communications Operating System Administration Guide*.

Additional Information

See the "Related Topics" section on page 1-11.

Last Successful Logon 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 logon.

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.

Additional Information

See the "Related Topics" section on page 1-11.

Accessibility

Cisco Unified Communications Manager Administration and Cisco Unified CM User Options 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.

Accessing the Icons in the Window

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.

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

Accessing the Buttons in the Window

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.

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.
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 Release 7.1(2)*
- *Upgrading Cisco Unified Communications Manager Release 7.1(2)*
- *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)*

Related Topics

- Introduction, page 1-1
- Key Features and Benefits, page 1-1
- Browsing to Cisco Unified Communications Manager Administration, page 1-2
- Using Internet Explorer 6 and HTTPS with Cisco Unified Communications Manager Administration, page 1-4
- Hypertext Transfer Protocol Over Secure Sockets Layer (HTTPS), page 1-4
- Navigating the Cisco Unified Communications Manager Administration Application, page 1-8
- Accessibility, page 1-10
- Where to Find More Information, page 1-10

PART 2

System Configuration

CHAPTER 2

Server Configuration

This chapter contains information on the following topics:

Server Configuration Settings

Use the Server Configuration window to specify the address of the server where Cisco Unified Communications Manager is installed. Table 2-1 describes the server configuration settings. For related procedures, see the "Related Topics" section on page 2-8.

Before You Begin

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 (see the "Deleting a Server" section on page 2-6).
- When you perform a fresh installation of Cisco Unified Communications Manager, you must define any subsequent servers (nodes) in the Cisco Unified Communications Manager Administration Server Configuration window before you can install Cisco Unified Communications Manager on each subsequent server. To define a subsequent node, click **Add New** and perform the procedure in the "Configuring a Server" section on page 2-5. After you add the subsequent server, you can then install the Cisco Unified Communications Manager 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.

Caution If your network supports IPv6 or IPv4 and IPv6 in dual-stack mode, you can provision your DNS server for IPv6 prior to upgrading from Cisco Unified Communications Manager Release 7.0(1) to Release 7.1(2). However, do not configure the DNS records for Cisco Unified Communications Manager for IPv6 until after you upgrade to Release 7.1(2). Configuring the DNS records for Cisco Unified Communications Manager for IPv6 prior to upgrading to Release 7.1(2) causes the upgrade to fail and causes your system to become nonfunctional after you reboot.

- 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 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.
- For additional information on changing the IP address or host name, refer to the document, *Changing the IP Address and Host Name for Cisco Unified Communications Manager Release 7.1(2)*.

Table 2-1 Server Configuration Settings

Field	Description
Server Information	
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** 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.

Table 2-1 Server Configuration Settings (continued)

Field	Description
Server Information	
IPv6 Name	This field supports IPv6. If your network uses DNS that can map to IPv6 addresses, you can enter the host name of the Cisco Unified Communications Manager 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, refer to "Running IPv6 CLI Commands or Configuring IPv6 in the Ethernet IPv6 Window" in 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. ⚠ **Caution** If your network supports IPv6 or IPv4 and IPv6 in dual-stack mode, you can provision your DNS server for IPv6 prior to upgrading from Cisco Unified Communications Manager Release 7.0(1) to Release 7.1(2). However, do not configure the DNS records for Cisco Unified Communications Manager for IPv6 until after you upgrade to Release 7.1(2). Configuring the DNS records for Cisco Unified Communications Manager for IPv6 prior to upgrading to Release 7.1(2) causes the upgrade to fail and causes your system to become nonfunctional after you reboot. **Tip** In addition to configuring the IPv6 Name field, you must configure the IP Address/Hostname field, so Cisco Unified Communications Manager can support features/devices that use IPv4 (or IPv4 and IPv6).
MAC Address	Consider this entry as optional. 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.

Finding a Server

Because you might have several servers in your network, Cisco Unified Communications Manager lets you locate specific servers on the basis of specific criteria. Use the following procedure to locate servers.

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.

Procedure

Step 1 Choose **System** > **Server.**

The Find and List Servers 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.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 2-8.

Configuring a Server

This section describes how to add or update a server address to the Cisco Unified Communications Manager database.

Before You Begin

Before you configure a server, review the following information:

- Make sure that you only add each server once on the Server Configuration window. If you add a server by using the host name and add the same server 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 (see the "Deleting a Server" section on page 2-6).
- When you perform a fresh installation of Cisco Unified Communications Manager, you must define any subsequent servers (nodes) in the Cisco Unified Communications Manager Administration Server Configuration window before you can install Cisco Unified Communications Manager on each subsequent server. To define a subsequent node, click **Add New** and perform the procedure in the "Configuring a Server" section on page 2-5. After you add the subsequent server, you can then install the Cisco Unified Communications Manager 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.

Caution If your network supports IPv6 or IPv4 and IPv6 in dual-stack mode, you can provision your DNS server for IPv6 prior to upgrading from Cisco Unified Communications Manager Release 7.0(1) to Release 7.1(2). However, do not configure the DNS records for Cisco Unified Communications Manager for IPv6 until after you upgrade to Release 7.1(2). Configuring the DNS records for Cisco Unified Communications Manager for IPv6 prior to upgrading to Release 7.1(2) causes the upgrade to fail and causes your system to become nonfunctional after you reboot.

- 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 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 this 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, refer to the *Cisco Unified Serviceability Administration Guide*.

- For additional information on changing the IP address or host name, refer to the document, *Changing the IP Address and Host Name for Cisco Unified Communications Manager Release 7.1(2)*.

Procedure

Step 1 Perform one of the following tasks:

- To add a server, choose **System** > **Server** and click **Add New**.
- To update a server, find the server by using the procedure in the "Finding a Server" section on page 2-4.

The Server Configuration window displays.

Step 2 Enter the appropriate settings as described in Table 2-1.

Step 3 To save the data and to add the server to 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).

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

Additional Information

See the "Related Topics" section on page 2-8.

Deleting a Server

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.

Before You Begin

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, refer to *Cisco Unified Serviceability Administration Guide*.
- To ensure that database files get updated correctly, you must reboot the cluster after you delete a server.
- After you delete the node, access Cisco Unified Reporting to verify 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.

Procedure

Step 1 Find the server by using the procedure in the “Finding a Server” section on page 2-4.

Step 2 From list of matching records, choose the server that you want to delete.

Step 3 Click the **Delete Selected Item** icon that displays in the tool bar in the upper, left corner of the window (or click the **Delete Selected** button that displays at the bottom of the window).

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 for Adding a Deleted Server Back to the Cluster

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 7.1(2) disk, perform a 7.1(2) installation on the node. If you have a disk with a compatible version of 5.X 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 7.1(2) 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, refer to 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.

Additional Information

See the "Related Topics" section on page 2-8.

Related Topics

- Server Configuration Settings, page 2-1
- Finding a Server, page 2-4
- Configuring a Server, page 2-5
- Deleting a Server, page 2-6
- Cisco Unified Communications Manager Configuration, page 3-1
- Internet Protocol Version 6 (IPv6), *Cisco Unified Communications Manager Features and Services Guide*
- *Changing the IP Address and Host Name for Cisco Unified Communications Manager Release 7.1(2)*

CHAPTER 3

Cisco Unified Communications Manager Configuration

Use the following topics to find and update a Cisco Unified Communications Manager configuration or to view system component version information:

Cisco Unified Communications Manager Configuration Settings

Use Cisco Unified Communications Manager configuration to specify the ports and other properties for each Cisco Unified Communications Manager that is installed in the same cluster. A cluster comprises a set of Cisco Unified Communications Managers that enables redundancy.

For the first node in a Cisco Unified Communications Manager cluster, the server gets automatically added as part of the installation. To add additional Cisco Unified Communications Managers to a cluster, the administrator must configure a server (by using Server Configuration) and then configure the Cisco Unified Communications Manager (by using Cisco Unified Communications Manager Configuration). This procedure repeats for each Cisco Unified Communications Manager that is in the cluster.

Table 3-1 describes the Cisco Unified Communications Manager configuration settings. For related procedures, see the "Related Topics" section on page 3-8.

Table 3-1 Cisco Unified Communications Manager Configuration 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.

Table 3-1 Cisco Unified Communications Manager Configuration Settings (continued)

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.
Auto-registration Information	
Starting Directory Number	Enter the first directory number to use for autoregistration of devices.
Ending Directory Number	Enter the last directory number to use for autoregistration of devices. **Note** Specifying a valid 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.
Partition	If you are not using partitions, choose <None>. If you are using partitions, choose the partition to which autoregistered directory numbers belong from the drop-down list box. **Tip** You must choose a range for autoregistration before you can choose a partition, external phone number mask or voice messaging box mask. If more than 250 partitions exist, the ellipsis (**...**) button displays next to the drop-down list box. 1. To display the Select Partition window, click the (**...**) button. 2. In the **List items where Name contains** field, enter a partial partition name. 3. In the list of partitions that displays in the **Select item to use** box, click the desired partition name. 4. Click **OK**.

Table 3-1 Cisco Unified Communications Manager Configuration Settings (continued)

Field	Description
External Phone Number Mask	Specify the mask that is used to format caller ID information for external (outbound) calls that are made from the autoregistered devices. • The mask can contain up to 50 characters. • Enter the literal digits that you want to appear in the caller ID information and use Xs to represent the directory number of the autoregistered 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 autoregistered device.
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 partition and external phone mask information when autoregistration is disabled.

Table 3-1 Cisco Unified Communications Manager Configuration Settings (continued)

Field	Description
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. • Refer to 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.
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. Refer to the *Cisco Unified Communications Manager Security Guide* for information about security configurations.

Finding a Cisco Unified Communications Manager

Because you may have several Cisco Unified Communications Managers in your network, Cisco Unified Communications Manager Administration lets you locate specific Cisco Unified Communications Managers on the basis of specific criteria. Use the following procedure to locate Cisco Unified Communications Managers.

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, the system retains your Cisco Unified Communications Manager search preferences until you modify your search.

Procedure

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

The Find and List Cisco Unified CMs 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.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 3-8.

Updating a Cisco Unified Communications Manager

This section describes how to update a Cisco Unified Communications Manager.

Procedure

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

The Find and List Cisco Unified CMs window displays.

Step 2 To update a Cisco Unified Communications Manager, locate the appropriate Cisco Unified Communications Manager as described in "Finding a Cisco Unified Communications Manager" section on page 3-4. Click the Cisco Unified Communications Manager that you want to update and continue with Step 3.

Step 3 Enter the appropriate settings as described in Table 3-1.

Step 4 Click **Save**.

Additional Information

See the "Related Topics" section on page 3-8.

Synchronizing a 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 will apply any outstanding configuration settings in the least-intrusive manner possible. (For example, a reset/restart may not be required on some affected devices.)

Procedure

Step 1 Choose **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**.

Additional Information

See the "Related Topics" section on page 3-8.

Cisco CallManager Service Activation/Deactivation

The following requirements apply to Cisco CallManager service activation and deactivation:

- Cisco CallManager Service Activation, page 3-7
- Cisco CallManager Service Deactivation, page 3-7

Additional Information

See the "Related Topics" section on page 3-8.

Cisco CallManager Service Activation

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.

Additional Information

See the "Related Topics" section on page 3-8.

Cisco CallManager Service Deactivation

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**.

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, refer to the *Cisco Unified Serviceability Administration Guide*.

Additional Information

See the "Related Topics" section on page 3-8.

Related Topics

- Cisco Unified Communications Manager Configuration Settings, page 3-1
- Finding a Cisco Unified Communications Manager, page 3-4
- Updating a Cisco Unified Communications Manager, page 3-6
- Synchronizing a Cisco Unified Communications Manager With Devices, page 3-6
- Cisco CallManager Service Activation/Deactivation, page 3-7
- Server Configuration, page 2-1
- *Cisco Unified Serviceability Administration Guide*

CHAPTER 4

Cisco Unified Communications Manager Group Configuration

Use the following topics to add, update, or delete a Cisco Unified Communications Manager group:

Cisco Unified Communications Manager Group Configuration Settings

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.

Table 4-1 describes the configuration settings for Cisco Unified Communications Manager groups. For related procedures, see the "Related Topics" section on page 4-6.

Table 4-1 Cisco Unified Communications Manager Group Configuration Settings

Field	Description
Cisco Unified Communications Manager Group Settings	
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.

Finding a Cisco Unified Communications Manager Group

Because you might have several Cisco Unified Communications Manager groups in your network, Cisco Unified Communications Manager Administration lets you locate specific Cisco Unified Communications Manager groups on the basis of specific criteria. Use the following procedure to locate Cisco Unified Communications Manager groups.

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.

Procedure

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

The Find and List Cisco Unified CM Groups 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.

To filter or search records

- From the drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 4-6.

Configuring a Cisco Unified Communications Manager Group

This section describes how to add, copy, or update a Cisco Unified Communications Manager group.

Before You Begin

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. See the "Updating a Cisco Unified Communications Manager" section on page 3-6 for more information.

Procedure

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

The Find and List Cisco Unified CM Groups window displays.

Step 2 Perform one of the following tasks:

- To copy an existing Cisco Unified Communications Manager Group, locate the appropriate Cisco Unified Communications Manager Group as described in the "Finding a Cisco Unified Communications Manager Group" section on page 4-3, choose the Cisco Unified Communications Manager Group that you want to copy, click **Copy** and continue with Step 3.
- To add a new Cisco Unified Communications Manager Group, click **Add New** and continue with Step 3.
- To update an existing Cisco Unified Communications Manager Group, locate the appropriate Cisco Unified Communications Manager Group as described in the "Finding a Cisco Unified Communications Manager Group" section on page 4-3 and continue with Step 3.

Step 3 Enter the appropriate settings as described in Table 4-1.

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 save the Cisco Unified Communications Manager Group configuration in the database.

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.

Additional Information

See the "Related Topics" section on page 4-6.

Synchronizing a Cisco Unified Communications Manager Group with Affected Devices

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

Procedure

Step 1 Choose **Media Resources > 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**.

Additional Information

See the "Related Topics" section on page 4-6.

Deleting a Cisco Unified Communications Manager Group

This section describes how to delete a Cisco Unified Communications Manager Group from the database.

Before You Begin

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. For more information about dependency records, see the "Accessing Dependency Records" section on page A-2.

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. See the "Configuring a Device Pool" section on page 9-11.
- Create or choose a different Cisco Unified Communications Manager group to be the Auto-registration Cisco Unified Communications Manager Group.

Procedure

Step 1 Find the Cisco Unified Communications Manager group by using the procedure in the "Finding a Cisco Unified Communications Manager Group" section on page 4-3.

Step 2 From the list of matching records, choose the group that you want to delete.

Step 3 Click the **Delete Selected** icon that displays in the tool bar in the upper, left corner of the window (or click the **Delete Selected** button that displays at the bottom of the window) to delete the Cisco Unified Communications Manager group.

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

Additional Information

See the "Related Topics" section on page 4-6.

Related Topics

- Cisco Unified Communications Manager Group Configuration Settings, page 4-1
- Cisco Unified Communications Manager Group Configuration, page 4-1
- Finding a Cisco Unified Communications Manager Group, page 4-3
- Synchronizing a Cisco Unified Communications Manager Group with Affected Devices, page 4-4
- Configuring a Cisco Unified Communications Manager Group, page 4-4
- Deleting a Cisco Unified Communications Manager Group, page 4-5

CHAPTER 5

Phone NTP Reference Configuration

Use the following topics to configure phone NTP references:

Phone NTP Reference Configuration Settings

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.

Table 5-1 describes the phone NTP reference configuration settings. For related procedures, see the "Related Topics" section on page 5-5.

Table 5-1 Phone NTP Reference Configuration 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.

Table 5-1 Phone NTP Reference Configuration Settings (continued)

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.

Finding the Phone NTP References

Because you can configure several phone NTP references in Cisco Unified Communications Manager Administration, Cisco Unified Communications Manager Administration allows you to locate specific phone NTP references. Use the following procedure to locate the phone NTP references that exist in Cisco Unified Communications Manager Administration.

Note During your work in a browser session, the cookies on the client machine store your find/list 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, the system retains your Cisco Unified Communications Manager search preferences until you modify your search.

Procedure

Step 1 Choose **System** > **Phone NTP Reference**.

The Find and List Phone NTP References 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.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 5-5.

Configuring the Phone NTP References

This section describes how to add a phone NTP reference to the Cisco Unified Communications Manager database or to update a phone NTP reference that exists in the database.

Procedure

Step 1 Choose **System** > **Phone NTP Reference**.

The Find and List window displays.

Step 2 Perform one of the following tasks:

- To add the phone NTP reference to the Cisco Unified Communications Manager database, click the **Add New** button and continue with Step 3.
- To update an existing phone NTP reference, locate the existing phone NTP reference as described in the "Finding the Phone NTP References" section on page 5-2 and continue with Step 3.

Step 3 Enter the appropriate settings as described in Table 5-1.

Step 4 To save the configuration 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).

Next Steps

After you add a new phone NTP reference to the Cisco Unified Communications Manager database, assign it to a date/time group. For more information, refer to the "Configuring a Date/Time Group" section on page 6-4.

Additional Information

See the "Related Topics" section on page 5-5.

Deleting the Phone NTP Reference

This section describes how to delete a phone NTP reference from the Cisco Unified Communications Manager database.

Before You Begin

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. For more information about dependency records, refer to the "Accessing Dependency Records" section on page A-2.

Procedure

Step 1 By using the procedure in the "Finding the Phone NTP References" section on page 5-2, find the phone NTP reference.

Step 2 To delete multiple phone NTP references, check the check boxes next to the appropriate phone NTP references in the Find and List window; then, click the **Delete Selected** icon or the **Delete Selected** button.

Step 3 To delete a single phone NTP reference, perform one of the following tasks:

- In the Find and List window, check the check box next to the appropriate phone NTP reference; then, click the **Delete Selected** icon or the **Delete Selected** button.
- In the Find and List window, click the Name link for the phone NTP reference. After the Phone NTP Reference Configuration window for that specific phone NTP reference displays, click the **Delete Selected** icon or the **Delete Selected** button.

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

Additional Information

See the "Related Topics" section on page 5-5.

Related Topics

- Phone NTP Reference Configuration Settings, page 5-1
- Phone NTP Reference Configuration, page 5-1
- Finding the Phone NTP References, page 5-2
- Configuring the Phone NTP References, page 5-3
- Deleting the Phone NTP Reference, page 5-4
- Finding a Date/Time Group, page 6-3
- Configuring a Date/Time Group, page 6-4
- Deleting a Date/Time Group, page 6-6
- Deleting a Date/Time Group, page 6-6

CHAPTER 6

Date/Time Group Configuration

Use the following topics to add, update, or delete Date/Time Groups, and to synchronize configuration changes with affected devices:

Date/Time Group Configuration Settings

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 24 time zones.

Table 6-1 describes the date/time group configuration settings. For related procedures, see the "Related Topics" section on page 6-6.

Table 6-1 Date/Time Group Configuration Settings

Field	Description
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.
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.
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, as described in the "Finding the Phone NTP References" section on page 5-2. Only phone NTP references that exist in the Cisco Unified Communications Manager database display. For information on adding a phone NTP reference to Cisco Unified Communications Manager Administration, see the "Configuring the Phone NTP References" section on page 5-3. 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.

Finding a Date/Time Group

Because you might have several date/time groups in your network, Cisco Unified Communications Manager Administration lets you locate specific date/time groups on the basis of specific criteria. Use the following procedure to locate date/time groups.

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.

Procedure

Step 1 Choose **System** > **Date/Time Group.**

The Find and List Date/Time Groups 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.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 6-6.

Configuring a Date/Time Group

This section describes how to add, copy, or update a date/time group to the Cisco Unified Communications Manager database.

Procedure

Step 1 Choose **System** > **Date/Time Group**.

The Find and List Date/Time Groups window displays.

Step 2 Perform one of the following tasks:

- To copy an existing date/time group, locate the appropriate date/time group as described in the "Finding a Date/Time Group" section on page 6-3, choose the date/time group that you want to copy, click the **Copy** icon that displays in the tool bar in the upper, left corner of the window (or the **Copy** button that displays at the bottom of the window), and continue with Step 3.
- To add a new date/time group, click the **Add New** button and continue with Step 3.
- To update an existing date/time group, locate the appropriate date/time group as described in the "Finding a Date/Time Group" section on page 6-3 and continue with Step 3.

Step 3 Enter the appropriate settings as described in Table 6-1.

Step 4 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, as described in the "Phone NTP Reference Configuration" section on page 5-1. To add a phone NTP reference to a date/time group for a phone that is running SIP, perform the following tasks:

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

b. Find the phone NTP reference(s) that you want to add, as described in the "Finding the Phone NTP References" section on page 5-2.

Only phone NTP references that exist in the Cisco Unified Communications Manager database display. For information on adding a phone NTP reference to Cisco Unified Communications Manager Administration, see the "Configuring the Phone NTP References" section on page 5-3.

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 5 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 6 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 described in "Synchronizing a Date/Time Group With Affected Devices" section on page 6-5 before deciding on whether to proceed to Step 7.

Step 7 To reset the devices that use the date/time group, click **Reset**.

Next Steps

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. For more information, refer to the "Configuring a Device Pool" section on page 9-11.

Additional Information

See the "Related Topics" section on page 6-6.

Synchronizing a Date/Time Group With Affected Devices

To synchronize devices to a date/time group that has undergone configuration changes, perform the following procedure, which will apply any outstanding configuration settings in the least-intrusive manner possible. (For example, a reset/restart may not be required on some affected devices.)

Procedure

Step 1 Choose **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**.

Additional Information

See the "Related Topics" section on page 6-6.

Deleting a Date/Time Group

This section describes how to delete a date/time group from the Cisco Unified Communications Manager database.

Before You Begin

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. For more information about dependency records, refer to the "Accessing Dependency Records" section on page A-2.

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. Refer to the "Configuring a Device Pool" section on page 9-11.
- Delete the device pools that use the date/time group that you want to delete. Refer to the "Deleting a Device Pool" section on page 9-13.

Procedure

Step 1 Find the date/time group by using the procedure in the "Finding a Date/Time Group" section on page 6-3.

Step 2 From the list of matching records, choose the date/time group that you want to delete.

Step 3 Click the **Delete Selected Item** icon that displays in the tool bar in the upper, left corner of the window (or click the **Delete Selected** button that displays at the bottom of the window) to delete the date/time group.

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

Additional Information

See the "Related Topics" section on page 6-6.

Related Topics

- Date/Time Group Configuration Settings, page 6-1
- Date/Time Group Configuration, page 6-1
- Finding a Date/Time Group, page 6-3

- Configuring a Date/Time Group, page 6-4
- Synchronizing a Date/Time Group With Affected Devices, page 6-5
- Deleting a Date/Time Group, page 6-6
- Finding the Phone NTP References, page 5-2
- Configuring the Phone NTP References, page 5-3

CHAPTER 7

Presence Group Configuration

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, a presence entity, from the device of the watcher.

Cisco Unified Communications Manager controls which destinations a watcher can monitor with presence groups. A 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 presence request. Presence authorization works with the presence groups that are configured to ensure that a watcher has permission to monitor the status of a destination.

After you configure the presence groups, you apply a 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 presence groups, refer to the "Presence" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

CHAPTER 8

Region Configuration

Use regions to specify the bandwidth that is used for audio and video calls within a region and between existing regions. Use the following procedures to add, update, or delete regions, and to synchronize configuration changes with affected devices:

- Region Configuration Settings, page 8-1
- Finding a Region, page 8-4
- Configuring a Region, page 8-5
- Synchronizing a Region With Affected Devices, page 8-9
- Deleting a Region, page 8-9
- Related Topics, page 8-10

Refer to the "Regions" section in the *Cisco Unified Communications Manager System Guide* for more information about configuring regions and selecting audio codecs.

Region Configuration Settings

Use regions to specify the bandwidth that is used for audio and video calls within a region and between existing regions.

- The audio codec determines the type of compression and the maximum amount of bandwidth that is used per audio call.
- The video call bandwidth comprises the sum of the audio bandwidth and video bandwidth but does not include overhead.

Note The default audio codec for all calls through Cisco Unified Communications Manager specifies G.711. If you do not plan to use any other audio codec, you do not need to use regions. See the "Related Topics" section on page 8-10 for more information.

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 inter-/intra-region audio codecs and video bandwidth.
- This enhancement requires an MCS 7845H1 or higher server.

- Refer to 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.

Table 8-1 summarizes the audio codec and video call bandwidth settings that can be specified for regions. For related procedures, see the “Related Topics” section on page 8-10.

Table 8-1 Region Configuration Settings

Field	Description
Region Information	
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	The entries in this column specify the audio codec relationship between the region that you are configuring and the region that displays in the corresponding row.
Video Call Bandwidth	The entries in this column specify the video call bandwidth relationship between the region that you are configuring and the region that displays in the corresponding row.
Link Loss Type	The entries in this column specify the link loss type relationship 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.

Table 8-1 Region Configuration Settings (continued)

Field	Description
Audio Codec	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 to use for calls between this region and the specified region. To choose the default setting, choose the Use System Default value. • Cisco recommends that you choose the default settings that you configured in the Cisco Unified Communications Manager Administration Service Parameters Configuration window. See the "Configuring Default Values" section on page 8-5. • Because of bandwidth constraints at most remote-site deployments, use G.729 as the recommended default audio codec setting between a new region and existing regions.
Video Call Bandwidth	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 kb/s, 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 bandwidth is allotted between this region and the specified region. • kbps—Click this button to allot video call bandwidth between the region that you are configuring and the specified region. Enter the bandwidth that is available for each video call between these two regions. Valid values range from 1 to 32256.
Link Loss Type	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 link loss type to use for calls between this region and the specified region. 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. • 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. • 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.

Finding a Region

Because you may have several regions in your network, Cisco Unified Communications Manager Administration lets you locate specific regions on the basis of specific criteria. Use the following procedure to locate regions.

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, the system retains your Cisco Unified Communications Manager search preferences until you modify your search.

Procedure

Step 1 Choose **System** > **Region**.

The Find and List Regions 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.

To filter or search records

- From the drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 8-10.

Configuring a Region

Use the following procedure to add or update a region.

Before You Begin

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 addition of a maximum of 2000 regions.

Configuring Default Values

Region entries contain the following values:

- Audio Codec—You define audio codec values that are to be used within the same region, and you also define audio codec values that are to be used between regions.
- Video Call Bandwidth—You define video call bandwidth values that are to be used within the same region, and you also define video call bandwidth values that are to be used between regions.
- Link Loss Type—You define the link loss types that are to be used within the same region, and you also define link loss types that are to be used between regions.

Tip If you set both the audio codec values and the video call bandwidth values to use the default, the system optimizes its performance by making more efficient use of resources.

Note Regions have default values for use within a region (the recommended default value specifies G.711), and regions have default values for use between regions (the recommended default value specifies G.729).

You configure the default values for regions in the Cisco Unified Communications Manager Administration Service Parameters Configuration window. Use the following procedure:

1. Choose **System** > **Service Parameters**.
2. From the drop-down Server list box, choose the Cisco Unified Communications Manager server that you want to configure.
3. From the drop-down Service list box, choose **Cisco CallManager (Active)** as the service.

4. The Cisco Unified Communications Manager Administration Service Parameter Configuration window displays.
5. Scroll down to **Clusterwide Parameters (System - Location and Region)** and configure the parameters in this section.
6. 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).

Use the following procedure to add or update a region.

Procedure

Step 1 Choose **System** > **Region**.

The Region Configuration window displays.

Step 2 Perform one of the following tasks:

- To add a new region, click the **Add New** button and continue with Step 3.
- To update an existing region, locate the appropriate region as described in the "Finding a Region" section on page 8-4 and continue with Step 3.

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

Step 3 In the Name field, enter the name that you want to assign to the region.

Step 4 To save the new region 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).

Step 5 To configure the default codecs to use within this region, click the name of this region to highlight it in the Regions window pane.

a. From the Audio Codec drop-down list box, choose a default audio codec value to use within this region.

   The audio codec determines the type of compression and the maximum amount of bandwidth that is allocated for these calls. See Table 8-2 for a summary of the available codec types and bandwidth usage.

b. In the Video Call Bandwidth column, click the appropriate radio button to configure the default value to specify the video bandwidth to use for video calls within this region.

   If you specify *None*, the system does not allow video calls.

c. From the Link Loss Type drop-down list box, choose a default link loss type to use within this region.

Note For enhanced scalability, 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 Use System Default in the Cisco Unified Communications Manager Administration Region Configuration window.

Step 6 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.

a. From the Audio Codec drop-down list box, choose a default audio codec value to use between this region and the region that you highlighted.

The audio codec determines the type of compression and the maximum amount of bandwidth that is allocated for these calls. See Table 8-2 for a summary of the available codec types and bandwidth usage.

b. In the Video Call Bandwidth column, click the appropriate radio button to configure the default value to specify the video bandwidth to use for video calls between this region and the region that you highlighted.

If you specify *None*, the system does not allow video calls between this region and the specified region.

c. From the Link Loss Type drop-down list box, choose a default link loss type to use between this region and the region that you highlighted.

Note For enhanced scalability, 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 7 To save the new region 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).

Tip The Region Configuration 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.

Next Step

After adding a new region to the database, you can use it to configure device pools. Devices acquire a region setting from the device pool to which they are assigned. See the "Configuring a Device Pool" section on page 9-11 for information on configuring device pools.

Additional Information

See the "Related Topics" section on page 8-10.

The total bandwidth that is used per call stream depends on the audio codec type as well as factors such as data packet size and overhead (packet header size). The bandwidth figures shown in Table 8-2 apply for 30-ms data packets and include IP headers. Each call comprises two call streams.

Note The codecs that Table 8-2 specifies correlate to an approximate bandwidth usage per call. For information on bandwidth usage for each codec, refer to *Cisco Unified Communications Solution Reference Network Design (SRND)* for the current release of Cisco Unified Communications Manager.

Table 8-2 Bandwidth That Audio Codecs Use

Audio Codec	Bandwidth Used Per Call (Including IP Headers) With 30-ms Data Packets	Description
G.711	80 kb/s	This codec represents the default codec for all Cisco Unified Communications Manager calls.
G.722	80 kb/s	Video endpoints typically prefer this codec.
G.723	24 kb/s	The system supports this low-bit-rate codec for use with older Cisco IP Phone 12 SP Series and Cisco IP Phone 30 VIP.
G.728/iLBC	26.66 kb/s for G.728 24 kb/s for iLBC	Video endpoints support the G.728 low-bit-rate codec. Internet Low Bit Rate Codec (iLBC) enables graceful speech quality degradation in the case of lost frames and is suitable for real-time communications.
G.729	24 kb/s	The system supports this low bit-rate codec for Cisco Unified IP Phone 7900.
Wideband/AAC	272 kb/s	The system supports this high-quality, high-bandwidth audio codec for IP-phone-to-IP-phone calls that the Cisco Unified IP Phone 7900 supports. Use this audio codec if you want to configure the Advanced Audio Codec (AAC) for calls between phones that are running SIP. Advanced Audio Codec (AAC) specifies a wideband voice codec that provides improved voice fidelity and equal or better sound quality over older codecs.
GSM	29 kb/s	The Global System for Mobile Communications (GSM) codec enables the MNET system for GSM wireless handsets to interoperate with Cisco Unified Communications Manager.

Synchronizing a Region With Affected Devices

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

Procedure

Step 1 Choose **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 Region 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**.

Additional Information

See the "Related Topics" section on page 8-10.

Deleting a Region

This section describes how to delete a region from the Cisco Unified Communications Manager database.

Before You Begin

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. For more information about dependency records, see the "Accessing Dependency Records" section on page A-2.

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. See the "Configuring a Device Pool" section on page 9-11.
- Delete the device pools that use the region that you want to delete. See the "Deleting a Device Pool" section on page 9-13.

Procedure

Step 1 Find the region by using the procedure in the "Finding a Region" section on page 8-4.

Step 2 From the list of matching records, choose the region that you want to delete.

Step 3 To delete the region, click the **Delete Selected** icon that displays in the tool bar in the upper, left corner of the window (or click the **Delete Selected** button that displays at the bottom of the window).

Tip The Region Configuration 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.

Additional Information

See the "Related Topics" section on page 8-10.

Related Topics

- Region Configuration Settings, page 8-1
- Finding a Region, page 8-4
- Configuring a Region, page 8-5
- Synchronizing a Region With Affected Devices, page 8-9
- Deleting a Region, page 8-9
- Regions, *Cisco Unified Communications Manager System Guide*
- Call Admission Control, *Cisco Unified Communications Manager System Guide*

CHAPTER 9

Device Pool Configuration

Use the following topics to add, update, or delete a device pool:

Refer to the "System-Level Configuration Settings" chapter in the *Cisco Unified Communications Manager System Guide* for more information about device pools and the device settings that are assigned through device pools.

Refer to the "Common Device Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide* for more information on configuring Common Device Configuration parameters.

Device Pool Configuration Settings

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 only 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.

Table 9-1 lists and describes device pool configuration settings. For related procedures, see the "Related Topics" section on page 9-14.

Table 9-1 Device Pool Configuration 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.

Table 9-1 Device Pool Configuration Settings (continued)

Field Name	Description
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.
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, refer to "Hold Reversion" in the *Cisco Unified Communications Manager Features and Services Guide*.
Local Route Group	From the drop-down list box, choose a route group to use as the local route group for the devices in this device pool. Choosing the default value <None> prevents implementation of the Local Route Group feature. Refer to the "Local Route Groups" chapter in the *Cisco Unified Communications Manager Administration Guide* for additional information about the Local Route Groups 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.

Table 9-1 Device Pool Configuration Settings (continued)

Field Name	Description
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.
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 more details about locations, see the "Location Configuration" section on page 17-1. For an explanation of location-based CAC across intercluster trunks, see "Location-Based Call Admission Control Over Intercluster Trunk" 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.

Table 9-1 Device Pool Configuration Settings (continued)

Field Name	Description
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.
Connection Monitor Duration	This setting defines the time that the IP phone monitors its connection to Cisco Unified Communications Manager before it unregisters from SRST and reregisters to Cisco Unified Communications Manager. The default value, which specifies 120 seconds, resides in the Connection Monitor Duration enterprise parameter. Change this setting if you need to disable the connection monitor (by changing the value to zero) or if you want to extend the connection monitor time. **Note** 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, refer to the "Survivable Remote Site Telephony References" section 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.

Table 9-1 Device Pool Configuration Settings (continued)

Field Name	Description
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.
Device Mobility Group	Device mobility groups represent the highest level geographic entities in your network and are used to support the device mobility feature.
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.

Table 9-1 Device Pool Configuration Settings (continued)

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 CSS 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, refer to "Introducing Geolocations" and "Geolocation Configuration" in the "Geolocations and Location Conveyance" chapter in the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocations, refer to the "Logical Partitioning" chapter 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, refer to "Introducing Geolocation Filters" and "Geolocation Filter Configuration" in the "Geolocations and Location Conveyance" chapter in the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocation filters, refer to the "Logical Partitioning" chapter in 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**.

Table 9-1 Device Pool Configuration Settings (continued)

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 "Configuring the Incoming Calling Party Settings in the Device Pool, Gateway, or Trunk Configuration Windows" in the *Cisco Unified Communications Manager Features and Services Guide*.

Table 9-1 Device Pool Configuration Settings (continued)

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 "Configuring the Incoming Calling Party Settings in the Device Pool, Gateway, or Trunk Configuration Windows" in the *Cisco Unified Communications Manager Features and Services Guide*.

Table 9-1 Device Pool Configuration Settings (continued)

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 "Configuring the Incoming Calling Party Settings in the Device Pool, Gateway, or Trunk Configuration Windows" in the *Cisco Unified Communications Manager Features and Services Guide*.

Table 9-1 Device Pool Configuration Settings (continued)

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 "Configuring the Incoming Calling Party Settings in the Device Pool, Gateway, or Trunk Configuration Windows" in the *Cisco Unified Communications Manager Features and Services Guide*.

Finding a Device Pool

Because you might have several device pools in your network, Cisco Unified Communications Manager Administration lets you locate specific device pools on the basis of specific criteria. Use the following procedure to locate device pools.

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

Procedure

Step 1 Choose **System** > **Device Pool**.

The Find and List Device Pools 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.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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.

Additional Information

See the “Related Topics” section on page 9-14.

Configuring a Device Pool

This section describes how to add, copy, or update a device pool to the Cisco Unified Communications Manager database. 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 Begin

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). Refer to the "Configuring a Cisco Unified Communications Manager Group" section on page 4-4.
- Date/time group (required). Refer to the "Configuring a Date/Time Group" section on page 6-4.
- Region (required). Refer to the "Configuring a Region" section on page 8-5.
- SRST reference (optional). Refer to the "Configuring an SRST Reference" section on page 19-4.
- Media resource group list (optional). Refer to the "Configuring a Media Resource Group List" section on page 80-3.
- Calling search space for auto-registration (optional). Refer to the "Configuring a Calling Search Space" section on page 53-4.
- Reverted call focus priority (optional). Refer to the "Hold Reversion" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
- Device mobility group (optional). See the "Configuring a Device Mobility Group" section in the *Cisco Unified Communications Manager Features and Services Guide*.
- Device mobility calling search space. See the "Configuring a Calling Search Space" section on page 53-4.
- Physical location (optional). See the "Configuring a Physical Location" section in the *Cisco Unified Communications Manager Features and Services Guide*.
- Location. See the "Configuring a Location" section on page 17-5.
- AAR group. See the "Configuring an AAR Group" section on page 37-4.
- AAR calling search space. See the "Configuring a Calling Search Space" section on page 53-4.

Procedure

Step 1 Choose **System** > **Device Pool**.

The Find and List Device Pools window displays.

Step 2 Perform one of the following tasks:

- To copy an existing device pool, locate the appropriate device pool as described in the "Finding a Device Pool" section on page 9-10, click the **Copy** button next to the device pool that you want to copy, and continue with Step 3.
- To add a new device pool, click the **Add New** button and continue with Step 3.
- To update an existing device pool, locate the appropriate device pool as described in the "Finding a Device Pool" section on page 9-10 and continue with Step 3.

Step 3 Enter the appropriate fields as described in Table 9-1.

Step 4 To save the device pool information to the database, click **Save**.

Additional Information

See the "Related Topics" section on page 9-14.

Synchronizing a Device Pool With Affected Devices

To synchronize devices to a device pool that has undergone configuration changes, perform the following procedure, which will apply any outstanding configuration settings in the least-intrusive manner possible. (For example, a reset/restart may not be required on some affected devices.)

Procedure

Step 1 Choose **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 Information 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**.

Additional Information

See the "Related Topics" section on page 9-14.

Deleting a Device Pool

This section describes how to delete a device pool from the Cisco Unified Communications Manager database.

Before You Begin

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. Refer to the "Deleting a Phone" section on page 91-33.
- Delete the devices that are assigned to the device pool that you want to delete. Refer to the "Deleting a Phone" section on page 91-33.

Procedure

Step 1 Find the device pool by using the procedure in the "Finding a Device Pool" section on page 9-10.

Step 2 From the list of matching records, choose the device pool that you want to delete.

Step 3 Click **Delete Selected**.

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

Additional Information

See the "Related Topics" section on page 9-14.

Related Topics

- Device Pool Configuration Settings, page 9-1
- Finding a Device Pool, page 9-10
- Configuring a Device Pool, page 9-11
- Synchronizing a Device Pool With Affected Devices, page 9-13
- Deleting a Device Pool, page 9-13
- Local Route Groups, *Cisco Unified Communications Manager Features and Services Guide*
- Calling Party Normalization, *Cisco Unified Communications Manager Features and Services Guide*

CHAPTER 10

Device Mobility Group Configuration

Device mobility groups support the device mobility feature. Device mobility groups represent the highest level geographic entities in your network. Depending upon the network size and scope, your device mobility groups could represent countries, regions, states or provinces, cities, or other entities. For example, an enterprise with a worldwide network might choose device mobility groups that represent individual countries, whereas an enterprise with a national or regional network might define device mobility groups that represent states, provinces, or cities.

Refer to "Device Mobility" in the *Cisco Unified Communications Manager Features and Services Guide* for more information on the Device Mobility feature.

CHAPTER 11

Device Mobility Info Configuration

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.

Refer to "Device Mobility" in the *Cisco Unified Communications Manager Features and Services Guide* for more information on the Device Mobility feature.

CHAPTER 12

DHCP Server Configuration

This chapter contains the following topics:

DHCP Server Configuration Settings

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.

Table 12-1 describes the server configuration settings. For related procedures, see the "Related Topics" section on page 12-6.

Table 12-1 DHCP Server Configuration 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.

Table 12-1 DHCP Server Configuration Settings (continued)

Server Information Field	Description
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.
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.

Activating 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 Unified 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. See the "Starting DHCP Monitor Service" section on page 12-3 to stop, start, or restart the service.

Additional Information

See the "Related Topics" section on page 12-6.

Starting 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 If the Cisco DHCP Monitor Service was activated by using "Activating DHCP Monitor Service" section on page 12-2, the Status displays as Activated.

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.

Additional Information

See the "Related Topics" section on page 12-6.

Finding a DHCP Server

Because you might have several servers in your network, Cisco Unified Communications Manager lets you locate specific DHCP servers on the basis of specific criteria. Use the following procedure to locate servers.

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, the system retains your Cisco Unified Communications Manager search preferences until you modify your search.

Procedure

Step 1 Choose **System** > **DHCP** > **DHCP Server**.

The Find and List DHCP Servers window displays.

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records:

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

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

Step 3 Click **Find**.

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

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

Step 4 From the list of records that display, click the link for the record 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.

Additional Information

See the "Related Topics" section on page 12-6.

Configuring a DHCP Server

This section describes how to add, copy, and update a DHCP server address to the Cisco Unified Communications Manager database.

Procedure

Step 1 Choose **System** > **DHCP** > **DHCP Server**

Step 2 Perform one of the following tasks:

- To add a DHCP server, click **Add New**.
- To update a server, find the server by using the procedure in the "Finding a DHCP Server" section on page 12-4.
- To copy a server, find the server by using the procedure in the "Finding a DHCP Server" section on page 12-4, select the DHCP server that you want by checking the check box next to the server name, and click the **Copy** icon.

The DHCP Server Configuration window displays.

Step 3 Enter the appropriate settings as described in Table 12-1.

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 save the data and to add the server to the database.

Additional Information

See the "Related Topics" section on page 12-6.

Deleting a DHCP Server

This section describes how to delete a DHCP server from the Cisco Unified Communications Manager database.

Procedure

Step 1 Find the DHCP server by using the procedure in the "Finding a DHCP Server" section on page 12-4.

Step 2 From list of matching records, choose the DHCP server that you want to delete.

Step 3 Click the **Delete Selected** icon that displays in the tool bar in the upper, left corner of the window (or click the **Delete Selected** button that displays at the bottom of the window) to delete the server.

If the server is not in use, Cisco Unified Communications Manager deletes it. If it is in use, an error message displays.

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

Additional Information

See the "Related Topics" section on page 12-6.

Related Topics

- DHCP Server Configuration Settings, page 12-1
- Activating DHCP Monitor Service, page 12-2
- Starting DHCP Monitor Service, page 12-3
- Finding a DHCP Server, page 12-4
- Configuring a DHCP Server, page 12-5
- Deleting a DHCP Server, page 12-5
- DHCP Subnet Configuration

Additional Information

- Dynamic Host Configuration Protocol, *Cisco Unified Communications Manager System Guide*

CHAPTER 13

DHCP Subnet Configuration

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

DHCP Subnet Configuration Settings

In the DHCP Subnet Configuration window, you can add subnets to the DHCP server. Table 13-1 describes the DHCP Subnet configuration settings. For related procedures, see the "Related Topics" section on page 13-4.

Table 13-1 DHCP Subnet Configuration Settings

Server Information Field	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.

Table 13-1 DHCP Subnet Configuration Settings (continued)

Server Information Field	Description
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.
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.

Finding a DHCP Subnet

Use the following procedure to locate DHCP subnets.

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, the system retains your Cisco Unified Communications Manager search preferences retained until you modify your search.

Procedure

Step 1 Choose **System** > **DHCP** > **DHCP Subnet**.

The Find and List DHCP Subnets window displays.

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records:

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

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

Step 3 Click **Find**.

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

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

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

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

The window displays the item that you choose.

Additional Information

See the "Related Topics" section on page 13-4.

Configuring a DHCP Subnet

This section describes how to add, update, or copy a DHCP subnet address to the Cisco Unified Communications Manager database.

Procedure

Step 1 Choose **System** > **DHCP** > **DHCP Subnet**

Step 2 Perform one of the following tasks:

- To add a DHCP subnet, click **Add New**.
- To update a subnet, find the subnet by using the procedure in the "Finding a DHCP Subnet" section on page 13-2.

- To copy a subnet, find the subnet by using the procedure in the "Finding a DHCP Subnet" section on page 13-2; select the DHCP server that you want by checking the check box next to the server name and click **Copy**.

The DHCP Subnet Configuration window displays.

Step 3 Enter the appropriate settings as described in Table 13-1.

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 save the data and to add the subnet to the database.

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

Additional Information

See the "Related Topics" section on page 13-4.

Deleting a DHCP Subnet

This section describes how to delete a DHCP subnet from the Cisco Unified Communications Manager database.

Procedure

Step 1 Find the DHCP subnet by using the procedure in the "Finding a DHCP Subnet" section on page 13-2.

Step 2 From list of matching records, choose the DHCP subnet that you want to delete.

Step 3 Click the **Delete Selected** icon that displays in the tool bar in the upper, left corner of the window (or click the **Delete Selected** button that displays at the bottom of the window) to delete the subnet.

If the subnet is not in use, Cisco Unified Communications Manager deletes it. If it is in use, a message displays.

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

Additional Information

See the "Related Topics" section on page 13-4.

Related Topics

- DHCP Subnet Configuration Settings, page 13-1
- Finding a DHCP Subnet, page 13-2

- Configuring a DHCP Subnet, page 13-3
- Deleting a DHCP Subnet, page 13-4
- DHCP Server Configuration, page 12-1
- Dynamic Host Configuration Protocol, *Cisco Unified Communications Manager System Guide*

CHAPTER 14

LDAP System Configuration

In Cisco Unified Communications Manager, LDAP directory configuration takes place in the following windows:

- LDAP System
- LDAP Directory
- LDAP Authentication

Use the following topics to configure LDAP system information:

- LDAP System Configuration Settings, page 14-1
- Updating LDAP System Information, page 14-3
- Related Topics, page 14-4

LDAP System Configuration 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. Table 14-1 describes the LDAP system configuration settings. For related procedures, see the "Related Topics" section on page 14-4.

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. Refer to the "Understanding the Directory" section on page 20-1 for more information about LDAP synchronization.

For end user data, you cannot use the End User Configuration window to update the attributes that get 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 window.

Note If end users exist in the Cisco Unified Communications Manager database before synchronization with a corporate directory occurs, the system will delete those end users that did not have a matching user ID in the corporate directory. 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* would be marked inactive and eventually get deleted by the garbage collector program.

Note After an LDAP Directory configuration for the DirSync service gets created or the LDAP user authentication is enabled, the settings in the LDAP System window become read only.

Note 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.

Table 14-1 LDAP System Configuration Settings

Field	Description
LDAP System Information	
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.

Table 14-1 LDAP System Configuration Settings (continued)

Field	Description
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 • Netscape or Sun ONE LDAP Server • OpenLDAP
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 • For Netscape Sun ONE LDAP Server and OpenLDAP – uid – mail – employeeNumber – telephoneNumber

Updating LDAP System Information

Use the following procedure to update LDAP system information.

Procedure

Step 1 Choose **System** > **LDAP** > **LDAP System**.

Step 2 Enter the appropriate configuration settings as described in Table 14-1.

Step 3 To save your changes, click **Save**.

Additional Information

See the "Related Topics" section on page 14-4.

Related Topics

- LDAP System Configuration Settings, page 14-1
- LDAP System Configuration, page 14-1
- Updating LDAP System Information, page 14-3
- Understanding the Directory, *Cisco Unified Communications Manager System Guide*
- LDAP Directory Configuration, page 15-1
- LDAP Authentication Configuration, page 16-1
- Application User Configuration, page 113-1
- End User Configuration, page 114-1
- Application Users and End Users, *Cisco Unified Communications Manager System Guide*

CHAPTER 15

LDAP Directory Configuration

LDAP directory configuration takes place in three related windows:

- LDAP System
- LDAP Directory
- LDAP Authentication

Use the following topics to configure LDAP directory information:

LDAP Directory Configuration Settings

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. Table 15-1 describes the LDAP directory configuration settings. For related procedures, see the "Related Topics" section on page 15-6.

Before You Begin

Before you can synchronize the LDAP directory, you must activate the Cisco DirSync service. For information about how to activate services, refer to 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 window.

Table 15-1 LDAP Directory Configuration 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.
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.
User Fields To Be Synchronized	

Cisco Unified Communications Manager User Fields	LDAP User Fields	
User ID	sAMAccountName or uid	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.

Table 15-1 LDAP Directory Configuration Settings (continued)

Field		Description
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.
Phone 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
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	department or department number	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
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.
LDAP Port		Enter the port number on which the corporate directory receives the LDAP requests. Default LDAP port for Microsoft Active Directory and for Netscape Directory specifies 389. Default LDAP port for Secured Sockets Layer (SSL) specifies 636.

Table 15-1 LDAP Directory Configuration Settings (continued)

Field	Description
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.

Finding an LDAP Directory

Use the following procedure to locate LDAP directory configurations.

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

Procedure

Step 1 Choose **System** > **LDAP** > **LDAP Directory**.

The Find and List LDAP Directories window displays.

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records:

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

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

Step 3 Click **Find**.

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

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

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

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

The window displays the item that you choose.

Additional Information

See the "Related Topics" section on page 15-6.

Configuring an LDAP Directory

This section describes how to add or update information about an LDAP directory that is used to synchronize user data with the Cisco Unified Communications Manager Administration database.

Procedure

Step 1 Choose **System** > **LDAP** > **LDAP Directory**.

The Find and List LDAP Directories window displays.

Step 2 Perform one of the following tasks:

- To add new information about an LDAP directory, locate the appropriate directory as described in the "Finding an LDAP Directory" section on page 15-4, click the **Add New** button, and continue with Step 3.
- To update existing information about an LDAP directory, locate the appropriate directory as described in the "Finding an LDAP Directory" section on page 15-4 and continue with Step 3.

Step 3 Enter the appropriate settings as described in Table 15-1.

Step 4 Click **Save**.

The new LDAP directory gets added or updated to the Cisco Unified Communications Manager database.

Additional Information

See the "Related Topics" section on page 15-6.

Deleting an LDAP Directory

This section describes how to delete an LDAP directory in Cisco Unified Communications Manager Administration.

Before You Begin

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

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

Procedure

Step 1 Find the LDAP directory that you want to delete by using the procedure in the "Finding an LDAP Directory" section on page 15-4.

Step 2 Click the name of the LDAP directory that you want to delete.

The LDAP directory that you chose displays.

Step 3 Click **Delete**.

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

Step 4 Click **OK**.

The window refreshes, and the LDAP directory gets deleted from the database.

Additional Information

See the "Related Topics" section on page 15-6.

Related Topics

- LDAP Directory Configuration Settings, page 15-1
- Finding an LDAP Directory, page 15-4
- Configuring an LDAP Directory, page 15-5
- Deleting an LDAP Directory, page 15-6
- Understanding the Directory, *Cisco Unified Communications Manager System Guide*
- LDAP System Configuration, page 14-1
- LDAP Authentication Configuration, page 16-1
- Application Users and End Users, *Cisco Unified Communications Manager System Guide*
- Application User Configuration, page 113-1
- End User Configuration, page 114-1

CHAPTER 16

LDAP Authentication Configuration

In Cisco Unified Communications Manager, LDAP directory configuration takes place in the following windows:

- LDAP System
- LDAP Directory
- LDAP Authentication

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 window.

Use the following topics to configure LDAP authentication information:

- LDAP Authentication Configuration Settings, page 16-1
- Updating LDAP Authentication Information, page 16-4
- Related Topics, page 16-5

LDAP Authentication Configuration Settings

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 window.

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.

Table 16-1 describes the LDAP authentication configuration settings. For related procedures, see the "Related Topics" section on page 16-5.

Table 16-1 LDAP Authentication Configuration 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.
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.

Table 16-1 LDAP Authentication Configuration Settings (continued)

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 For When the 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 For When the 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.

Table 16-1 LDAP Authentication Configuration Settings (continued)

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.

Updating LDAP Authentication Information

Use the following procedure to update LDAP authentication information.

Before You Begin

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 authorization settings. Refer to the "Understanding the Directory" section on page 20-1 for more information about LDAP synchronization.

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

Procedure

Step 1 Choose **System > LDAP > LDAP Authentication**.

The LDAP Authentication window displays.

Step 2 Enter the appropriate configuration settings as described in Table 16-1.

Step 3 To save your changes, click **Save**.

Additional Information

See the "Related Topics" section on page 16-5.

Related Topics

- LDAP Authentication Configuration Settings, page 16-1
- Updating LDAP Authentication Information, page 16-4
- Understanding the Directory, *Cisco Unified Communications Manager System Guide*
- LDAP System Configuration, page 14-1
- LDAP Directory Configuration, page 15-1
- Application Users and End Users, *Cisco Unified Communications Manager System Guide*
- Application User Configuration, page 113-1
- End User Configuration, page 114-1

CHAPTER 17

Location Configuration

The following topics explain locations in more detail:

Location Configuration Settings

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, refer to the "Call Admission Control" chapter 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** 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 an MCS 7845H1 or higher server.
- Refer to 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.

Table 17-1 describes the location configuration settings. For related procedures, see the “Related Topics” section on page 17-7.

Table 17-1 Location Configuration Settings

Field	Description
Location Information	
Name	Enter the name of the new location that you are creating. Two default locations that cannot be modified exist: • 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. • Phantom—The Phantom location specifies unlimited audio bandwidth and unlimited video bandwidth. Specify this location to allow successful call admission control for calls across intercluster trunks that use either the H.323 protocol or SIP. **Note** Both Hub_None and Phantom locations do allow configuration of the associated RSVP policy setting(s).

Table 17-1 Location Configuration Settings (continued)

Field	Description
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 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** Each call comprises two call streams. To improve audio quality, lower the bandwidth setting, so fewer active calls are allowed on the link to this location.
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. Video calls can, however, take place within this location. • Unlimited bandwidth—Click the Unlimited radio button. • 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.
Locations RSVP Settings	
Location	This display-only field displays locations for which the interlocation 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.

Table 17-1 Location Configuration Settings (continued)

Field	Description
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.
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 the "Clusterwide Default RSVP Policy" section of 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.

Finding a Location

Because you might have several locations in your network, Cisco Unified Communications Manager Administration lets you locate specific locations on the basis of specific criteria. Use the following procedure to find locations.

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

Procedure

Step 1 Choose **System** > **Location**.

The Find and List Locations window displays.

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records

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

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

Step 3 Click **Find**.

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

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

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

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

The window displays the item that you choose.

Additional Information

See the "Related Topics" section on page 17-7.

Configuring a Location

This section describes how to add, copy, or update a location to the Cisco Unified Communications Manager database.

Before You Begin

Before configuring a location, you must configure the Cisco Unified Communications Managers that form the cluster. Before configuring a location, you must configure the Cisco Unified Communications Manager. For details, see the "Updating a Cisco Unified Communications Manager" section on page 3-6

Procedure

Step 1 Choose **System** > **Location**.

The Find and List Locations window displays.

Step 2 Perform one of the following tasks:

- To copy an existing location, locate the appropriate location as described in the "Finding a Location" section on page 17-4, click the **Copy** button next to the location that you want to copy, and continue with Step 3.
- To add a new location, click the **Add New** button and continue with Step 3.
- To update an existing location, locate the appropriate location as described in the "Finding a Location" section on page 17-4 and continue with Step 3.

Step 3 Enter the appropriate settings as described in Table 17-1.

Step 4 To save the location information in the database, click **Save**.

Next Steps

After adding a new location to the database, you can assign devices to that location; for example, see

- Gateway Configuration, page 90-1
- Cisco Unified IP Phone Configuration, page 91-1
- CTI Route Point Configuration, page 88-1

Additional Information

See the "Related Topics" section on page 17-7.

Deleting a Location

This section describes how to delete a location from the Cisco Unified Communications Manager database.

Before You Begin

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. For more information about dependency records, see the "Accessing Dependency Records" section on page A-2. 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.

Procedure

Step 1 Find the location by using the procedure in the "Finding a Location" section on page 17-4.

Step 2 From the list of matching records, choose the location that you want to delete.

Step 3 Click **Delete Selected**.

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

Additional Information

See the "Related Topics" section on page 17-7.

Resynchronizing a Location Bandwidth

This section describes how to resynchronize the bandwidth for a location. When calls are blocked from using the link for a location, bandwidth leakage may have occurred that may reduce the allotted bandwidth for the location. You can resynchronize the location bandwidth to the maximum amount that is assigned to this location without resetting the Cisco Unified Communications Manager server. For more information, refer to the "Bandwidth Calculations" section in the Call Admission Control chapter of the *Cisco Unified Communications Manager System Guide*.

Procedure

Step 1 Find the location by using the procedure in the "Finding a Location" section on page 17-4.

Step 2 From the list of matching records, choose the location that you want to resynchronize.

The Location Configuration window displays.

Step 3 To resynchronize the bandwidth for the chosen location, click **Resync Bandwidth**.

This following message displays: "If calls are using the bandwidth for this location when the bandwidth is resynchronized, the bandwidth might be oversubscribed until all calls that are using the bandwidth for this location disconnect."

Step 4 To continue, click **OK** or to cancel, click **Cancel**.

Additional Information

See the "Related Topics" section on page 17-7.

Related Topics

- Location Configuration, page 17-1
- Location Configuration Settings, page 17-1
- Finding a Location, page 17-4
- Configuring a Location, page 17-5

- Deleting a Location, page 17-6
- Resynchronizing a Location Bandwidth, page 17-7

CHAPTER 18

Physical Location Configuration

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.

Refer to Device Mobility in the *Cisco Unified Communications Manager Features and Services Guide* for more information on the device mobility feature.

CHAPTER 19

Survivable Remote Site Telephony Configuration

Use the following topics to add, update, copy, or delete a SRST reference:

- SRST Reference Configuration Settings, page 19-1
- Finding an SRST Reference, page 19-2
- Configuring an SRST Reference, page 19-4
- Deleting an SRST Reference, page 19-4
- Related Topics, page 19-5

SRST Reference Configuration Settings

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, refer to the "Survivable Remote Site Telephony References" section in the *Cisco Unified Communications Manager System Guide*.

Table 19-1 describes the SRST reference configuration settings. For related procedures, see the "Related Topics" section on page 19-5.

Table 19-1 SRST Reference Configuration 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.

Table 19-1 SRST Reference Configuration Settings (continued)

Field	Description
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.
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.

Finding an SRST Reference

Because you might have several SRST references in your network, Cisco Unified Communications Manager lets you locate specific SRST references based on specific criteria. Use the following procedure to locate SRST references that are defined by a particular user.

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

Procedure

Step 1 Choose **System** > **SRST.**

The Find and List SRST References 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.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 19-5.

Configuring an SRST Reference

The following procedure describes how to add, update or copy an SRST reference.

Procedure

Step 1 Choose **System** > **SRST**.

Step 2 Perform one of the following tasks:

- To add a new SRST reference, click the **Add New** button and continue with Step 3.
- To update an existing SRST reference, locate the appropriate SRST reference as described in the "Finding an SRST Reference" section on page 19-2 and continue with Step 3.
- To copy an existing SRST reference, locate the appropriate SRST reference as described in the "Finding an SRST Reference" section on page 19-2, click the **Copy** button next to the SRST reference that you want to copy, and continue with Step 3.

Step 3 Enter or update the appropriate settings as described in Table 19-1.

Step 4 Click **Save**.

Note If devices are associated with this SRST reference, a message displays to tell you that devices need to be reset for the update to take effect. Cisco Unified Communications Manager may drop calls in progress on an affected gateway may be dropped when the gateway is reset.

To reset the affected devices, click the **Reset Devices** button when the update is complete. If you do not want to reset the devices at this time, you can return to this item at any time and click the **Reset Devices** button to initiate the required device resets.

Additional Information

See the "Related Topics" section on page 19-5.

Deleting an SRST Reference

The following procedure describes how to delete an SRST reference.

Before You Begin

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. For more information about dependency records, see the "Accessing Dependency Records" section on page A-2. 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. Refer to the "Configuring a Device Pool" section on page 9-11.

- Delete the device pools that are using the SRST reference that you want to delete. See the "Deleting a Device Pool" section on page 9-13.

Procedure

Step 1 In the menu bar, choose **System** > **SRST**.

Step 2 Locate the SRST reference that you want to delete. See the "Finding an SRST Reference" section on page 19-2.

Step 3 Check the check box of the SRST reference that you want to delete and click **Delete Selected**.

A message displays, that tells you that you cannot undo this action.

Step 4 To delete the SRST reference, click **OK** or to cancel the deletion, click **Cancel**.

⚠ **Caution** Before initiating this action, 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.

Tip You can also delete an SRST reference by locating and displaying the SRST reference that you want to delete and clicking **Delete**.

Additional Information

See the "Related Topics" section on page 19-5.

Related Topics

- SRST Reference Configuration Settings, page 19-1
- Finding an SRST Reference, page 19-2
- Configuring an SRST Reference, page 19-4
- Deleting an SRST Reference, page 19-4
- Survivable Remote Site Telephony References, *Cisco Unified Communications Manager System Guide*

CHAPTER 20

MLPP Domain Configuration

Use the following topics to add, update, or delete MLPP domains:

- MLPP Domain Configuration Settings, page 20-1
- Finding an MLPP Domain, page 20-2
- Configuring an MLPP Domain, page 20-3
- Deleting an MLPP Domain, page 20-3
- Related Topics, page 20-4

MLPP Domain Configuration Settings

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.

Table 20-1 describes the MLPP domain configuration settings. For related procedures, see the "Related Topics" section on page 20-4.

Table 20-1 MLPP Domain Configuration 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 *Default*. 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.

Note You can add secure MLPP over SIP trunks by configuring a Resource Priority Namespace Network Domain and Resource Priority Namespace List. See Configuring a Resource Priority Namespace Network Domain, page 21-3 and Configuring a Resource Priority Namespace List, page 22-3.

Additional Information

See the "Related Topics" section on page 20-4.

Finding an MLPP Domain

Because you might have several MLPP domains in your network, Cisco Unified Communications Manager Administration lets you locate specific MLPP domains on the basis of specific criteria. Use the following procedure to locate MLPP domains.

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

Procedure

Step 1 Choose **System** > **MLPP> Domain** > **MLPP Domain.**

The Find and List MLPP Domains 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.

To filter or search records

- From the drop-down list box, select a search pattern.
- 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.

Additional Information

See the “Related Topics” section on page 20-4.

Configuring an MLPP Domain

This section describes how to configure an MLPP domain in the Cisco Unified Communications Manager database.

Procedure

Step 1 Choose **System** > **MLPP** > **Domain** > **MLPP Domain**.

The Find and List MLPP Domains window displays.

Step 2 Perform one of the following tasks:

- To copy an existing MLPP domain, locate the appropriate MLPP domain as described in the “Finding an MLPP Domain” section on page 20-2, click the **Copy** button next to the MLPP domain that you want to copy, and continue with Step 3.
- To add a new MLPP domain, click the **Add New** button, and continue with Step 3.
- To update an existing MLPP domain, locate the appropriate MLPP domain as described in the “Finding an MLPP Domain” section on page 20-2, and continue with Step 3.

Step 3 In the MLPP Domain Configuration window that displays, enter or edit the appropriate settings as described in Table 20-1.

Step 4 Click **Save** to save the new or updated MLPP domain in the database.

Additional Information

See the “Related Topics” section on page 20-4.

Deleting an MLPP Domain

This section describes how to delete an MLPP domain from the Cisco Unified Communications Manager database.

Before You Begin

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, refer to the "Accessing Dependency Records" section on page A-2. 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.

Procedure

Step 1 Find the MLPP domain by using the procedure in the "Finding an MLPP Domain" section on page 20-2.

Step 2 From the list of matching records, choose the MLPP domain that you want to delete.

Step 3 Click **Delete**.

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

Additional Information

See the "Related Topics" section on page 20-4.

Related Topics

- MLPP Domain Configuration Settings, page 20-1
- Finding an MLPP Domain, page 20-2
- Configuring an MLPP Domain, page 20-3
- Deleting an MLPP Domain, page 20-3
- Configuring a Resource Priority Namespace Network Domain, page 21-3
- Configuring a Resource Priority Namespace List, page 22-3
- Multilevel Precedence and Preemption, *Cisco Unified Communications Manager Features and Services Guide*

CHAPTER 21

Resource Priority Namespace Network Domain Configuration

Use the following topics to add, update, or delete Resource Priority Namespace Network Domains:

- Resource Priority Namespace Network Domain Configuration Settings, page 21-1
- Finding a Resource Priority Namespace Network Domain, page 21-2
- Configuring a Resource Priority Namespace Network Domain, page 21-3
- Deleting a Resource Priority Namespace Network Domain, page 21-4
- Related Topics, page 21-4

Resource Priority Namespace Network Domain Configuration Settings

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.

Table 21-1 describes the Resource Priority Namespace Network Domain configuration settings. For related procedures, see the "Related Topics" section on page 21-4.

Table 21-1 Resource Priority Namespace Network Domain Configuration 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.
Make this the Default Resource Priority Namespace Network Domain	Check the box if you want the domain name to be the default.

Additional Information

See the “Related Topics” section on page 21-4.

Finding a Resource Priority Namespace Network Domain

Because you might have several resource priority namespace network domains in your network, Cisco Unified Communications Manager Administration lets you locate specific Resource Priority Namespace Network Domains on the basis of specific criteria. Use the following procedure to locate Resource Priority Namespace Network Domains.

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

Procedure

Step 1 Choose **System** > **MLPP** > **Namespace** > **Resource Priority Namespace Network Domain.**

The Find and List Resource Priority Namespace Network Domain 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.

To filter or search records

- From the drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 21-4.

Configuring a Resource Priority Namespace Network Domain

This section describes how to configure a Resource Priority Namespace Network Domain in the Cisco Unified Communications Manager database.

Procedure

Step 1 Choose **System** > **MLPP** > **Namespace** > **Resource Priority Namespace Network Domain**.

The Find and List Resource Priority Namespace Network Domain window displays.

Step 2 Perform one of the following tasks:

- To copy an existing Resource Priority Namespace Network Domain, locate the appropriate Resource Priority Namespace Network Domain as described in the "Finding a Resource Priority Namespace Network Domain" section on page 21-2. Click the **Copy** button next to the Resource Priority Namespace Network Domain that you want and continue with Step 3.
- To add a new Resource Priority Namespace Network Domain, click the **Add New** button, and continue with Step 3.
- To update an existing Resource Priority Namespace Network Domain, locate the appropriate Resource Priority Namespace Network Domain as described in the "Finding a Resource Priority Namespace Network Domain" section on page 21-2 and continue with Step 3.

Step 3 In the Resource Priority Namespace Network Domain Configuration window that displays, enter or edit the appropriate settings as described in Table 21-1.

Step 4 Click **Save** to save the new or updated Resource Priority Namespace Network Domain in the database.

Additional Information

See the "Related Topics" section on page 21-4.

Deleting a Resource Priority Namespace Network Domain

This section describes how to delete a Resource Priority Namespace Network Domain from the Cisco Unified Communications Manager database.

Before You Begin

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, refer to the "Accessing Dependency Records" section on page A-2.

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.

Procedure

Step 1 Find the Resource Priority Namespace Network Domain by using the procedure in the "Finding a Resource Priority Namespace Network Domain" section on page 21-2.

Step 2 From the list of matching records, choose the Resource Priority Namespace Network Domain that you want to delete.

Step 3 Click **Delete**.

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

Additional Information

See the "Related Topics" section on page 21-4.

Related Topics

- Resource Priority Namespace Network Domain Configuration Settings, page 21-1
- Finding a Resource Priority Namespace Network Domain, page 21-2
- Configuring a Resource Priority Namespace Network Domain, page 21-3
- Deleting a Resource Priority Namespace Network Domain, page 21-4
- Finding a Resource Priority Namespace List, page 22-2
- Configuring a Resource Priority Namespace List, page 22-3
- Configuring SIP Profiles, page 101-10

- Configuring a Translation Pattern, page 60-10
- Multilevel Precedence and Preemption, *Cisco Unified Communications Manager Features and Services Guide*

CHAPTER 22

Resource Priority Namespace List Configuration

Use the following topics to add, update, or delete Resource Priority Namespace Lists:

Resource Priority Namespace List Configuration Settings

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.

Table 22-1 describes the Resource Priority Namespace List configuration settings. For related procedures, see the "Related Topics" section on page 22-4.

Table 22-1 Resource Priority Namespace List Configuration 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.
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.

Additional Information

See the "Related Topics" section on page 22-4.

Finding a Resource Priority Namespace List

Because you might have several Resource Priority Namespace Lists in your network, Cisco Unified Communications Manager Administration lets you locate specific Resource Priority Namespace Lists on the basis of specific criteria. Use the following procedure to locate MLPP domains.

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

Procedure

Step 1 Choose **System** > **MLPP** > **Namespace** > **Resource Priority Namespace List.**

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

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records

- From the drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 22-4.

Configuring a Resource Priority Namespace List

This section describes how to configure a Resource Priority Namespace List in the Cisco Unified Communications Manager database.

Procedure

Step 1 Choose **System** > **MLPP** > **Namespace** > **Resource Priority Namespace List**.

The Find and List Resource Priority Namespace List window displays.

Step 2 Perform one of the following tasks:

- To copy an existing Resource Priority Namespace List, locate the appropriate Resource Priority Namespace List as described in the "Finding a Resource Priority Namespace List" section on page 22-2, click the **Copy** button next to the Resource Priority Namespace List that you want to copy, and continue with Step 3.
- To add a new Resource Priority Namespace List, click the **Add New** button, and continue with Step 3.
- To update an existing Resource Priority Namespace List, locate the appropriate Resource Priority Namespace List as described in the "Finding a Resource Priority Namespace List" section on page 22-2, and continue with Step 3.

Step 3 In the Resource Priority Namespace List Configuration window that displays, enter or edit the appropriate settings as described in Table 22-1.

Step 4 Click **Save** to save the new or updated Resource Priority Namespace List in the database.

Additional Information

See the "Related Topics" section on page 22-4.

Deleting a Resource Priority Namespace List

This section describes how to delete a Resource Priority Namespace List from the Cisco Unified Communications Manager database.

Before You Begin

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. For more information about dependency records, refer to the "Accessing Dependency Records" section on page A-2. 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 Network Domain List that you want to delete.
- Delete the devices that are using the Resource Priority Namespace List that you want to delete.

Procedure

Step 1 Find the Resource Priority Namespace List by using the procedure in the "Finding a Resource Priority Namespace List" section on page 22-2.

Step 2 From the list of matching records, choose the Resource Priority Namespace List that you want to delete.

Step 3 Click **Delete**.

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

Additional Information

See the "Related Topics" section on page 22-4.

Related Topics

- Resource Priority Namespace List Configuration Settings, page 22-1
- Finding a Resource Priority Namespace List, page 22-2
- Configuring a Resource Priority Namespace List, page 22-3
- Deleting a Resource Priority Namespace List, page 22-3
- Configuring a Resource Priority Namespace Network Domain, page 21-3
- SIP Profile Configuration Settings, page 101-1

CHAPTER 23

Enterprise Parameters Configuration

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, refer to the "Device Defaults Configuration" section on page 94-1 and refer to the "System-Level Configuration Settings" section of the *Cisco Unified Communications Manager System Guide*.

You cannot add or delete enterprise parameters, but you can use the following procedures to update existing enterprise parameters or synchronize enterprise-parameter configuration changes with affected devices. Refer to the following sections:

- Updating Enterprise Parameters, page 23-1
- Synchronizing Enterprise Parameters With Affected Devices, page 23-2

Note 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.

Tip 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.

Updating Enterprise Parameters

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**.

Synchronizing Enterprise Parameters With Affected Devices

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

Procedure

Step 1 Choose **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 24

Enterprise Phone Configuration

In the Enterprise Phone Configuration window, you can configure parameters that will apply to all phones that support these parameters.

Configuring Enterprise Phone Parameters

To configure parameters in the Enterprise Phone Configuration window, follow these steps:

Procedure

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

Step 2 Update the parameter settings as desired.

Select the “Override Common Settings” box for each setting 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 window and the Device Configuration window for various devices. 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.

CHAPTER 25

Service Parameters Configuration

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 question mark button 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.

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

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

Use the following topics to configure or display service parameters:

- Configuring Service Parameters for a Service on a Server, page 25-1
- Displaying Parameters for a Service, page 25-3

Configuring Service Parameters for a Service on a Server

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 question mark button in the Service Parameter Configuration window.

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, refer to *Upgrading Cisco Unified Communications Manager*.
- 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, refer to 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.

Before You Begin

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

- Make sure that servers are configured. Refer to the "Server Configuration" section on page 2-1 for more information.
- 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, refer to the *Cisco Unified Serviceability Administration Guide* for more information.

Use the following procedure to configure the service parameters for a particular service on a particular server.

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 question mark button. 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.

Additional Information

See the “Related Topics” section on page 25-4.

Displaying Parameters for a Service

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.

Additional Information

See the "Related Topics" section on page 25-4.

Related Topics

- Displaying Parameters for a Service, page 25-3
- Configuring Service Parameters for a Service on a Server, page 25-1
- *Cisco Unified Serviceability Administration Guide*

CHAPTER 26

Phone Security Profile Configuration

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

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.

CHAPTER 27

SIP Trunk Security Profile Configuration

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

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.

CHAPTER 28

CUMA Server Security Profile Configuration

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, refer to 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.

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.

CHAPTER 29

Application Server Configuration

The following topics provide information about working with and configuring application servers in Cisco Unified Communications Manager Administration:

Application Server Configuration Settings

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 Presence, and Cisco Emergency Responder, and to synchronize Cisco Unified Communications Manager systems and applications, such as Cisco Web Dialer.

Table 29-1 describes the available settings in the Application Server window. For related procedures, see the "Related Topics" section on page 29-5.

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*.

Table 29-1 Application Server Configuration 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 servers, choose Cisco Unified Presence).

Table 29-1 Application Server Configuration Settings (continued)

Field	Description
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.

Finding an Application Server

The following procedure describes how to find and list application servers.

Procedure

Step 1 Choose **System** > **Application Server**.

The Find and List Application Servers window displays.

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records

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

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

Step 3 Click **Find**.

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

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

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

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

The window displays the item that you choose.

Additional Information

See the "Related Topics" section on page 29-5.

Configuring Application Servers

The following procedure describes how to configure application servers in Cisco Unified Communications Manager Administration.

Before You Begin

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.

Procedure

Step 1 Choose **System** > **Application Server**.

The Find and List Application Servers window displays.

Step 2 Perform one of the followings tasks:

- To copy an existing application server, locate the server that you want to copy as described in Finding an Application Server, page 29-2; click the server name. The Application Server Configuration window displays. Click the **Copy** button and continue with Step 4.
- To add a new application server, click the **Add New** button and continue with Step 3.
- To update an existing application server, locate the appropriate server as described in Finding an Application Server, page 29-2, and continue with Step 4.

Step 3 From the Application Server Type drop-down list box, choose the appropriate server type and click **Next**. After you choose an application server type, you cannot modify it.

Step 4 Enter the appropriate settings as described in Table 29-1.

Step 5 Click **Save**.

Additional Information

See the "Related Topics" section on page 29-5.

Deleting an Application Server

To delete an application server by using Cisco Unified Communications Manager Administration, perform the following procedure.

Procedure

Step 1 Choose **System** > **Application Server**.

The Find and List Application Servers window displays.

Step 2 To locate a specific application server, enter search criteria and click **Find**.

A list of application servers that match the search criteria displays.

Step 3 Perform one of the following actions:

- Check the check boxes next to the application servers that you want to delete and click **Delete Selected**.
- Delete all the application servers in the window by clicking **Select All** and then **Delete Selected**.
- Choose the name of the application server that you want to delete from the list to display its current settings and click **Delete**.

A confirmation dialog displays.

Step 4 Click **OK**.

Additional Information

See the "Related Topics" section on page 29-5.

Related Topics

- Application Server Configuration Settings, page 29-1
- Finding an Application Server, page 29-2
- Configuring Application Servers, page 29-3
- Deleting an Application Server, page 29-4
- Cisco Unity Messaging Integration, *Cisco Unified Communications Manager System Guide*
- Application User Configuration, page 113-1

CHAPTER 30

License Unit Report

This chapter contains information on the following topics:

- Generating a License Unit Report, page 30-1
- Related Topics, page 30-2

Generating a License Unit Report

Use the license unit report to display the total license capacity and the number of licenses in use. This tool generates a report that lists the total number of available licenses. The license unit report also displays the software license version that is installed on the Cisco Unified Communications Manager server.

Note For more information on requesting licenses, refer to the *Cisco Unified Communications Manager System Guide*.

A unit license refers to a fixed number of device license units that correspond to each phone type. For example, Cisco Unified IP Wireless 7920 requires four device license units, and a Cisco Unified IP Phone 7970 requires five device license units. If you are provisioning four 7920 phones and four 7970 phones, you require 36 phone license units.

The number of licensed units in the license file corresponds to the number of unit licenses for all the phone types that are purchased.

The License Unit Report window displays the status of a license file. For example, the Status column for each license type may display Demo, Missing, or Uploaded.

Note To determine the number of license unit that are required for each device, choose **System** > **Licensing** > **License Unit Calculator**. This window lists the number of license units that are required for each type of device.

Use the following procedure to generate a report for the number of licenses that are available.

Procedure

Step 1 Choose **System** > **Licensing** > **License Unit Report**.

Step 2 The License Unit Report window displays. This window displays the number of phone licenses, number of node licenses, and software license versions. Phone and node licenses that are available display by

- Units Authorized
- Units Used
- Units Remaining

The software license version displays the

- License Server Name
- Cisco Unified Communications Manager Software Version

Additional Information

See the "Related Topics" section on page 30-2.

Related Topics

- License Unit Report, page 30-1
- Generating a License Unit Report, page 30-1
- License Unit Calculator, page 31-1
- License File Upload, page 32-1

CHAPTER 31

License Unit Calculator

This chapter contains information on the following topics:

- Calculating License Units, page 31-1
- Related Topics, page 31-2

Calculating License Units

Use this window to calculate the number of phone unit licenses that are required for a specific configuration of a type of phones and number of phones of each type. A device license unit refers to a fixed number of license units that corresponds to each phone type. Cisco Unified IP Wireless Phone 7920 requires four license units, and a Cisco Unified IP Phone 7970 requires five units. If you are adding four 7920 phones and four 7970 phones, you require 36 phone license units.

For more information about the different types of device license units, see Licensing in the *Cisco Unified Communications Manager System Guide*.

Use the following procedure to calculate the number of phone licenses that are required when the number of phone types and the total number of phones per phone type are entered.

Procedure

Step 1 Choose **System > Licensing> License Unit Calculator**.

The License Unit Calculator window displays. The number of license units that are consumed per device displays, corresponding to the node or device.

Step 2 In the Number of Devices column, update the number of needed devices, corresponding to each node or phone.

Step 3 Click **Calculate**.

The total number of Cisco Unified Communications Manager node license units and phone license units displays.

Additional Information

See the "Related Topics" section on page 31-2.

Related Topics

- Calculating License Units, page 31-1
- License Unit Report, page 30-1
- License File Upload, page 32-1
- Licensing, *Cisco Unified Communications Manager System Guide*
- *Cisco Unified Serviceability Administration Guide*

CHAPTER 32

License File Upload

License files contain the information that is needed to enforce licenses for Cisco Unified Communications Manager. This chapter contains the following topics on uploading license files:

- Starting the License Manager Service, page 32-1
- Obtaining a License File, page 32-2
- Uploading a License File, page 32-5
- Deleting a License File Name, page 32-7
- Related Topics, page 32-7

Starting the License Manager Service

The Cisco Unified Communications Manager server where the license file is loaded assumes the functionality of a license manager. (The license file gets loaded on the first node only.) For information on license files, refer to the "Obtaining a License File" section on page 32-2.

The license manager serves as the logical component that keeps track of the licenses that get purchased and used. It refers to the processes that control the checkin and checkout of the licenses. It keeps track of the number of license units that are required for each phone and application type. The license manager has responsibility for issuing and reclaiming licenses and for detecting whether an overdraft of licenses occurs.

Start the license manager service by using Cisco Unified Serviceability. This section describes the procedures to start, stop, or restart the service.

Note Because license manager is a network service, it automatically starts and runs after the Cisco Unified Communications Manager installation.

Procedure

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

The Control Center–Network Services window displays.

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

Step 3 Click the radio button for **Cisco License Manager**.

Step 4 If you want to start the License Manager service, click **Start**.

Step 5 If you want to stop the License Manager service, click **Stop**.

Step 6 If you want to restart the License Manager, click **Restart**.

Additional Information

See the Related Topics, page 32-7.

Obtaining a License File

Licensing helps manage Cisco Unified Communications Manager licenses and enforces the licenses for Cisco Unified Communications Manager applications and the number of devices. This section provides information on obtaining licenses for new Cisco Unified Communications Manager systems and/or device installations as well as for Cisco Unified Communications Manager nodes that have been upgraded from various releases.

Note You do not need to obtain new licenses if you are upgrading within a software release train, such as Cisco Unified Communications Manager 6.0(1) to 6.1(1).

To obtain a license, see the section that applies to your situation:

- If you are installing new Cisco Unified Communications Manager or devices that require additional device license units, see the "New Cisco Unified Communications Manager Nodes and Devices" section on page 32-2.
- If you are upgrading from Cisco Unified CallManager 4.x, obtain a software feature license as described in "Obtaining a Software Feature License" section on page 32-3 and then upgrade the product licenses as described in the "Upgrading Product Licenses" section on page 32-4.
- If you are upgrading from supported versions of Cisco Unified Communications Manager 5.x or 6.x, see the "Obtaining a Software Feature License" section on page 32-3.

New Cisco Unified Communications Manager Nodes and Devices

Use the following procedure to obtain a node license file for new Cisco Unified Communications Manager nodes (servers) and to obtain device licenses for new devices that require additional device license units.

Each node in your cluster requires one node license unit. Each device type requires a fixed number of licenses units, depending on the type. For example, Cisco Unified IP Phone 7920 requires four license units, and Cisco Unified IP Phone 7970 requires five units. If you want licenses for four Cisco Unified IP Phones 7920 and four Cisco Unified IP Phones 7970 phones, you require 36 phone license units.

Cisco Unified Communications Manager contains a starter licenses that you can use to begin new installations of Cisco Unified Communications Manager. The system overwrites the starter license when you obtain and upload your permanent licenses. For more information on starter licenses, see the "Starter Licenses" section in the *Cisco Unified Communications Manager System Guide*.

You use the Product Authorization Key (PAK) that came with your product to obtain the necessary permanent licenses, as described in the following procedure.

Procedure

Step 1 Enter the Product Authorization Key (PAK) that you received with your Cisco Unified Communications Manager or phone order in the License Registration web tool at http://www.cisco.com/go/license.

Step 2 Click **Submit**.

Step 3 Follow the system prompts. You must enter the MAC address of the Ethernet 0 NIC of the first node of the Cisco Unified Communications Manager cluster. You must enter a valid e-mail address as well as the number of nodes and device license units for which you want licenses.

Note For information on calculating the number of device license units that are required for the devices in your system, refer to the "Calculating License Units" section on page 31-1.

The system sends the license file(s) to you via e-mail by using the E-mail ID that you provided. The format of a license file specifies CCM<timestamp>.lic. If you retain the .lic extension, you can rename the license file. You cannot use the license if you edit the contents of the file in any way.

Note One license file may apply to more than one node in your cluster. For information on how to interpret the license file, see the "Uploading a License File" section on page 32-5.

Step 4 You must upload the license file to the server with the matching MAC address that you provided in Step 3. See the "Uploading a License File" section on page 32-5. This server then takes on the functionality of the license manager.

Note You can use the licenses that are specified in the license file only within the cluster on which the license file is uploaded.

Additional Information

See the "Related Topics" section on page 32-7.

Obtaining a Software Feature License

A software feature license activates features on your system for the specified license version. To use previous device license versions with this version of Cisco Unified Communications Manager, make sure that you obtain the software feature license for the Cisco Unified Communications Manager version that is running on your system.

Use this procedure to obtain a software feature license:

Procedure

Step 1 Navigate to the License Registration web tool at http://www.cisco.com/go/license.

Step 2 Enter the Product Authorization Key (PAK) that you received with your Cisco Unified Communications Manager upgrade.

Step 3 Click **Submit**.

Step 4 Follow the system prompts. You must enter the MAC address of the Ethernet 0 NIC of the first node of the Cisco Unified Communications Manager cluster. You must also enter a valid e-mail address.

The system sends the license file to you via e-mail by using the e-mail address that you provided. To view the contents of a software feature license, refer to "License File Contents" in the *Cisco Unified Communications Manager System Guide*.

Step 5 You must upload the software license file to the server with the matching MAC address that you provided in Step 4. See the "Uploading a License File" section on page 32-5.

Step 6 If you are upgrading from Cisco Unified CallManager 4.x, perform the procedure that is described in the "Upgrading Product Licenses" section on page 32-4.

Additional Information

See the Related Topics, page 32-7.

Upgrading Product Licenses

When you upgrade from supported Cisco Unified CallManager 4.x releases, the system calculates the licenses that are required for existing devices and existing nodes and generates an intermediate file (XML file) that contains this information. You use this file to obtain license files that you can import into Cisco Unified Communications Manager Administration. (Refer to Procedure 2.) Alternately, you can use the license file that Data Migration Assistant (DMA) generates. (Refer to Procedure 1.)

You receive these licenses free of cost because you are already using these phones for a Cisco Unified CallManager 4.x release.

Use either Procedure 1 or Procedure 2 to obtain licenses for Cisco Unified Communications Manager when you upgrade from supported 4.x releases.

Procedure 1

Step 1 When you use Data Migration Assistant to migrate your data, choose the **Export > Storage Location > Destination Option for License File** tool to specify a local directory destination for the license file licupgrade.lic

Note Do not specify a mapped network directory for the Local Directory. If you do, be aware that DMA may not be able to create the destination folder.

Step 2 Run DMA according to instructions in the *Data Migration Assistant User Guide*.

Step 3 Upgrade the Cisco Unified Communications Manager servers according to instructions in the document *Upgrading Cisco Unified Communications Manager Release 7.1(2) from Cisco Unified Communications Manager 4.x Releases.*

Step 4 Upload the license file to the server with the matching MAC address of the Ethernet 0 NIC of the first node of the Cisco Unified Communications Manager cluster.

Step 5 If your system requires additional device license units, you can obtain licenses for new devices that you are adding to the upgraded system. For detailed instructions, see the "New Cisco Unified Communications Manager Nodes and Devices" section on page 32-2.

Procedure 2

Step 1 After you complete the Cisco Unified Communications Manager Administration upgrade process, as described in *Upgrading Cisco Unified Communications Manager*, navigate to Cisco Unified Communications Manager Administration and choose **System > Licensing > License File Upload**.

The License File Upload window displays.

Step 2 Choose the licugrade_<upgrade version>.lic file from the Existing Files drop-down list and click **View File**. The window refreshes and displays the license information for existing devices and nodes. Copy this information. To copy the contents on this window, you can use **Ctrl-A** (Select All) and **Ctrl-C** (Copy).

Step 3 Navigate to the License Registration web tool at https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet?FormId=806.

Step 4 Enter the MAC address of the Ethernet 0 NIC of the first node of the Cisco Unified Communications Manager in the cluster.

Step 5 In the text box that is provided, paste the license file contents that you copied in Step 2 by using the appropriate keyboard shortcuts, such as **Ctrl-V**.

Step 6 Enter a valid e-mail address and click **Continue**. A license file generates.

The system sends the license file to you through e-mail by using the e-mail address that you provided.

Step 7 You must upload the license file to the server with the matching MAC address that you provided in Step 4. See the "Uploading a License File" section on page 32-5.

Step 8 You can obtain licenses for new devices that you are adding to the upgraded system, if your system requires additional device license units. For detailed instructions, see the "New Cisco Unified Communications Manager Nodes and Devices" section on page 32-2.

Additional Information

See the Related Topics, page 32-7.

Uploading a License File

Use the following procedure to upload a license file to the Cisco Unified Communications Manager server with the matching MAC address that is provided when a license file is requested. For information about obtaining a license file, see the "Obtaining a License File" section on page 32-2. The Cisco Unified Communications Manager server where the license file is loaded takes on the functionality of the license manager.

The License File Upload window may display a message that uploading the license file removes the starter (demo) licenses for the feature.

After you upgrade to Cisco Unified Communications Manager 7.1 from a compatible Cisco Unified CM 5.X or 6.X release, the Cisco CallManager service does not automatically run, even though Cisco Unified Serviceability shows that the Cisco CallManager service is activated. Immediately after you complete the upgrade to Cisco Unified Communications Manager 7.1, upload the software feature license that is required for Cisco Unified Communications Manager 7.1 in Cisco Unified Communications Manager Administration and restart the Cisco CallManager service in Cisco Unified Serviceability. Until you perform these tasks, devices fail to register with Cisco Unified Communications Manager 7.1.

Note Upload the license file only on the first node of Cisco Unified Communications Manager cluster.

Procedure

Step 1 Choose **System** > **Licensing** > **License File Upload**.

The License File Upload window displays.

Step 2 The Existing License Files drop-down list box displays the license files that are already uploaded to the server.

Note To view the file content of any existing files, choose the file from the drop-down list box and click **View File**.

Step 3 To choose a new license file to upload, click **Upload License File**.

The Upload File pop-up window displays.

Step 4 To upload to the server, click **Browse** to choose a license file.

Note The format of the license file that you receive specifies CCM<timestamp>.lic. If you retain the .lic extension, you can rename the license file. You cannot use the license if you edit the contents of the file in any way.

Step 5 Click **Upload**.

After the upload process completes, the Upload Result file displays.

Step 6 Click **Close**.

Step 7 In the License File Upload window, the status of the uploaded file displays. In Cisco Unified Serviceability, restart the Cisco CallManager service.

Note The system uploads the license file into the database only if the version that is specified in the license file is greater than or equal to the Cisco Unified Communications Manager version that is running in the cluster. If the version check fails, an alarm gets generated, and you should get a new license file with the correct version. The system bases the version check only on major releases.

Additional Information

See the “Related Topics” section on page 32-7.

Deleting a License File Name

You cannot delete a license file name through Cisco Unified Communications Manager Administration. For information on how to delete a license file name, refer to the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

Related Topics

- Starting the License Manager Service, page 32-1
- Obtaining a License File, page 32-2
- Upgrading Product Licenses, page 32-4
- Uploading a License File, page 32-5
- Deleting a License File Name, page 32-7
- Calculating License Units, page 31-1
- Generating a License Unit Report, page 30-1
- Licensing, *Cisco Unified Communications Manager System Guide*
- *Command Line Interface Reference Guide for Cisco Unified Solutions*

CHAPTER 33

License Capabilities Assignment Configuration

Use the following topics to add or update a license capabilities assignment:

License Capabilities Assignment Configuration Settings

Capabilities Assignment allows system administrators to enable the Cisco Unified Presence (CUP) and Cisco Unified Personal Communicator (CUPC) capabilities for users. You must ensure that licenses for CUP and CUPC are available.

Make license capabilities assignments to existing users. Before you begin, ensure that users exist on your system by choosing **User Management** > **End User** and clicking **Find**.

Before you begin configuring the capabilities assignments for users, determine how many CUP (servers and clients) and CUPC licenses are required for your system by choosing **Licensing** > **License Unit Calculator**. Acquire the required licenses by using **Licensing** > **License File Upload**. Verify the total licenses by using **Licensing** > **License Unit Report**.

Table 33-1 describes the license capabilities assignment configuration settings. For related procedures, see the "Related Topics" section on page 33-4.

Table 33-1 License Capabilities Assignment Configuration Settings

Field	Description
User Information	
User ID	Displays the name of the user for which you are enabling capabilities assignment.

Table 33-1 License Capabilities Assignment Configuration Settings (continued)

Field	Description
Capabilities Assignment Information	
Enable CUP (Cisco Unified Presence)	To enable CUP for this user, check the Enable CUP (Cisco Unified Presence) check box.
Enable CUPC (Cisco Unified Personal Communicator)	To enable CUPC for this user, check the Enable UPC (Cisco Unified Personal Communicator) check box. You can enable both CUP and CUPC; however, if you want CUPC, you must also enable CUP.

Finding a License Capabilities Assignment

Because you might have several license capabilities assignments for users in your network, Cisco Unified Communications Manager Administration lets you locate specific capabilities assignments on the basis of specific criteria. Use the following procedure to find locations.

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

Procedure

Step 1 Choose **System** > **Licensing** > **Capabilities Assignment**.

The Find and List Capabilities Assignment window displays.

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records

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

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

Step 3 Click **Find**.

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

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

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

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

The window displays the item that you choose.

Additional Information

See the "Related Topics" section on page 33-4.

Configuring the Capabilities Assignments for One User

This section describes how to add or update a capabilities assignment for a user to the Cisco Unified Communications Manager database.

Before You Begin

Before configuring a capabilities assignment, you must obtain licenses from Cisco Systems by using the License File Upload under the System menu.

Procedure

Step 1 Choose **System** > **Licensing > Capabilities Assignment**.

The Find and List Capabilities Assignment window displays.

Step 2 To add a new capabilities assignment or update an existing capabilities assignment, locate the appropriate capabilities assignment as described in the "Finding a License Capabilities Assignment" section on page 33-2 and continue with Step 3.

The Capabilities Assignments Configuration window displays.

Step 3 Check the appropriate check box as described in Table 33-1.

Step 4 To save the capabilities assignment information in the database, click **Save**.

Additional Information

See the "Related Topics" section on page 33-4.

Configuring the Capabilities Assignments for Multiple Users

This section describes how to add or update capabilities assignments for multiple users to the Cisco Unified Communications Manager database.

Before You Begin

Before configuring a capabilities assignment, you must obtain licenses from Cisco Systems by using the License File Upload under the System menu.

Note You can assign licenses for up to 250 users when you are using the bulk assignment capability.

Procedure

Step 1 Choose **System** > **Licensing** > **Capabilities Assignment**.

The Find and List Capabilities Assignment window displays.

Step 2 To add a new capabilities assignment or update an existing capabilities assignment, locate the appropriate capabilities assignment as described in the "Finding a License Capabilities Assignment" section on page 33-2 and continue with Step 3.

Step 3 To enable a new capabilities assignment or to update an existing capabilities assignment for multiple users, check the check boxes next to the users or click the **Select All** button.

Step 4 Click the **Bulk Assignment** button.

The Capabilities Assignments Configuration window displays.

Step 5 Check the appropriate check box as described in Table 33-1.

Step 6 To save the capabilities assignment information in the database, click **Save**.

Additional Information

See the "Related Topics" section on page 33-4.

Related Topics

- License Capabilities Assignment Configuration Settings, page 33-1
- License Capabilities Assignment Configuration, page 33-1
- Finding a License Capabilities Assignment, page 33-2
- Configuring the Capabilities Assignments for One User, page 33-3
- Configuring the Capabilities Assignments for Multiple Users, page 33-3
- *Cisco Unified Communications Manager Bulk Administration Guide*

CHAPTER 34

Autoregistration Configuration

This section covers the following topics on autoregistration configuration:

Autoregistration Configuration Settings

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.

Table 34-1 describes the autoregistration configuration settings. For more information about related procedures, see the "Related Topics" section on page 34-6.

Table 34-1 Autoregistration Configuration Settings

Field Name	Description
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.

Table 34-1 Autoregistration Configuration Settings (continued)

Field Name	Description
Ending Directory Number	Enter the last 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.
Partition	Choose the partition to which autoregistered directory numbers belong. If you are not using partitions, choose <None>. You must choose a valid directory number range for autoregistration before you can choose a partition and external phone number mask. The partition field resets if you disable autoregistration. If a large number of partitions exist, the **Find** button displays next to the drop-down list box. Click the **Find** button to display the Find and List Partitions window. In the Find partition where field, choose search criteria and enter a partial partition name. In the list of partitions that displays, click the desired partition name and click **OK**.
External Phone Number Mask	Specify the mask that is used to format caller ID information for external (outbound) calls that are made from the autoregistered devices. The mask can contain up to 50 characters. Enter the literal digits that you want to appear in the caller ID information and use Xs to represent the directory number of the autoregistered device. For example, if you specify a mask of 972813XXXX and enable the Use External Phone Number Mask option on the route pattern that is used to make the external call, an external call from extension 1234 displays a caller ID number of 9728131234. If you specify a mask of all literal digits (such as 9728135000) to represent a main attendant number, that literal number becomes the caller ID that displays for an external call from any autoregistered device.
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 partition and external phone mask information fields also reset when you disable autoregistration.

Enabling 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 Communications Manager**.

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 34-1.

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

Step 7 Choose **System** > **Cisco Unified Communications Manager Group**.

The Find and List Cisco Unified Communications Manager Groups window displays. Click **Find**.

Step 8 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 Step 4. The Cisco Unified Communications Managers get selected in the order in which they are listed in the Cisco Unified Communications Manager group.

Step 9 If you made any changes to the group configuration, click **Save** to save the changes in the database.

Step 10 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 11 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 12 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 13 Install the devices that you want to autoregister.

Step 14 Reconfigure the autoregistered devices and assign them to their permanent device pools.

Step 15 In the Enterprise Parameters Configuration window, set the Auto Registration Phone Protocol setting to SIP or SCCP, whichever is needed.

Step 16 If you autoregister more phones with a different protocol, repeat Step 1 through Step 15.

Additional Information

See the "Related Topics" section on page 34-6.

Disabling Autoregistration

This section describes how to disable autoregistration.

Procedure

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

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 through Step 4 for each Cisco Unified Communications Manager where you want to disable autoregistration.

Additional Information

See the "Related Topics" section on page 34-6.

Reusing 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**.

Additional Information

See the "Related Topics" section on page 34-6.

Related Topics

- Autoregistration Configuration Settings, page 34-1
- Enabling Autoregistration, page 34-3
- Disabling Autoregistration, page 34-4
- Reusing Autoregistration Numbers, page 34-5

CHAPTER 35

Geolocation Configuration

The **System** > **Geolocation Configuration** menu option in Cisco Unified Communications Manager Administration allows configuration of 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, including configuration details, refer to "Introducing Geolocations" and "Geolocation Configuration" in the "Geolocations and Location Conveyance" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

For more information on how the logical partitioning feature uses geolocations, refer to the "Logical Partitioning" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

CHAPTER 36

Geolocation Filter Configuration

The **System > Geolocation Filter** menu option in Cisco Unified Communications Manager Administration allows configuration of geographic location filters for use with geographic locations and logical partition policies to provision logical partitioning.

For an explanation of geolocation filters, including configuration details, refer to "Introducing Geolocation Filters" and "Geolocation Filter Configuration" in the "Geolocations and Location Conveyance" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

For more information on how the logical partitioning feature uses geolocation filters, refer to the "Logical Partitioning" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

PART 3

Call Routing Configuration

CHAPTER 37

Automated Alternate Routing Group Configuration

Use the following topics to find, add, update, or delete AAR groups:

AAR Group Configuration Settings

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*.)

Refer to the "Understanding Route Plans" chapter of the *Cisco Unified Communications Manager System Guide* for more information about automated alternate routing groups.

Table 37-1 describes the AAR group configuration settings. For related procedures, see the "Related Topics" section on page 37-5.

Table 37-1 AAR Group Configuration 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 (_).
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.
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.

Additional Information

See the "Related Topics" section on page 37-5.

Finding an AAR Group

Because you might have several automated alternate routing (AAR) groups in your network, Cisco Unified Communications Manager lets you locate specific AAR groups based on specific criteria. Use the following procedure to locate AAR groups.

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

Procedure

Step 1 Choose **Call Routing** > **AAR Group**.

The Find and List Automated Alternate Routing Groups window displays.

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records:

- From the first drop-down list box, select a search parameter.
- Specify the appropriate search text, if applicable.

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

Step 3 Click **Find**.

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

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

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

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

The window displays the item that you choose.

Additional Information

See the "Related Topics" section on page 37-5.

Configuring an AAR Group

The following procedure describes how to configure an AAR group.

Procedure

Step 1 Choose **Call Routing** > **AAR Group**.

The Find and List Automated Alternate Routing Groups window displays.

Step 2 Perform one of the followings tasks:

- To add a new AAR group, click the **Add New** button, and continue with Step 3.
- To update an existing AAR group, locate the appropriate AAR group as described in the "Finding an AAR Group" section on page 37-3, and continue with Step 3.

Step 3 In the AAR Group Configuration window that displays, enter a name in the AAR Group Name field. The name can contain alphanumeric characters, any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure each AAR group name is unique. The current size for this field is 20 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.

Step 4 Click **Save**.

Step 5 Choose the appropriate settings as described in Table 37-1.

Step 6 To configure this AAR group, click **Save**.

Additional Information

See the "Related Topics" section on page 37-5.

Deleting an AAR Group

The following procedure describes how to delete an AAR group.

Before You Begin

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. For more information about dependency records, see the "Accessing Dependency Records" section in the *Cisco Unified Communications Manager Administration Guide*. You must remove the AAR group from all devices to which it belongs before deleting the AAR group.

Procedure

Step 1 Choose **Call Routing** > **AAR Group** in the menu bar.

Step 2 Locate the AAR group that you want to delete. See the "Finding an AAR Group" section on page 37-3.

Step 3 Check the check box next to the AAR group that you want to delete and click **Delete Selected**.

A dialog box displays to warn you that you cannot undo deletion of AAR groups.

Step 4 To delete the group, click **OK**, or to cancel the action, click **Cancel**. If you click **OK**, the Cisco Unified Communications Manager removes the AAR group from the AAR group list.

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

Additional Information

See the "Related Topics" section on page 37-5.

Related Topics

- AAR Group Configuration Settings, page 37-1
- Finding an AAR Group, page 37-3
- Configuring an AAR Group, page 37-4
- Deleting an AAR Group, page 37-4
- Automated Alternate Routing, *Cisco Unified Communications Manager System Guide*

CHAPTER 38

Application Dial Rules Configuration

The following sections describe dial rules configuration:

Application Dial Rule Configuration Settings

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.

Table 38-1 describes the available settings in the Application Dial Rule Configuration window. For more information about related procedures, see the "Related Topics" section on page 38-5.

Table 38-1 Application Dial Rule Configuration Settings

Field	Description
Name	Enter a name in the Name field. The name can contain up to 20 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure each application dial rule name is unique.
Description	Enter a description of the application dial rule in the Description field or leave blank.

Table 38-1 Application Dial Rule Configuration Settings (continued)

Field	Description
Number Begins With	Enter the initial digits of the directory numbers to which you want to apply this application dial rule. Valid values include numeric digits (0 through 9), plus (+), asterisk (*), and pound (#).
Number of Digits	Enter the length of the dialed numbers to which you want to apply this application dial rule. Enter a number of digits between 1 and 100 or the characters +, *, and #.
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. Enter a number of digits between 0 and 100.
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 up to 100), plus (+), asterisk (*), and pound (#).
Application Dial Rule Priority	Choose the dial rule priority as top, bottom, or middle. **Tip** This field displays when you enter the Prefix With Pattern information.

Additional Information

See the "Related Topics" section on page 38-5.

Finding a Dial Rule

Because you might have several dial rules in your network, Cisco Unified Communications Manager lets you locate specific dial rules based on specific criteria. Use the following procedure to locate dial rules.

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

Procedure

Step 1 Choose **Call Routing > Dial Rules > Application Dial Rules**.

The Find and List Application Dial Rules window displays.

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records:

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

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

Step 3 Click **Find**.

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

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

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

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

The window displays the item that you choose.

Additional Information

See the "Related Topics" section on page 38-5.

Configuring Dial Rules

Perform the following procedure to add a new dial rule or update an existing dial rule. See Application Dial Rules Configuration Error Checking in the *Cisco Unified Communications Manager System Guide* for dial rule design and error checking.

Procedure

Step 1 In the menu bar, choose **Call Routing** > **Dial Rules** > **Application Dial Rules**.

The Find and List Application Dial Rules window displays.

Step 2 Perform one of the followings tasks:

- To add a new dial rule, click the **Add New** button and continue with Step 3.
- To update an existing dial rule, locate the appropriate dial rule as described in "Finding a Dial Rule" section on page 38-2, and continue with Step 3.

Step 3 Enter the appropriate dial rule information settings as found in Table 38-1.

Step 4 Click the **Save** button.

Note If more than one dial rule exists, you can change the priority of the dial rules. See the "Reprioritizing a Dial Rule" section on page 38-4.

Additional Information

See the "Related Topics" section on page 38-5.

Deleting a Dial Rule

Perform the following procedure to delete a dial rule.

Procedure

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

Step 2 Locate the application dial rule that you want to delete. See the "Finding a Dial Rule" section on page 38-2.

Step 3 Check the check box next to the application dial rule that you want to delete and click **Delete Selected**.

A dialog box appears to warn you that you cannot undo deletion of application dial rules.

Step 4 To delete the group, click **OK**, or to cancel the action, click **Cancel**. If you click **OK**, the Cisco Unified Communications Manager removes the application dial rule from the application dial rules list.

Note You can delete multiple dial rules from the Find and List Application Dial Rules window by checking the check boxes next to the appropriate dial rules and clicking **Delete Selected**. You can delete all the AAR groups in the window by clicking **Select All** and then clicking **Delete Selected**.

Additional Information

See the "Related Topics" section on page 38-5.

Reprioritizing a 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**.

Additional Information

See the "Related Topics" section on page 38-5.

Related Topics

- Application Dial Rule Configuration Settings, page 38-1
- Finding a Dial Rule, page 38-2
- Configuring Dial Rules, page 38-3
- Deleting a Dial Rule, page 38-4
- Reprioritizing a Dial Rule, page 38-4

CHAPTER 39

Directory Lookup Dial Rules Configuration

This section contains the following topics:

Directory Lookup Dial Rule Configuration Settings

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.

Table 39-1 describes the available settings in the Phone Configuration window. For more information about related procedures, see the "Related Topics" section on page 39-4.

Table 39-1 Directory Lookup Dial Rule Configuration 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 (_).
Description	Enter a description of the directory lookup dial rule in the Description field or leave blank.
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 (#).

Table 39-1 Directory Lookup Dial Rule Configuration Settings (continued)

Field	Description
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 0 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 (#).

Finding a Directory Lookup Dial Rule

Use the following procedure to locate directory lookup dial rules.

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

Procedure

Step 1 Choose **Call Routing** > **Dial Rules** > **Directory Lookup Dial Rules**.

The Directory Lookup Dial Rule Find and List window displays.

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records:

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

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

Step 3 Click **Find**.

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

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

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

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

The window displays the item that you choose.

Additional Information

See the "Related Topics" section on page 39-4.

Configuring Directory Lookup Dial Rules

Perform the following procedure to add and update a directory lookup dial rule.

Procedure

Step 1 Choose **Call Routing** > **Dial Rules** > **Directory Lookup Dial Rules**.

The Directory Lookup Dial Rule Find and List window displays.

Step 2 Perform one of the following tasks:

- To add a new directory lookup dial rule, click **Add New**.
- To edit an existing directory lookup dial rule, display the appropriate dial as described in the "Finding a Directory Lookup Dial Rule" section on page 39-2.

The Directory Lookup Dial Rule Configuration window displays.

Step 3 Enter the appropriate settings as described in Table 39-1.

Step 4 Click **Save**.

Additional Information

See the "Related Topics" section on page 39-4.

Deleting a Directory Lookup Dial Rule

Perform the following procedure to delete a directory lookup dial rule.

Procedure

Step 1 Choose **Call Routing** > **Dial Rules** > **Directory Lookup Dial Rules**.

The Directory Lookup Dial Rule Find and List window displays.

Step 2 To locate a specific directory lookup dial rule, enter search criteria and click **Find**.

A list of phones that match the search criteria displays.

Step 3 Perform one of the following actions:

- Check the check boxes next to the directory lookup dial rules that you want to delete and click **Delete Selected**.
- Delete all the directory lookup dial rules in the window by checking the check box in the matching records title bar and clicking **Delete Selected**.
- Display the directory lookup dial rule that you want to delete by clicking the name of the directory lookup dial rule and clicking **Delete**.

A confirmation dialog displays.

Step 4 To delete the directory lookup dial rules, click **OK**; to cancel the action, click **Cancel**.

Additional Information

See the "Related Topics" section on page 39-4.

Related Topics

- Directory Lookup Dial Rule Configuration Settings, page 39-1
- Finding a Directory Lookup Dial Rule, page 39-2
- Configuring Directory Lookup Dial Rules, page 39-3
- Deleting a Directory Lookup Dial Rule, page 39-4

Application Dial Rules

- Dial Rules Overview, *Cisco Unified Communications Manager System Guide*
- Application Dial Rules Configuration, page 38-1
- Configuring Dial Rules, page 38-3

Cisco Unified Communications Manager Attendant Console

- Configuring Cisco Unified Communications Manager Attendant Console Users, *Cisco Unified Communications Manager Features and Services Guide*
- Cisco Unified Communications Manager Attendant Console, *Cisco Unified Communications Manager Features and Services Guide*

CHAPTER 40

SIP Dial Rules Configuration

The following sections describe SIP dial rules configuration:

SIP Dial Rule Configuration Settings

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, and 7971. 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.

Table 40-1 describes the available settings in the SIP Dial Rules Configuration window. For more information about related procedures, see the "Related Topics" section on page 40-9.

Table 40-1 SIP Dial Rule Configuration 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	
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" section on page 40-5 for specific pattern formats. • Button—This parameter specifies the dial pattern to which line button 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.

Table 40-1 SIP Dial Rule Configuration Settings (continued)

Field	Description
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.
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.

Finding a SIP Dial Rule

Because you may have several SIP dial rules in your network, Cisco Unified Communications Manager lets you locate specific SIP dial rules based on specific criteria. Use the following procedure to locate SIP dial rules.

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

Procedure

Step 1 Choose **Call Routing** > **Dial Rules** > **SIP Dial Rules**.

The Find and List SIP Dial Rules window displays.

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records

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

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

Step 3 Click **Find**.

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

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

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

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

The window displays the item that you choose.

Additional Information

See the "Related Topics" section on page 40-9.

Configuring SIP Dial Rules

Perform the following procedure to add or update a SIP dial rule.

Procedure

Step 1 In the menu bar, choose **Call Routing** > **Dial Rules** > **SIP Dial Rules**.

The Find and List SIP Dial Rules window displays.

Step 2 Perform one of the followings tasks:

- To add a new SIP dial rule, click the **Add New** button and continue with Step 3.
- To update an existing SIP dial rule, locate the appropriate SIP dial rule as described in "Finding a SIP Dial Rule" section on page 40-3 and continue with Step 9.

Step 3 From the Dial Pattern drop-down list box, choose either 7905_7912 or 7940_7960_OTHER as the SIP dial rule type.

Step 4 Click the **Next** button.

The SIP Dial Rule Configuration redisplays with updated information.

Step 5 Enter a name and description of the Dial Rule that you are creating by using the information as described in Table 40-1. Click **Save**.

The SIP Dial Rule Configuration redisplays with updated information.

Step 6 Enter a name for the pattern description by using the information as described in Table 40-1.

Step 7 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.

Step 8 From the Dial Parameter drop-down list box, choose the type of parameter by using the information as described in Table 40-1.

Step 9 Enter the appropriate value, parameter, and description for the dial rule as described in Table 40-1.

Step 10 After completing a configuration, click the **Save** button.

Additional Information

See the "Related Topics" section on page 40-9.

Pattern Formats

See the following formats 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 "t*n*" set the timeout to *n* seconds.

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

- Characters "r*n*" repeat the last pattern *n* times.

Note The characters ">#" and "t*n*" 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

Table 40-2 provides some example SIP dial rules for the 7905_7912 dial rules.

Table 40-2 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.

Table 40-3 provides some example SIP dial rules for the 7940_7960_OTHER dial rules.

Table 40-3 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.
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.

Deleting a SIP Dial Rule

Perform the following procedure to delete a 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 delete. See the "Finding a SIP Dial Rule" section on page 40-3.

Step 3 Check the check box next to the SIP dial rule that you want to delete and click **Delete Selected**.

A dialog box displays to warn you that you cannot undo deletion of SIP dial rules.

Step 4 To delete the SIP dial rule, click **OK** or, to cancel the action, click **Cancel**. If you click **OK**, Cisco Unified Communications Manager removes the SIP dial rule from the SIP dial rules list.

Note You can delete multiple dial rules from the Find and List SIP Dial Rules window by checking the check boxes next to the appropriate dial rules and clicking **Delete Selected**. You can delete all the SIP dial rules in the window by clicking **Select All** and then clicking **Delete Selected**.

Additional Information

See the "Related Topics" section on page 40-9.

Resetting a 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. See the "Finding a SIP Dial Rule" section on page 40-3.

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:

- **Restart—**Restarts the chosen devices without shutting them down (reregisters the phones with Cisco Unified Communications Manager).
- **Reset**—Shuts down, then restarts, the device.
- **Close**—Closes the Reset Device dialog without performing any action.

Additional Information

See the "Related Topics" section on page 40-9.

Synchronizing Configuration of a SIP Dial Rule with Affected SIP Phones

To synchronize a SIP phone with a SIP Dial Rule that has undergone configuration changes, perform the following procedure, which will apply any outstanding configuration settings in the least-intrusive manner possible. (For example, a reset/restart may not be required on some affected 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**.

Additional Information

See the "Related Topics" section on page 40-9.

Related Topics

- SIP Dial Rule Configuration Settings, page 40-1
- Finding a SIP Dial Rule, page 40-3
- Configuring SIP Dial Rules, page 40-4
- SIP Dial Rules Examples, page 40-6
- Deleting a SIP Dial Rule, page 40-7
- Resetting a SIP Dial Rule, page 40-8
- Synchronizing Configuration of a SIP Dial Rule with Affected SIP Phones, page 40-8
- Dial Rules Overview, *Cisco Unified Communications Manager System Guide*

CHAPTER 41

Route Filter Configuration

Use the following topics to add, update, copy, or delete a route filter:

Route Filter Configuration Settings

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).

Refer 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.

Table 41-1 describes the route filter configuration settings.

Table 41-1 Route Filter Configuration 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	
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 41-2 in the "Route Filter Tag Descriptions" section on page 41-7 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 41-3 in the "Route Filter Tag Descriptions" section on page 41-7 for explanations of the route filter operators, such as NOT-SELECTED.

Additional Information

See the "Related Topics" section on page 41-10.

Finding a Route Filter

Because you might have several route filters in your network, Cisco Unified Communications Manager lets you locate specific route filters on the basis of specific criteria. Use the following procedure to locate route filters.

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

Procedure

Step 1 Choose **Call Routing** > **Route Filter**.

The Find and List Route Filters 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.

To filter or search records

- From the drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 41-10.

Configuring a Route Filter

The following procedure describes how to configure a route filter.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Call Routing** > **Route Filter**.

Step 2 Perform one of the following tasks:

- To copy an existing route filter, locate the appropriate route filter as described in the "Finding a Route Filter" section on page 41-2, click the **Copy** button next to the route filter that you want to copy, and continue with Step 3.
- To add a new route filter, click the **Add New** button and continue with Step 3.
- To update an existing route filter, locate the appropriate route filter as described in the "Finding a Route Filter" section on page 41-2, and continue with Step 3.

Step 3 In the Route Filter Configuration window that displays, enter the appropriate settings as described in Table 41-1, Table 41-2, and Table 41-3.

Step 4 To add the route filter, click **Save**.

Note Refer to the "Synchronizing a Route Filter With Affected Devices" section on page 41-6 before deciding whether to proceed to Step 5 below.

Step 5 If you are updating a route filter, click **Reset Devices**. Resetting the devices that are associated with the route filter causes calls on affected gateways to drop.

Additional Information

See the "Related Topics" section on page 41-10.

Adding and Editing 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. See the "Finding a Route Filter" section on page 41-2.

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 For help with entering data for route filter tags and operators for the North American Numbering Plan, see the "Route Filter Tag Descriptions" section on page 41-7.

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.

Note For help with entering data for route filter tags and operators for the North American Numbering Plan, see the "Route Filter Tag Descriptions" section on page 41-7.

Step 8 To save your changes to this route filter clause, click **Save**.

Additional Information

See the "Related Topics" section on page 41-10.

Removing 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.

Additional Information

See the "Related Topics" section on page 41-10.

Synchronizing a Route Filter With Affected Devices

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

Procedure

Step 1 Choose **Call Routing** > **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**.

Additional Information

See the "Related Topics" section on page 41-10.

Deleting a Route Filter

The following procedure describes how to delete a route filter.

Before You Begin

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. For more information about dependency records, see the "Accessing Dependency Records" section on page A-2. 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. See the "Configuring a Route Pattern" section on page 44-11 and the "Configuring a Translation Pattern" section on page 60-10.
- Delete the route patterns/hunt pilots, translation patterns, or other items that are using the route filter that you want to delete. See the "Deleting a Route Pattern" section on page 44-12 and the "Deleting a Translation Pattern" section on page 60-11.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Call Routing** > **Route Filter**.

Step 2 Locate the route filter that you want to delete. See the "Finding a Route Filter" section on page 41-2.

Step 3 Check the check box of the route filter that you want to delete and click **Delete Selected**.

A message displays that states that you cannot undo this action.

Caution Check carefully to ensure that you are deleting the correct route filter before initiating this action. You cannot retrieve deleted route filters. If a route filter is accidentally deleted, you must rebuild it.

Step 4 To delete the route filter, click **OK** or to cancel the deletion, click **Cancel**.

Tip You can also delete a route filter by locating and displaying the route filter that you want to delete and clicking **Delete**.

Additional Information

See the "Related Topics" section on page 41-10.

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 Table 17-5 in the "Special Characters and Settings" section of the *Cisco Unified Communications Manager System Guide* for definitions of wildcard characters.) The descriptions in Table 41-2 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. Table 41-2 describes the route filter tags for the North American Numbering Plan.

Table 41-2 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.
SUBSCRIBER	This tag specifies the last four digits of a seven-digit directory number in the form XXXX.

Table 41-2 Route Filter Tags (continued)

Tag	Description
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. Refer to 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. Refer to 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. Table 41-3 describes the operators that can be used with route filter tags.

Table 41-3 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.

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.

Additional Information

See the "Related Topics" section on page 41-10.

Related Topics

- Route Filter Configuration Settings, page 41-1
- Finding a Route Filter, page 41-2
- Configuring a Route Filter, page 41-4
- Adding and Editing Route Filter Clauses, page 41-4
- Removing Route Filter Clauses, page 41-5
- Synchronizing a Route Filter With Affected Devices, page 41-6
- Deleting a Route Filter, page 41-6
- Route Filter Tag Descriptions, page 41-7
- Understanding Route Plans, *Cisco Unified Communications Manager System Guide*

CHAPTER 42

Route Group Configuration

Use the following topics to add or delete a route group or to add devices to or to remove devices from a route group:

Route Group Configuration Settings

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, refer to the "Local Route Groups" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Table 42-1 describes the route group configuration settings. For related procedures, see the "Related Topics" section on page 42-7.

Table 42-1 Route Group Configuration 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.

Table 42-1 Route Group Configuration Settings (continued)

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 n^{th} member is the member to which Cisco Unified Communications Manager most recently extended a call. If the *n*th 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.

Table 42-1 Route Group Configuration Settings (continued)

Field	Description
Current Route Group Members	
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 "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.

Additional Information

See the "Related Topics" section on page 42-7.

Finding a Route Group

Because you might have several route groups in your network, Cisco Unified Communications Manager lets you locate specific route groups based on specific criteria. Use the following procedure to locate route groups.

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

Procedure

Step 1 Choose **Call Routing** > **Route/Hunt** > **Route Group**.

The Find and List Route Groups 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.

To filter or search records

- From the drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 42-7.

Configuring a Route Group

The following procedure describes how to configure a route group.

Procedure

Step 1 Choose **Call Routing** > **Route/Hunt** > **Route Group**.

Step 2 Perform one of the followings tasks:

- To copy an existing route group, locate the appropriate route group as described in the "Finding a Route Group" section on page 42-3, click the **Copy** button next to the route group that you want to copy, and continue with Step 3.
- To add a new route group, click the **Add New** button, and continue with Step 3.
- To update an existing route group, locate the appropriate route group as described in the "Finding a Route Group" section on page 42-3, and continue with Step 3.

Step 3 In the Route Group Configuration window that displays, enter a name in the Route Group Name field. The name can contain 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.

Step 4 Choose the appropriate settings as described in Table 42-1.

Note You must choose at least one device for a new route group before adding the new route group.

Step 5 To add or update this route group, click **Save**.

Additional Information

See the "Related Topics" section on page 42-7.

Adding Devices to a 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. See the "Finding a Route Group" section on page 42-3.

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.**

Additional Information

See the "Related Topics" section on page 42-7.

Removing Devices from a 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. See the "Finding a Route Group" section on page 42-3.

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**.

Additional Information

See the "Related Topics" section on page 42-7.

Deleting a Route Group

The following procedure describes how to delete a route group.

Before You Begin

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. For more information about dependency records, refer to the "Accessing Dependency Records" section on page A-2. 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. See the "Removing Route Groups from a Route List" section on page 43-5.

Tip To delete route groups and route patterns, first delete the route pattern; second, delete the route list; and finally, delete the route group.

Procedure

Step 1 Choose **Call Routing** > **Route/Hunt** > **Route Group**.

Step 2 Locate the route group that you want to delete. See the "Finding a Route Group" section on page 42-3.

Step 3 Check the check box next to the route group that you want to delete and click **Delete Selected**.

A dialog box displays to warn you that you cannot undo deletion of route groups.

Step 4 To delete the route group, click **OK**, or, to cancel the action, click **Cancel**. If you click **OK**, the Cisco Unified Communications Manager removes the route group from the route group list.

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

Additional Information

See the "Related Topics" section on page 42-7.

Related Topics

Route Groups

- Route Group Configuration Settings, page 42-1
- Finding a Route Group, page 42-3
- Configuring a Route Group, page 42-4
- Adding Devices to a Route Group, page 42-5
- Removing Devices from a Route Group, page 42-6
- Deleting a Route Group, page 42-6
- Understanding Route Plans, *Cisco Unified Communications Manager System Guide*
- Local Route Groups, *Cisco Unified Communications Manager Features and Services Guide*

Route Lists

- Adding a Route List, page 43-2
- Adding Route Groups to a Route List, page 43-4

CHAPTER 43

Route List Configuration

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.

Use the following topics to add or remove route lists or to add, remove, or change the order of route groups in a route list:

Finding Route Lists

Because you might have several route lists in your network, Cisco Unified Communications Manager lets you use specific criteria to locate specific route lists. To locate route lists, use the following procedure.

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

Procedure

Step 1 Choose **Call Routing** > **Route/Hunt** > **Route List**.

The Find and List Route 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 Step 3.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 43-7.

Adding a Route List

The following procedure describes how to add a route list.

Procedure

Step 1 Choose **Call Routing** > **Route/Hunt** > **Route List**.

Step 2 Click **Add New**.

Step 3 In the Route List 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 that each route list name is unique to the route plan.

Timesaver 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.

Add a description in the Description field.

Step 4 From the 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 Communications Manager.

Note If you choose a Cisco Unified Communications Manager group that has only one configured Cisco Unified Communications Manager, 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.

Step 5 To add this route list, click **Save**.

Note A popup message reminds you that you must add at least one route group to this route list for it to accept calls.

The Route List Configuration window displays the newly added route list.

Step 6 By default, the system checks the Enable this Route List check box for the 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.

Step 7 Add at least one route group to the new route list.

To add a route group to this list, click **Add Route Group** and perform Step 4 through Step 8 of the "Adding Route Groups to a Route List" section on page 43-4.

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.

Additional Information

See the "Related Topics" section on page 43-7.

Adding Route Groups to a 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, refer to the "Route Groups and Route Lists" section 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. See the "Finding Route Lists" section on page 43-1.

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 are configuring the Local Route Group feature, add the Standard Local Route Group to the route list by selecting the *Standard Local Route Group* entry in the drop-down list box.

Refer to the "Local Route Groups" chapter 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 "Calling and Called Party Transformations" in 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 "Called Party Number Transformations Settings" in 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 list on the left side of the window.

Step 8 To add more route groups to this list, click **Add Route Group** and repeat Step 3 through Step 7.

Step 9 When you finish adding route groups to the route list, click **Save**.

Note Refer to the "Synchronizing a Route List With Affected Route Groups" section on page 43-6 before deciding whether to proceed to Step 10 below.

Step 10 Click **Reset** for changes to take effect. When the popup windows display, click **OK**.

Additional Information

See the "Related Topics" section on page 43-7.

Removing Route Groups from a 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. See the "Finding Route Lists" section on page 43-1.

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**. If you click **OK**, when the window refreshes, the route group no longer appears in the route list.

Step 6 Click **Reset** for the changes to take effect. Click **OK** in response to the popup windows.

Additional Information

See the "Related Topics" section on page 43-7.

Changing the Order of Route Groups in a 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. See the "Finding Route Lists" section on page 43-1.

Step 3 From the Selected Groups list, choose a route group.

Step 4 To move the route group up or down in the list, select 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 **OK** in response to the popup windows.

Additional Information

See the "Related Topics" section on page 43-7.

Synchronizing a Route List With Affected Route Groups

To synchronize route groups with a route list that has undergone configuration changes, perform the following procedure, which will apply any outstanding configuration settings in the least-intrusive manner possible. (For example, a reset/restart may not be required on some affected devices.)

Procedure

Step 1 Choose **Call Routing** > **Route/Hunt** > **Route List**.

The Find and List Route Lists window displays.

Step 2 Choose the search criteria to use.

Step 3 Click **Find**.

The window displays a list of route lists that match the search criteria.

Step 4 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 5 Click **Apply Config to Selected**.

The **Apply Configuration Information** dialog displays.

Step 6 Click **OK**.

Additional Information

See the "Related Topics" section on page 43-7.

Deleting a Route List

The Cisco Unified Communications Manager associates a route list with a route pattern. You cannot delete a route list if it is associated 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. For more information about dependency records, see the "Accessing Dependency Records" section on page A-2.

Tip To delete route groups and route patterns, first delete the route pattern; second, delete the route list, and finally, delete the route group.

The following procedure describes how to delete a route list.

Procedure

Step 1 Choose **Call Routing** > **Route/Hunt** > **Route List**.

Step 2 Locate the route list that you want to delete. See the "Finding Route Lists" section on page 43-1.

Step 3 Click **Delete Selected**.

A dialog box displays to warn you that you cannot undo the deletion of a route list.

Step 4 To delete the route list, click **OK** or to cancel the action, click **Cancel**.

Caution You cannot delete a route list if it is associated with one or more route patterns.

Additional Information

See the "Related Topics" section on page 43-7.

Related Topics

- Finding Route Lists, page 43-1
- Adding a Route List, page 43-2
- Adding Route Groups to a Route List, page 43-4
- Removing Route Groups from a Route List, page 43-5
- Changing the Order of Route Groups in a Route List, page 43-6
- Synchronizing a Route List With Affected Route Groups, page 43-6

- Deleting a Route List, page 43-7
- Understanding Route Plans, *Cisco Unified Communications Manager System Guide*
- Understanding How Presence Works with Route Lists, *Cisco Unified Communications Manager Features and Services Guide*
- Local Route Groups, *Cisco Unified Communications Manager Features and Services Guide*

CHAPTER 44

Route Pattern Configuration

Use the following topics to find, add, update, copy, or delete a route pattern:

Route Pattern Configuration Settings

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.

Refer to "Understanding Route Plans" in *Cisco Unified Communications Manager System Guide* for more detailed route pattern information.

Note Refer to the "Local Route Groups" chapter 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.

Table 44-1 describes the available fields in the Route Pattern Configuration window. For related procedures, see the "Related Topics" section on page 44-13.

Table 44-1 Route Pattern Configuration 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 the "Wildcards and Special Characters in Route Patterns and Hunt Pilots" section in the *Cisco Unified Communications Manager System Guide* for more information about wildcards.
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. See the "Partition Configuration" section on page 52-1 for more information on how to use partitions. 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 Finding a Partition procedure in the *Cisco Unified Communications Manager Administration Guide*. **Note** To set the maximum list box items, choose **System > Enterprise Parameters** and choose **CCMAdmin Parameters**. **Note** Make sure that the combination of route pattern, route filter, and partition is unique within the Cisco Unified Communications Manager cluster.
Description	Enter a description of the route pattern.
Numbering Plan	Choose a numbering plan.

Table 44-1 Route Pattern Configuration Settings (continued)

Field	Description
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. Find and choose a route filter name by using the Finding a Route Filter procedure in the *Cisco Unified Communications Manager Administration Guide*. **Note** To set the maximum list box items, choose **System** > **Enterprise Parameters** and choose **CCMAdmin Parameters**.
MLPP Precedence	Choose an MLPP precedence setting for this 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** Refer to the "Precedence" section in the "Multilevel Precedence and Preemption" chapter of the *Cisco Unified Communications Manager Features and Services Guide* for more information.
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**. Refer to the *Cisco Unified Communications Manager Features and Services Guide* for more information.
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.

Table 44-1 Route Pattern Configuration Settings (continued)

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.
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.

Table 44-1 Route Pattern Configuration Settings (continued)

Field	Description
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 NANP 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 the "Calling Party Number Transformations Settings" section 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 NANP 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.
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.

Table 44-1 Route Pattern Configuration Settings (continued)

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 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.

Table 44-1 Route Pattern Configuration Settings (continued)

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. For more information about this field, see Table 17-11 in the "Connected Party Presentation and Restriction Settings" section in the *Cisco Unified Communications Manager System Guide*.

Table 44-1 Route Pattern Configuration Settings (continued)

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 Table 17-11 in the "Connected Party Presentation and Restriction Settings" section 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 the "Discard Digits Instructions" section 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 NANP 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 NANP 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.

Table 44-1 Route Pattern Configuration Settings (continued)

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.

Table 44-1 Route Pattern Configuration Settings (continued)

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, go to http://www.nanpa.com/.
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.

Additional Information

See the "Related Topics" section on page 44-13.

Finding a Route Pattern

Because you might have several route patterns in your network, Cisco Unified Communications Manager lets you use specific criteria to locate specific route patterns. To locate route patterns, use the following procedure.

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

Procedure

Step 1 Choose **Call Routing** > **Route/Hunt** > **Route Pattern**.

The Find and List Route Patterns 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.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 44-13.

Configuring a Route Pattern

This section describes how to configure a route pattern.

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 the "Special Characters and Settings" section in the *Cisco Unified Communications Manager System Guide* for more information about wildcards.

Procedure

Step 1 Choose **Call Routing** > **Route/Hunt** > **Route Pattern**.

Step 2 Perform one of the following tasks:

- To copy an existing route pattern, locate the appropriate route pattern as described in the "Finding a Route Pattern" section on page 44-10, click the **Copy** button next to the route pattern that you want to copy, and continue with Step 3.
- To add a new route pattern, click the **Add New** button and continue with Step 3.
- To update an existing route pattern, locate the appropriate route pattern as described in the "Finding a Route Pattern" section on page 44-10 and continue with Step 3.

Note If you change the gateway or route list, you must click **Update** prior to choosing the **Edit** link. Otherwise, you get linked to the previous gateway or route list.

Step 3 In the Route Pattern Configuration window that displays, enter the appropriate settings as described in Table 44-1.

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.

Step 4 Click **Save**.

Additional Information

See the "Related Topics" section on page 44-13.

Deleting a Route Pattern

This section describes how to delete a route pattern.

Procedure

Step 1 Choose **Call Routing** > **Route/Hunt** > **Route Pattern**.

Step 2 Locate the route pattern that you want to delete. See the "Finding a Route Pattern" section on page 44-10.

Step 3 Check the check box of the route pattern that you want to delete and click **Delete Selected**.

A message that displays states that you cannot undo this action.

Step 4 To delete the route pattern, click **OK,** or, to cancel the deletion, click **Cancel**.

Tip You can also delete a route pattern by locating and displaying the route pattern that you want to delete and clicking **Delete**.

Additional Information

See the "Related Topics" section on page 44-13.

Related Topics

- Route Pattern Configuration Settings, page 44-1
- Finding a Route Pattern, page 44-10
- Configuring a Route Pattern, page 44-11
- Deleting a Route Pattern, page 44-12
- Wildcards and Special Characters in Route Patterns and Hunt Pilots, *Cisco Unified Communications Manager System Guide*
- Configuring a Route Filter, page 41-4
- Understanding Route Plans, *Cisco Unified Communications Manager System Guide*
- Local Route Groups, *Cisco Unified Communications Manager Features and Services Guide*

CHAPTER 45

Line Group Configuration

Use the following topics to add or delete a line group or to add directory numbers to or to remove directory numbers from a line group:

Line Group Configuration Settings

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.

Table 45-1 describes the line group configuration settings.

Table 45-1 Line Group Configuration Settings

Field	Description
Line Group Information	
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.
RNA Reversion Timeout	Enter a time, in seconds, after which Cisco Unified Communications Manager 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 Communications Manager 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 Communications Manager distributes a call to idle or available members starting from the $(n+1)^{th}$ member of a line group, where the n^{th} member is the member to which Cisco Unified Communications Manager most recently extended a call. If the n^{th} member is the last member of a line group, Cisco Unified Communications Manager distributes a call starting from the top of the line group. • Longest Idle Time—If you choose this distribution algorithm, Cisco Unified Communications Manager 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 Communications Manager 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*.

Table 45-1 Line Group Configuration Settings (continued)

Field	Description
Hunt Options	
No Answer	For a given distribution algorithm, choose a hunt option for Cisco Unified Communications Manager 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 Communications Manager 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 Communications Manager 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 Communications Manager 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 Communications Manager skips the remaining members of this line group when the RNA reversion timeout value elapses for the first member. Cisco Unified Communications Manager then proceeds directly to the next line group in a hunt list. • Stop hunting—If you choose this hunt option, Cisco Unified Communications Manager stops hunting after trying to distribute a call to the first member of this line group and the member does not answer the call.

Table 45-1 Line Group Configuration Settings (continued)

Field	Description
Busy	For a given distribution algorithm, choose a hunt option for Cisco Unified Communications Manager 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 Communications Manager 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 Communications Manager 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 Communications Manager 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 Communications Manager skips the remaining members of this line group upon encountering a busy member. Cisco Unified Communications Manager proceeds directly to the next line group in a hunt list. • Stop hunting—If you choose this hunt option, Cisco Unified Communications Manager stops hunting after trying to distribute a call to the first busy member of this line group.

Table 45-1 Line Group Configuration Settings (continued)

Field	Description
Not Available	For a given distribution algorithm, choose a hunt option for Cisco Unified Communications Manager 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 Communications Manager 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 Communications Manager 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 Communications Manager 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 Communications Manager skips the remaining members of this line group upon encountering the first unavailable member. Cisco Unified Communications Manager proceeds directly to the next line group in a hunt list. • Stop hunting—If you choose this hunt option, Cisco Unified Communications Manager stops hunting after trying to distribute a call to the first unavailable member of this line group.
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**.

Table 45-1 Line Group Configuration Settings (continued)

Field	Description
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 "Route Plan Overview" 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 Communications Manager 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.

Additional Information

See the "Related Topics" section on page 45-10.

Finding a Line Group

Because you may have several line groups in your network, Cisco Unified Communications Manager lets you locate specific line groups on the basis of specific criteria. Use the following procedure to locate line groups.

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

Procedure

Step 1 Choose **Call Routing** > **Route/Hunt** > **Line Group**.

The Find and List Line Groups 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.

To filter or search records

- From the drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 45-10.

Configuring a Line Group

The following procedure describes how to configure a 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 Perform one of the following tasks:

- To copy an existing line group, locate the appropriate line group as described in the "Finding a Line Group" section on page 45-6, click the **Copy** button next to the line group that you want to copy and continue with Step 3.
- To add a new line group, click the **Add New** button and continue with Step 3.
- To update an existing line group, locate the appropriate line group as described in the "Finding a Line Group" section on page 45-6 and continue with Step 3.

Step 3 In the Line Group Configuration window that displays, enter a name in the Line Group Name field. The name can contain 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.

Step 4 Choose the appropriate settings as described in Table 45-1.

Step 5 To add or update this line group, click **Save**.

Additional Information

See the "Related Topics" section on page 45-10.

Adding Members to a 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. See the "Finding a Line Group" section on page 45-6.

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.

Additional Information

See the "Related Topics" section on page 45-10.

Removing Members from a 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. See the "Finding a Line Group" section on page 45-6.

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**.

Additional Information

See the "Related Topics" section on page 45-10.

Deleting a Line Group

The following procedure describes how to delete a line group.

Before You Begin

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. For more information about dependency records, see the "Accessing Dependency Records" section on page A-2. 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. See the "Removing Route Groups from a Route List" section on page 43-5.

Tip To delete line groups and hunt pilots; first, delete the hunt pilot; second, delete the hunt list; and finally, delete the line group.

Procedure

Step 1 Choose **Call Routing** > **Route/Hunt** > **Line Group**.

Step 2 Locate the line group that you want to delete. See the "Finding a Line Group" section on page 45-6.

Step 3 Check the check box next to the line group that you want to delete and click **Delete Selected**.

A dialog box displays to warn you that you cannot undo deletion of line groups.

Step 4 To delete the line group, click **OK** or to cancel the action, click **Cancel**. If you click **OK**, the Cisco Unified Communications Manager removes the line group.

Note You can delete multiple line groups from the Find and List Line Groups window by checking the check boxes next to the appropriate line groups and clicking **Delete Selected**. You can delete all the line groups in the window by clicking **Select All** and clicking **Delete Selected**.

Additional Information

See the "Related Topics" section on page 45-10.

Related Topics

Line Groups

- Line Group Configuration Settings, page 45-1
- Finding a Line Group, page 45-6
- Configuring a Line Group, page 45-8
- Adding Members to a Line Group, page 45-8

- Removing Members from a Line Group, page 45-9
- Deleting a Line Group, page 45-10

Route Lists and Route Groups

- Adding a Route List, page 43-2
- Adding Route Groups to a Route List, page 43-4
- Understanding Route Plans, *Cisco Unified Communications Manager System Guide*

CHAPTER 46

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.

Use the following topics 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:

- Finding Hunt Lists, page 46-1
- Adding a Hunt List, page 46-2
- Adding Line Groups to a Hunt List, page 46-4
- Removing Line Groups from a Hunt List, page 46-5
- Changing the Order of Line Groups in a Hunt List, page 46-5
- Synchronizing a Hunt List With Affected Line Groups, page 46-6
- Deleting a Hunt List, page 46-6

Finding 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 Step 3.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 46-7.

Adding a 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.

Timesaver 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:

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.

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 through Step 6 of the "Adding Line Groups to a Hunt List" section on page 46-4.

Additional Information

See the "Related Topics" section on page 46-7.

Adding Line Groups to a 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. See the "Finding Hunt Lists" section on page 46-1.

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 through Step 5.

Step 7 When you finish adding line groups to the hunt list, click **Save**.

Note Refer to the "Synchronizing a Hunt List With Affected Line Groups" section on page 46-6 before deciding whether to proceed to Step 8 below.

Step 8 To reset the hunt list, click **Reset**. When the popup windows display, click **OK**.

Additional Information

See the "Related Topics" section on page 46-7.

Removing Line Groups from a 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. See the "Finding Hunt Lists" section on page 46-1.

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.

Additional Information

See the "Related Topics" section on page 46-7.

Changing the Order of Line Groups in a 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. See the "Finding Hunt Lists" section on page 46-1.

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.

Additional Information

See the "Related Topics" section on page 46-7.

Synchronizing a Hunt List With Affected Line Groups

To synchronize line groups with a hunt list that has undergone configuration changes, perform the following procedure, which will apply any outstanding configuration settings in the least-intrusive manner possible. (For example, a reset/restart may not be required on some affected devices.)

Procedure

Step 1 Choose **Call Routing** > **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**.

Additional Information

See the "Related Topics" section on page 46-7.

Deleting a 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. For more information about dependency records, see the "Accessing Dependency Records" section on page A-2.

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. See the "Finding Hunt Lists" section on page 46-1.

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.

Additional Information

See the "Related Topics" section on page 46-7.

Related Topics

- Finding Hunt Lists, page 46-1
- Adding a Hunt List, page 46-2
- Adding Line Groups to a Hunt List, page 46-4
- Removing Line Groups from a Hunt List, page 46-5
- Changing the Order of Line Groups in a Hunt List, page 46-5
- Synchronizing a Hunt List With Affected Line Groups, page 46-6
- Deleting a Hunt List, page 46-6
- Understanding Route Plans, *Cisco Unified Communications Manager System Guide*

CHAPTER 47

Hunt Pilot Configuration

Use the following topics to add, configure, or delete a hunt pilot:

Hunt Pilot Configuration Settings

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.

Refer to "Understanding Route Plans" in *Cisco Unified Communications Manager System Guide* for more detailed hunt pilot information.

Table 47-1 describes the available fields in the Hunt Pilot Configuration window. For related procedures, see the "Related Topics" section on page 47-14.

Table 47-1 Hunt Pilot Configuration 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 the "Wildcards and Special Characters in Route Patterns and Hunt Pilots" section in the *Cisco Unified Communications Manager System Guide* for more information about wildcards.
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. See the "Partition Configuration" section on page 52-1 for more information on how to use partitions. 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 Finding a Partition procedure in the *Cisco Unified Communications Manager Administration Guide*. **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 Communications Manager cluster.
Description	Enter a description of the hunt pilot.
Numbering Plan	Choose a numbering plan.

Table 47-1 Hunt Pilot Configuration Settings (continued)

Field	Description
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. Find and choose a route filter name by using the Finding a Route Filter procedure in the *Cisco Unified Communications Manager Administration Guide*. **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** Refer to the "Precedence" section in the "Multilevel Precedence and Preemption" chapter of the *Cisco Unified Communications Manager Features and Services Guide* for more information.
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.

Table 47-1 Hunt Pilot Configuration Settings (continued)

Field	Description
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 Communications Manager 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.
Urgent Priority	If the dial plan contains overlapping hunt lists, Cisco Unified Communications Manager 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 Communications Manager must route a call immediately.

Table 47-1 Hunt Pilot Configuration Settings (continued)

Field	Description
Hunt Forward 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: • Use Personal Preferences—Use this check box to enable the Call Forward No Coverage (CFNC) settings for the original called number that forwarded the call to this hunt pilot. The CFNC setting specifies a call forwarding reason that you administer in the Directory Number Configuration window. Calls get diverted based on the value in the directory number Coverage/Destination field when a call to the directory number first diverts to coverage, and coverage either exhausts or times out, and the associated hunt pilot for coverage specifies Use Personal Preferences for its final forwarding. **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 calls are forwarded. • Calling Search Space—This setting applies to all devices that are using this directory number.
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: • Use Personal Preferences—Use this check box to enable the Call Forward No Coverage (CFNC) settings for the original called number that forwarded the call to this hunt pilot. The CFNC setting specifies a call forwarding reason that you administer in the Directory Number Configuration window. Calls get diverted based on the value in the directory number Coverage/Destination field when a call to the directory number first diverts to coverage, and coverage either exhausts or times out, and the associated hunt pilot for coverage specifies Use Personal Preferences for its final forwarding. **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 calls are forwarded. • Calling Search Space—This setting applies to all devices that are using this directory number.

Table 47-1 Hunt Pilot Configuration Settings (continued)

Field	Description
Maximum Hunt Timer	Enter a value (in seconds) that specifies the maximum time for hunting. 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 Communications Manager only uses the configuration for the Maximum Hunt Timer setting if you configure the Hunt Forward settings in the Hunt Pilot Configuration window.
Park Monitoring	
Park Monitoring Forward No Retrieve Destination	This release of Cisco Unified Communications Manager does not support this setting.
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 for the NANP 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 the "Calling Party Number Transformations Settings" section 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 NANP 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.

Table 47-1 Hunt Pilot Configuration Settings (continued)

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 hunt pilot. 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 Table 17-8 in the "Calling Party Number Transformations Settings" section in the *Cisco Unified Communications Manager System Guide*.
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 hunt pilot. 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 Table 17-8 in the "Calling Party Number Transformations Settings" section in the *Cisco Unified Communications Manager System Guide*.

Table 47-1 Hunt Pilot Configuration Settings (continued)

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 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 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.

Table 47-1 Hunt Pilot Configuration Settings (continued)

Field	Description
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 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 Communications Manager to block the display of the connected party phone number. For more information about this field, see Table 17-11 in the "Connected Party Presentation and Restriction Settings" section in the *Cisco Unified Communications Manager System Guide*.
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 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 Communications Manager to block the display of the connected party name. For more information about this field, see Table 17-11 in the "Connected Party Presentation and Restriction Settings" section 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 hunt pilot. The discard digits that display depend on the numbering plan that you choose from the Numbering Plan drop-down list box. See the "Discard Digits Instructions" section 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.
Called Party Transform Mask	Enter a transformation mask value. Valid entries for the NANP 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.

Table 47-1 Hunt Pilot Configuration Settings (continued)

Field	Description
Prefix Digits (Outgoing Calls)	Enter prefix digits in the Prefix Digits (Outgoing Calls) field. Valid entries for the NANP 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 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.

Table 47-1 Hunt Pilot Configuration Settings (continued)

Field	Description
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.
AAR Group Settings	
AAR Group	Choose an Automated Alternate Routing (AAR) group from the drop-down list box. **Note** You can enable AAR for this hunt pilot only if all members of the line group are in the same location.
External Number Mask	Enter an external number mask value for the hunt pilot. Cisco Unified Communications Manager 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.

Finding a Hunt Pilot

Because you may have several hunt pilots in your network, Cisco Unified Communications Manager lets you use specific criteria to locate specific hunt pilots. To locate hunt pilots, use the following procedure.

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

Procedure

Step 1 Choose **Call Routing** > **Route/Hunt** > **Hunt Pilot**.

The Find and List Hunt Pilots 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.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 47-14.

Configuring a Hunt Pilot

This section describes how to configure a hunt pilot.

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 the "Special Characters and Settings" section in the *Cisco Unified Communications Manager System Guide* for more information about wildcards.

Procedure

Step 1 Choose **Call Routing > Route/Hunt > Hunt Pilot**.

The Find and List Hunt Pilots window displays.

Step 2 Perform one of the following tasks:

- To copy an existing hunt pilot, locate the appropriate hunt pilot as described in "Finding a Hunt Pilot" section on page 47-11. Click the **Copy** button next to the hunt pilot that you want to copy. The window displays the copy of the hunt pilot. Change the value in the Hunt Pilot field, and continue with Step 3.
- To add a new hunt pilot, click the **Add New** button and continue with Step 3.
- To update an existing hunt pilot, locate the appropriate hunt pilot as described in "Finding a Hunt Pilot" section on page 47-11, and continue with Step 3.

Step 3 Enter the appropriate settings as described in Table 47-1.

Step 4 Click **Save**.

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.

Additional Information

See the "Related Topics" section on page 47-14.

Deleting a Hunt Pilot

This section describes how to delete a hunt pilot.

Procedure

Step 1 Choose **Call Routing** > **Route/Hunt** > **Hunt Pilot**.

Step 2 Locate the hunt pilot that you want to delete. See the "Finding a Hunt Pilot" section on page 47-11.

Step 3 Check the check box of the hunt pilot that you want to delete and click **Delete Selected**.

A message that displays states that you cannot undo this action.

Step 4 To delete the hunt pilot, click **OK** or to cancel the deletion, click **Cancel**.

Tip You can also delete a hunt pilot by locating and displaying the hunt pilot that you want to delete and clicking **Delete**.

Additional Information

See the "Related Topics" section on page 47-14.

Related Topics

- Hunt Pilot Configuration Settings, page 47-1
- Finding a Hunt Pilot, page 47-11
- Configuring a Hunt Pilot, page 47-12
- Deleting a Hunt Pilot, page 47-14
- Understanding Route Plans, *Cisco Unified Communications Manager System Guide*
- Wildcards and Special Characters in Route Patterns and Hunt Pilots, *Cisco Unified Communications Manager System Guide*
- Configuring a Route Filter, page 41-4

CHAPTER 48

SIP Route Pattern Configuration

This section contains information on the following topics:

SIP Route Pattern Configuration Settings

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 there are no default SIP route patterns in Cisco Unified Communications Manager, the administrator must set them up.

Domain name examples: cisco.com, my-pc.cisco.com, *.com, rtp-ccm[1-5].cisco.com

Valid characters for domain names: [, -, ., 0-9, A-Z, a-z, *, and].

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).

Valid characters for IP addresses: 0-9, ., and /

Before you begin:

Ensure at least one SIP Profile and SIP trunk are configured before you can configure a SIP route pattern.

Table 48-1 describes the SIP route pattern configuration settings. For related procedures, see the "Related Topics" section on page 48-7.

Table 48-1 SIP Route Pattern Configuration 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. **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. **Note** 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.
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.
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. See the "Partition Configuration" section on page 52-1 for more information on how to use partitions. 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 OK. **Note** To set the maximum list box items, choose **System > Enterprise Parameters** and choose CCMAdmin Parameters. **Note** Make sure that the combination of SIP route pattern, route filter, and partition is unique within the Cisco Unified Communications Manager cluster.
SIP Trunk	(Required) Use the drop-down list to choose the SIP trunk to which the SIP route pattern should be associated.

Table 48-1 SIP Route Pattern Configuration Settings (continued)

Field	Description
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.
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 the "Calling Party Number Transformations Settings" section 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 Table 17-8 in the "Calling Party Number Transformations Settings" section in the *Cisco Unified Communications Manager System Guide*.

Table 48-1 SIP Route Pattern Configuration Settings (continued)

Field	Description
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 Table 17-8 in the "Calling Party Number Transformations Settings" section in the *Cisco Unified Communications Manager System Guide*.
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 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. For more information about this field, see Table 17-11 in the "Connected Party Presentation and Restriction Settings" section 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 Table 17-11 in the "Connected Party Presentation and Restriction Settings" section in the *Cisco Unified Communications Manager System Guide*.

Finding a SIP Route Pattern

Because you can have several SIP route patterns in your network, Cisco Unified Communications Manager lets you locate specific SIP route patterns on the basis of specific criteria. Use the following procedure to locate SIP route patterns.

Note During your work in a browser session, the cookies on the client machine store your find/list search preference. 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, the machine retains your Cisco Unified Communications Manager search preferences until you modify your search.

Procedure

Step 1 Choose **Call Routing** > **SIP Route Pattern**.

The Find and List SIP Route Patterns window displays.

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records:

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

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

Step 3 Click **Find**.

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

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

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

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

The window displays the item that you choose.

Additional Information

See the "Related Topics" section on page 48-7.

Configuring a SIP Route Pattern

This section describes how to add, update, or copy a SIP route pattern.

Before You Begin

You must configure a SIP trunk before you can configure the SIP route pattern. See the "Configuring a Trunk" section on page 92-48.

Procedure

Step 1 Perform one of the following tasks:

- To add a SIP route pattern, choose **Call Routing** > **SIP Route Pattern** and click **Add New**.
- To update a SIP route pattern, find the pattern by using the procedure in the "Finding a SIP Route Pattern" section on page 48-5
- To copy a SIP route pattern, find the pattern that you want to copy by using the procedure in the "Finding a SIP Route Pattern" section on page 48-5. Click the **Copy** icon that is associated with the pattern that you want to copy.

The SIP Route Pattern Configuration window displays.

Step 2 Enter the appropriate settings as described in Table 48-1.

Step 3 To save the data and to add the server to 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).

Additional Information

See the "Related Topics" section on page 48-7.

Deleting a SIP Route Pattern

This section describes how to delete a SIP route pattern from the Cisco Unified Communications Manager database.

Procedure

Step 1 Find the SIP route pattern by using the procedure in the "Finding a SIP Route Pattern" section on page 48-5.

Step 2 From the list of matching records, choose the SIP route pattern that you want to delete.

Step 3 To delete the SIP route pattern, click the **Delete Selected Item** icon that displays in the tool bar in the upper, left corner of the window (or click the **Delete Selected** button that displays at the bottom of the window).

If the SIP route pattern is not in use, Cisco Unified Communications Manager deletes it. If it is in use, a message displays.

Additional Information

See the "Related Topics" section on page 48-7.

Related Topics

- SIP Route Pattern Configuration Settings, page 48-1
- Finding a SIP Route Pattern, page 48-5
- Configuring a SIP Route Pattern, page 48-6
- Deleting a SIP Route Pattern, page 48-6
- Understanding Session Initiation Protocol (SIP)

CHAPTER 49

Access List Configuration

Mobile Connect 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 on Mobile Connect and how to configure access lists, refer to the Cisco Unified Mobility chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

CHAPTER 50

Time Period Configuration

Use the following topics to add, update, copy, or delete a time period:

Time Period Configuration Settings

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, refer to "Time-of-Day Routing" in the *Cisco Unified Communications Manager System Guide*.

Table 50-1 describes the time period configuration settings. For related procedures, see the "Related Topics" section on page 50-6.

Table 50-1 Time Period Configuration 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.

Table 50-1 Time Period Configuration Settings (continued)

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 o*n 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.

Additional Information

See the "Related Topics" section on page 50-6.

Finding a Time Period

Because you might have several time periods in your network, Cisco Unified Communications Manager lets you locate specific time periods by using specific criteria as the basis. Use the following procedure to locate time periods.

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

Procedure

Step 1 Choose **Call Routing** > **Class of Control** > **Time Period**.

The Find and List Time Periods window displays.

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records:

- From the drop-down list box, select a search parameter.
- Specify the appropriate search text, if applicable.

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

Step 3 Click **Find**.

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

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

Step 4 From the list of records that display, click the link for the record 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.

Additional Information

See the "Related Topics" section on page 50-6.

Configuring a Time Period

The following procedure describes how to configure a time period.

Procedure

Step 1 In the menu bar, choose **Call Routing** > **Class of Control** > **Time Period**.

The Find and List Time Periods window displays.

Step 2 Perform one of the following tasks:

- To copy an existing time period, locate the appropriate time period as described in "Finding a Time Period" section on page 50-3. Click the **Copy** icon next to the time period that you want to copy. The window displays the copy of the time period. Change the value in the Name field, and continue with Step 3.
- To add a new time period, click the **Add New** button, and continue with Step 3.

- To update an existing time period, locate the appropriate time period as described in "Finding a Time Period" section on page 50-3, and continue with Step 3.

Step 3 Enter the appropriate settings as described in Table 50-1.

Step 4 Click **Save**.

Additional Information

See the "Related Topics" section on page 50-6.

Deleting a Time Period

The following procedure describes how to delete a time period.

Before You Begin

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. For more information about dependency records, see the "Accessing Dependency Records" section on page A-2. 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. See the "Configuring a Time Schedule" section on page 51-4.
- Delete the time schedules that are using the time period that you want to delete. See the "Deleting a Time Schedule" section on page 51-4.

Procedure

Step 1 In the menu bar, choose **Call Routing > Class of Control > Time Period**.

Step 2 Locate the time period that you want to delete. See the "Finding a Time Period" section on page 50-3.

Step 3 Check the check box of the time period that you want to delete and click **Delete Selected**.

A message displays that states that you cannot undo this action.

Step 4 Click **OK** to delete the time period or click **Cancel** to cancel the deletion.

Caution Before initiating this action, check carefully to ensure that you are deleting the correct time period. You cannot retrieve deleted time periods. If a time period is accidentally deleted, you must rebuild it.

Tip You can also delete a time period by locating and displaying the time period that you want to delete and clicking **Delete**.

Additional Information

See the "Related Topics" section on page 50-6.

Related Topics

- Time Period Configuration Settings, page 50-1
- Finding a Time Period, page 50-3
- Configuring a Time Period, page 50-4
- Deleting a Time Period, page 50-5
- Time-of-Day Routing, *Cisco Unified Communications Manager System Guide*

CHAPTER 51

Time Schedule Configuration

Use the following topics to find, add, update, copy, or delete a time schedule:

- Time Schedule Configuration Settings, page 51-1
- Finding a Time Schedule, page 51-2
- Configuring a Time Schedule, page 51-4
- Deleting a Time Schedule, page 51-4
- Related Topics, page 51-5

Time Schedule Configuration Settings

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, refer to "Time-of-Day Routing" in the *Cisco Unified Communications Manager System Guide*.

Table 51-1 describes the time schedule configuration settings.

Table 51-1 Time Schedule Configuration 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.

Table 51-1 Time Schedule Configuration Settings (continued)

Field	Description
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.
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. **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.

Additional Information

See the "Related Topics" section on page 51-5.

Finding a Time Schedule

Because you might have several time schedules in your network, Cisco Unified Communications Manager lets you locate specific time schedules by using specific criteria as the basis. Use the following procedure to locate time schedules.

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

Procedure

Step 1 Choose **Call Routing** > **Class of Control** > **Time Schedule**.

The Find and List Time Schedules window displays.

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records:

- From the drop-down list box, select a search parameter.
- Specify the appropriate search text, if applicable.

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

Step 3 Click **Find**.

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

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

Step 4 From the list of records that display, click the link for the record 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.

Additional Information

See the "Related Topics" section on page 51-5.

Configuring a Time Schedule

The following procedure describes how to configure a time schedule.

Procedure

Step 1 In the menu bar, choose **Call Routing** > **Class of Control** > **Time Schedule**.

The Find and List Time Schedules window displays.

Step 2 Perform one of the following tasks:

- To copy an existing time schedule, locate the appropriate time schedule as described in the "Finding a Time Schedule" section on page 51-2. Click the **Copy** icon next to the time schedule that you want to copy. The window displays the copy of the time schedule. Change the value in the Name field, and continue with Step 3.
- To add a new time schedule, click the **Add New** button and continue with Step 3.
- To update an existing time schedule, locate the appropriate time schedule as described in the "Finding a Time Schedule" section on page 51-2, and continue with Step 3.

Step 3 Enter the appropriate settings as described in Table 51-1.

Step 4 Click **Save**.

Additional Information

See the "Related Topics" section on page 51-5.

Deleting a Time Schedule

The following procedure describes how to delete a time schedule.

Before You Begin

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. For more information about dependency records, see the "Accessing Dependency Records" section on page A-2. 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. See the "Configuring a Partition" section on page 52-4.
- Delete the partitions that are using the time schedule that you want to delete. See the "Partition Configuration" chapter.

Procedure

Step 1 In the menu bar, choose **Call Routing > Class of Control > Time Schedule**.

Step 2 Locate the time schedule that you want to delete. See the "Finding a Time Schedule" section on page 51-2.

Step 3 Check the check box of the time schedule that you want to delete and click **Delete Selected**.

A message displays that states that you cannot undo this action.

Step 4 To delete the time schedule, click **OK** or to cancel the deletion, click **Cancel**.

Caution Before initiating this action, check carefully to ensure that you are deleting the correct time schedule. You cannot retrieve deleted time schedules. If a time schedule is accidentally deleted, you must rebuild it.

Tip You can also delete a time schedule by locating and displaying the time schedule that you want to delete and clicking **Delete**.

Additional Information

See the "Related Topics" section on page 51-5.

Related Topics

- Time Schedule Configuration Settings, page 51-1
- Finding a Time Schedule, page 51-2
- Configuring a Time Schedule, page 51-4
- Deleting a Time Schedule, page 51-4
- Time-of-Day Routing, *Cisco Unified Communications Manager System Guide*

CHAPTER 52

Partition Configuration

Use the following topics to find, add, update, or delete route partitions:

Partition Configuration Settings

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, refer to "Partitions and Calling Search Spaces" in the *Cisco Unified Communications Manager System Guide*.

Table 52-1 describes the partition configuration settings. For related procedures, see the "Related Topics" section on page 52-7.

Table 52-1 Partition Configuration Settings

Field	Description
Partition Information	
(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 alphanumeric 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. Table 52-2 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. 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.

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.

Tip You can enter multiple partitions at the same time by entering the partition name and description, if applicable, in the Partition Name & Description text box. Remember to use one line for each partition entry and to separate the partition name and description with a comma.

Table 52-2 provides examples of the maximum number of partitions that can be added to a calling search space if partition names are of fixed length. Refer to "Partition Name Limitations" in the *Cisco Unified Communications Manager System Guide* for details about how this maximum number is calculated.

Table 52-2 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

Additional Information

See the "Related Topics" section on page 52-7.

Finding a Partition

Because you might have several partitions in your network, Cisco Unified Communications Manager lets you locate specific partitions based on specific criteria. Use the following procedure to locate partitions.

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

Procedure

Step 1 Choose **Call Routing** > **Class of Control** > **Partition**.

The Find and List Partitions window displays.

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records:

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

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

Step 3 Click **Find**.

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

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

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

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

The window displays the item that you choose.

Additional Information

See the "Related Topics" section on page 52-7.

Configuring a Partition

Perform the following procedure to add a partition.

Procedure

Step 1 In the menu bar, choose **Call Routing > Class of Control > Partition**.

The Find and List Partitions window displays.

Step 2 Perform one of the following tasks:

- To add a new partition, click the **Add New** button, and continue with Step 3.
- To update an existing partition, locate the appropriate partition as described in "Finding a Partition" section on page 52-3, and continue with Step 3.

Step 3 Enter the appropriate settings as described in Table 52-1.

Step 4 Click **Save**.

If you are updating a partition, click **Reset,** or use the **Apply Config** button as described in the "Synchronizing a Partition With Affected Devices" section on page 52-5. When you reset devices that are associated with the partition, all calls on affected gateways drop.

Note You can configure multiple partitions. To enter multiple partitions, use one line for each partition entry. You can enter up to 75 partitions; 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.

Additional Information

See the "Related Topics" section on page 52-7.

Searching for a 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**.

Additional Information

See the "Related Topics" section on page 52-7.

Synchronizing a Partition With Affected Devices

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

Procedure

Step 1 Choose **Call Routing** > **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**.

Additional Information

See the "Related Topics" section on page 52-7.

Deleting a Partition

The following procedure describes how to delete a partition.

Before You Begin

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. For more information about dependency records, refer to the "Accessing Dependency Records" section on page A-2. 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.

Procedure

Step 1 In the menu bar, choose **Call Routing** > **Class of Control** > **Partition.**

Step 2 Locate the partition that you want to delete. See the "Finding a Partition" section on page 52-3.

Step 3 Check the check box of the partition that you want to delete and click **Delete Selected**.

Tip You can delete all the partitions in the list by clicking **Select All** and then clicking **Delete Selected**.

A message displays that states that you cannot undo this action.

Step 4 To delete the partition, click **OK** or to cancel the deletion, click **Cancel**.

Caution Before initiating this action, check carefully to ensure that you are deleting the correct partition. You cannot retrieve deleted partitions. If a partition is accidentally deleted, you must rebuild it.

Tip You can also delete a partition by locating and displaying the partition that you want to delete and clicking **Delete**.

Additional Information

See the "Related Topics" section on page 52-7.

Related Topics

- Partition Configuration Settings, page 52-1
- Finding a Partition, page 52-3
- Configuring a Partition, page 52-4
- Synchronizing a Partition With Affected Devices, page 52-5
- Deleting a Partition, page 52-6
- Searching for a Partition, page 52-5
- Local Route Groups, *Cisco Unified Communications Manager Features and Services Guide*

CHAPTER 53

Calling Search Space Configuration

Use the following topics to find, add, update, copy, or delete a calling search space:

Calling Search Space Configuration Settings

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, refer to "Partitions and Calling Search Spaces" in the *Cisco Unified Communications Manager System Guide*.

Table 53-1 describes the calling search space configuration settings. For related procedures, see the "Related Topics" section on page 53-5.

Table 53-1 Calling Search Space Configuration 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.

Table 53-1 Calling Search Space Configuration Settings (continued)

Field	Description
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 (_).
Route Partitions for this Calling Search Space	
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. Table 53-2 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.

Table 53-2 provides examples of the maximum number of partitions that can be added to a calling search space if partition names are of fixed length. Refer to "Partition Name Limitations" in the *Cisco Unified Communications Manager System Guide* for details about how this maximum number is calculated.

Table 53-2 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

Additional Topics

See the "Related Topics" section on page 53-5.

Finding a Calling Search Space

Because you might have several calling search spaces in your network, Cisco Unified Communications Manager lets you locate specific calling search spaces by using specific criteria as the basis. Use the following procedure to locate calling search spaces.

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

Procedure

Step 1 Choose **Call Routing** > **Class of Control** > **Calling Search Space**.

The Find and List Calling Search Spaces window displays.

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records:

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

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

Step 3 Click **Find**.

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

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

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

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

The window displays the item that you choose.

Additional Topics

See the "Related Topics" section on page 53-5.

Configuring a Calling Search Space

The following procedure describes how to copy, add, and update a calling search space.

Procedure

Step 1 In the menu bar, choose **Call Routing** > **Class of Control** > **Calling Search Space**.

Step 2 Perform one of the followings tasks:

- To copy an existing calling search space, locate the appropriate calling search space as described in "Finding a Calling Search Space" section on page 53-3. Click the **Copy** icon next to the calling search space that you want to copy. The window displays the copy of the calling search space. Change the Calling Search Space Name, and continue with Step 3.
- To add a calling search space, click the **Add New** button, and continue with Step 3.
- To update an existing calling search space, locate the appropriate calling search space as described in "Finding a Calling Search Space" section on page 53-3, and continue with Step 3.

Step 3 Enter the appropriate settings as described in Table 53-1.

Step 4 Click **Save**.

Additional Topics

See the "Related Topics" section on page 53-5.

Deleting a Calling Search Space

The following procedure describes how to delete a calling search space.

Before You Begin

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. For more information about dependency records, refer to the "Accessing Dependency Records" section on page A-2. 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. Refer to the "Directory Number Configuration" section on page 64-1 and the "Configuring a Translation Pattern" section on page 60-10.
- Delete the devices, lines, or translation patterns that are using the calling search space that you want to delete. Refer to the "Removing a Directory Number from a Phone" section on page 64-28, and the "Deleting a Translation Pattern" section on page 60-11.

Procedure

Step 1 In the menu bar, choose **Call Routing > Class of Control > Calling Search Space**.

Step 2 Locate the calling search space that you want to delete. See the "Finding a Calling Search Space" section on page 53-3.

Step 3 Check the check box of the calling search space that you want to delete and click **Delete Selected**.

A message displays that states that you cannot undo this action.

Step 4 To delete the calling search space, Click **OK** or click **Cancel**.

Caution Before initiating this action, check carefully to ensure that you are deleting the correct calling search space. You cannot retrieve deleted calling search spaces. If a calling search space is accidentally deleted, you must rebuild it.

Tip You can also delete a calling search space by locating and displaying the calling search space that you want to delete and clicking **Delete**.

Additional Topics

See the "Related Topics" section on page 53-5.

Related Topics

- Calling Search Space Configuration Settings, page 53-1
- Finding a Calling Search Space, page 53-3
- Configuring a Calling Search Space, page 53-4
- Deleting a Calling Search Space, page 53-4
- Local Route Groups, *Cisco Unified Communications Manager Features and Services Guide*

CHAPTER 54

Intercom Partition Configuration

An intercom partition contains a list of route patterns [directory number (DN) and route patterns]. Partitions facilitate call routing by dividing the route plan into logical subsets that are based on organization, location, and call type. For more information about partitions, refer to "Partitions and Calling Search Spaces" in the *Cisco Unified Communications Manager System Guide*.

For more information about intercom partitions, refer to the "Intercom" chapter in the *Cisco Unified Communications Manager Features and Services Guide.*

CHAPTER 55

Intercom Calling Search Space Configuration

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, refer to "Partitions and Calling Search Spaces" in the *Cisco Unified Communications Manager System Guide*. For more information about intercom and intercom calling search spaces, refer to the "Intercom" chapter in the *Cisco Unified Communications Manager Features and Services Guide.*

CHAPTER 56

Intercom Directory Number Configuration

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, refer to the "Intercom" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

CHAPTER 57

Intercom Translation Pattern Configuration

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, refer to the "Intercom" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

CHAPTER 58

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 "Client Matter Codes and Forced Authorization Codes" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Additional Cisco Documentation

- *Cisco Unified Communications Manager Bulk Administration Guide*
- *Cisco Unified Serviceability Administration Guide*

CHAPTER 59

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 "Client Matter Codes and Forced Authorization Codes" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Additional Cisco Documentation

- *Cisco Unified Communications Manager Bulk Administration Guide*
- *Cisco Unified Serviceability Administration Guide*

CHAPTER 60

Translation Pattern Configuration

Use the following topics to add, update, copy, or delete a translation pattern:

- Translation Pattern Configuration Settings, page 60-1
- Finding a Translation Pattern, page 60-9
- Configuring a Translation Pattern, page 60-10
- Deleting a Translation Pattern, page 60-11

Translation Pattern Configuration Settings

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.

Table 60-1 describes the available fields in the Translation Pattern Configuration window. For related procedures, see the "Related Topics" section on page 60-12.

Table 60-1 Translation Pattern Configuration 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.

Table 60-1 Translation Pattern Configuration Settings (continued)

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. Find and choose a partition name (see the "Finding a Partition" section on page 52-3). **Note** To set the maximum list box items, choose **System > Enterprise Parameters** and choose **CCMAdmin Parameters**. **Note** 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.
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. Refer to the "Wildcards and Special Characters in Route Patterns and Hunt Pilots" section in the *Cisco Unified Communications Manager System Guide* and the "Route Filter Configuration Settings" section on page 41-1 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 **OK**. **Note** To set the maximum list box items, choose **System > Enterprise Parameters** and choose **CCMAdmin Parameters**.

Table 60-1 Translation Pattern Configuration Settings (continued)

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** Refer to the "Precedence" section in the "Multilevel Precedence and Preemption" chapter of 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.
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 (see the "Finding a Calling Search Space" section on page 53-3). **Note** To set the maximum list box items, choose **System** > **Enterprise Parameters** and choose **CCMAdmin Parameters**.
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

Table 60-1 Translation Pattern Configuration Settings (continued)

Field	Description
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.
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 NANP 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. Refer to the "Adding a Route List" section on page 43-2 for more detailed information.
Prefix Digits (Outgoing Calls)	Enter prefix digits. Valid entries for the NANP 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.

Table 60-1 Translation Pattern Configuration Settings (continued)

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 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 Table 17-8 in the "Calling Party Number Transformations Settings" section 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 the "Configuring a Device Profile" section on page 97-8 and Table 91-1 in the "Configuring Speed-Dial Buttons or Abbreviated Dialing" section on page 91-34 for information about the Ignore Presentation Indicators (internal calls only) field. For more information about call display restrictions, refer to the Call Display Restrictions chapter in the *Cisco Unified Communications Manager Features and Services Guide.*
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 Table 17-8 in the "Calling Party Number Transformations Settings" section in the *Cisco Unified Communications Manager System Guide*.

Table 60-1 Translation Pattern Configuration Settings (continued)

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 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 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.

Table 60-1 Translation Pattern Configuration Settings (continued)

Field	Description
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. For more information about this field, see Table 17-11 in the "Connected Party Presentation and Restriction Settings" section in the *Cisco Unified Communications Manager System Guide*.
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 Table 17-11 in the "Connected Party Presentation and Restriction Settings" section 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. Refer to the "Discard Digits Instructions" section 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 NANP 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.

Table 60-1 Translation Pattern Configuration Settings (continued)

Field	Description
Prefix Digits (Outgoing Calls)	Enter prefix digits. Valid entries for the NANP 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.
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.

Table 60-1 Translation Pattern Configuration Settings (continued)

Field	Description
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.

Additional Information

See the "Related Topics" section on page 60-12.

Finding a Translation Pattern

Because you might have several translation patterns in your network, Cisco Unified Communications Manager lets you locate specific translation patterns by using specific criteria as the basis. Use the following procedure to locate translation patterns.

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

Procedure

Step 1 Choose **Call Routing > Translation Pattern**.

The Find and List Translation Patterns 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.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 60-12.

Configuring a Translation Pattern

This section describes how to configure a translation pattern.

Before You Begin

Configure the following Cisco Unified Communications Manager items before configuring a translation pattern:

- Partition
- Route filter
- Calling search space
- Resource-Priority Namespace Network Domain

Procedure

Step 1 Choose **Call Routing** > **Translation Pattern**.

The Find and List Translation Patterns window displays.

Step 2 Perform one of the followings tasks:

- To copy an existing translation pattern, locate the appropriate translation pattern as described in the "Finding a Translation Pattern" section on page 60-9, click the **Copy** button next to the translation pattern that you want to copy, and continue with Step 3.
- To add a new translation pattern, click the **Add New** button, and continue with Step 3.
- To update an existing translation pattern, locate the appropriate translation pattern as described in the "Finding a Phone" section on page 91-26, and continue with Step 3.

Step 3 In the Translation Pattern Configuration window that displays, enter the appropriate configuration settings as described in Table 60-1.

Step 4 Click **Save**.

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.

The Translation Pattern Configuration window displays the newly configured translation pattern.

Additional Information

See the "Related Topics" section on page 60-12.

Deleting a Translation Pattern

This section describes how to delete a translation pattern.

Procedure

Step 1 Choose **Call Routing** > **Translation Pattern**.

Step 2 Locate the translation pattern that you want to delete. See the "Finding a Translation Pattern" section on page 60-9.

Step 3 Check the check box of the translation pattern that you want to delete and click **Delete Selected**.

A message displays that states that you cannot undo this action.

Step 4 To delete the translation pattern, click **OK** or to cancel the deletion, click **Cancel**.

Caution 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.

Tip

You can also delete a translation pattern by locating and displaying the translation pattern that you want to delete and clicking **Delete**.

Additional Information

See the "Related Topics" section on page 60-12.

Related Topics

- Translation Pattern Configuration Settings, page 60-1
- Finding a Translation Pattern, page 60-9
- Configuring a Translation Pattern, page 60-10
- Deleting a Translation Pattern, page 60-11
- Understanding Route Plans, *Cisco Unified Communications Manager System Guide*
- Configuring a Resource Priority Namespace Network Domain, page 21-3
- Configuring a Resource Priority Namespace List, page 22-3

CHAPTER 61

Call Park

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, refer to the Call Park and Directed Call Park chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

CHAPTER 62

Directed Call Park

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, refer to the Call Park and Directed Call Park chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

CHAPTER 63

Call Pickup Group Configuration

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, refer to the Call Pickup chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

CHAPTER 64

Directory Number Configuration

The following sections provide information about working with and configuring directory numbers (DNs) in Cisco Unified Communications Manager Administration:

Directory Number Configuration Settings

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.
- 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.

Table 64-1 describes the fields that are available in the Directory Number Configuration window. For related procedures, see the "Related Topics" section on page 64-30.

Note 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 SEPXXXXXXXXXXXX,” 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 are changed, the new settings will apply to all the shared lines.

Table 64-1 Directory Number Configuration 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.
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. Find and choose a partition name (see the “Finding a Partition” section on page 52-3). **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.

Table 64-1 Directory Number Configuration Settings (continued)

Field	Description
Alerting Name	Enter a name that you want to display on the phone of the caller. This setting, which supports the Identification Services for the QSIG protocol, applies to shared and nonshared directory numbers. If you configure an alerting name for a directory number with shared-line appearances, when the phone rings at the terminating PINX, the system performs the following tasks: • Forwards the name of the caller that is assigned to the directory number. • Applies the Connected Name Restrictions (CONR) that are configured for the translation pattern (if restrictions exist); the originating PINX may modify the CONR, depending on the route pattern configuration. If you do not configure an alerting name, “Name Not Available” may display on the caller phone. If you do not enter a name for the Display (Internal Caller ID) field, the information in the Alerting Name field displays in the Display (Internal Caller ID) field. Setting the Always Display Original Dialed Number service parameter to True impacts the alerting name functionality. If you set the service parameter to True, the alerting name does not display on the calling phone; only the original dialed number displays.
ASCII Alerting Name	This field provides the same information as the *Alerting Name* field, but you must limit input to ASCII characters. Devices that do not support Unicode (internationalized) characters display the content of the *Alerting Name ASCII* field.
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.
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. See the “Line Group Configuration” section on page 45-1 for more information about configuring line groups. **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.

Table 64-1 Directory Number Configuration Settings (continued)

Field	Description
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. See the "Cisco Unified IP Phone Configuration" chapter or the "Device Profile Configuration" chapter for more information about configuring phones or device profiles. 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.

Table 64-1 Directory Number Configuration Settings (continued)

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. For configuration information about calling search space for directory numbers, see the "Calling Search Space" section on page 64-23. 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, refer to Partitions and Calling Search Spaces, in the *Cisco Unified Communications Manager System Guide*.
Presence Group	Configure this field with the Presence feature. From the drop-down list box, choose a 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 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. Refer to the "Presence" chapter in the *Cisco Unified Communications Manager Features and Services 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.

Table 64-1 Directory Number Configuration Settings (continued)

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.
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.

Table 64-1 Directory Number Configuration Settings (continued)

Field	Description
Call Forward and Call Pickup Settings	
Calling Search Space Activation Policy	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.

Table 64-1 Directory Number Configuration Settings (continued)

Field	Description
	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 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. See Service Parameters Configuration for information on accessing and configuring service parameters. **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.

Table 64-1 Directory Number Configuration Settings (continued)

Field	Description
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.
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 field, Calling Search Space, page 64-5, for information about how the combination of Primary and Secondary CFA CSSs works

Table 64-1 Directory Number Configuration Settings (continued)

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 Busy Trigger, page 64-22 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. See 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.

Table 64-1 Directory Number Configuration Settings (continued)

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 Busy Trigger, page 64-22 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.

Table 64-1 Directory Number Configuration Settings (continued)

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.

Table 64-1 Directory Number Configuration Settings (continued)

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.

Table 64-1 Directory Number Configuration Settings (continued)

Field	Description
Forward No Coverage Internal	For complete information about Call Coverage, see Call Coverage in 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.

Table 64-1 Directory Number Configuration Settings (continued)

Field	Description
Forward No Coverage External	For complete information about Call Coverage, see Call Coverage in 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.

Table 64-1 Directory Number Configuration Settings (continued)

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. See the "Service Parameters Configuration" section on page 25-1.
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. See the "Service Parameters Configuration" section on page 25-1.
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	
Park Monitoring Forward No Retrieve Destination External	This release of Cisco Unified Communications Manager does not support this setting.
Park Monitoring Forward No Retrieve Destination Internal	This release of Cisco Unified Communications Manager does not support this setting.

Table 64-1 Directory Number Configuration Settings (continued)

Field	Description
Park Monitoring Reversion Timer	This release of Cisco Unified Communications Manager does not support this setting.
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. For configuration information about calling search space for directory numbers, see the "Calling Search Space" section on page 64-23.
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.
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.
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.
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.

Table 64-1 Directory Number Configuration Settings (continued)

Field	Description
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 alphanumeric 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.)
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.)
ASCII Line Text Label	This field provides the same information as the *Line Text Label* field, but you must limit input to ASCII characters. Devices that do not support Unicode (internationalized) characters display the content of the *ASCII Line Text Label* 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.)
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.)

Table 64-1 Directory Number Configuration Settings (continued)

Field	Description
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.)
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.

Table 64-1 Directory Number Configuration Settings (continued)

Field	Description
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.
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.

Table 64-1 Directory Number Configuration Settings (continued)

Field	Description
Recording Option	This field determines the recording option on the line appearance of an agent. By default, the recording option specifies *Call Recording Disabled*. Choose one of the following options: • Call Recording Disabled—The calls that the agent makes on this line appearance are not recorded. • Automatic Call Recording Enabled—The calls that the agent makes on this line appearance are automatically recorded. • Application Invoked Call Recording Enabled—The calls that the agent makes on this line appearance are recorded if an application invokes calling recording. When the recording option is set to either Automatic Call Recording Enabled or Application Invoked Call Recording Enabled, the line appearance can be associated with a recording profile. When automatic recording is enabled, the application recording requests get 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.
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.
Logged 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.

Table 64-1 Directory Number Configuration Settings (continued)

Field	Description
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** To review how this setting works for devices with shared line appearances, refer 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, refer to "Shared Line Appearance" in the *Cisco Unified Communications Manager System Guide*.
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.

Table 64-1 Directory Number Configuration Settings (continued)

Field	Description
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. Refer to "Finding an End User" section on page 114-8 for more information about finding end users. 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.

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**.

Additional Topic

See the "Related Topics" section on page 64-30.

Finding a Directory Number

Use the following procedure to find a directory number (DN).

Procedure

Step 1 Choose **Call Routing** > **Directory Number**. Records from an active (prior) query may also display in the window.

The Find and List Directory Numbers window displays.

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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.

Additional Topics

See the "Related Topics" section on page 64-30.

Configuring a Directory Number

Follow these instructions to add or update a directory number (DN). You can configure the call forward, call pickup, and MLPP phone features while you are adding the directory number.

Tip You can assign patterns to 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.

For information on how to configure Private Line Automatic Ringdown (PLAR), see the "Configuring Private Line Automatic Ringdown (PLAR)" section on page 64-27.

Procedure

Step 1 Choose **Call Routing** > **Directory Number**.

The Find and List Directory Numbers window displays.

Step 2 To locate a specific directory number, enter search criteria and click **Find**.

A list of directory numbers that match the search criteria displays.

Step 3 Perform one of the followings tasks:

- To add a directory number, click the **Add New** button to add a new directory number. The Directory Number Configuration window displays.

  Note The Phone Configuration window provides an alternate method for adding a directory number. Use the **Device** > **Phone** menu option and create a new phone or search for an existing phone. After you create the new phone or display the existing phone, click either the *Line [1] - Add a new DN* or *Line [2] - Add a new DN* link in the Association Information area on the left side of the Phone Configuration window. The Directory Number Configuration window displays, and you can continue with Step 4 of this procedure.

- To update a directory number, click the directory number that you want to update. The Directory Number Configuration window displays.

Step 4 Update the appropriate settings as described in Table 64-1.

Step 5 Click **Save**.

Note Refer to the "Synchronizing a Directory Number With Affected Devices" section on page 64-26 before deciding whether to proceed to Step 6 below.

Step 6 Click **Reset Phone**. For more information, refer to the "Resetting a Phone" section on page 91-32.

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.

Additional Topics

See the "Related Topics" section on page 64-30.

Synchronizing a Directory Number With Affected Devices

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

Procedure

Step 1 Choose **Call Routing** > **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**.

Additional Information

See the "Related Topics" section on page 64-30.

Configuring 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.

The following example 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. To enable PLAR functionality from A/A', see the following example:

Tip Step 1 through Step 4 apply if you want to configure PLAR for phones that are running SCCP. For phones that are running SIP, you must perform Step 1 through Step 6. Before you attempt to configure PLAR, verify that your phone model supports PLAR. To determine whether your phone supports PLAR, refer to the *Cisco Unified IP Phone Administration Guide* that supports your phone model and this release of Cisco Unified Communications Manager.

Example for How to Configure PLAR

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.)

Removing a Directory Number from a 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. For more information about dependency records, refer to the "Accessing Dependency Records" section on page A-2.

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. For more information, refer to the "Deleting Unassigned Directory Numbers" section on page 67-2.

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**. For more information, refer to the "Resetting a Phone" section on page 91-32.

Additional Topics

See the "Related Topics" section on page 64-30.

Creating a 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, refer to 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. Refer to Cisco Unity and Cisco Unity Connection Configuration Checklist in the *Cisco Unified Communications Manager System Guide*.
- You must configure Cisco Unity Connection servers. Refer to 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. Refer to 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, refer to 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 64-1.

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. Refer to the applicable *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

Additional Topics

See the "Related Topics" section on page 64-30.

Related Topics

- Directory Number Configuration Settings, page 64-1
- Finding a Directory Number, page 64-24
- Configuring a Directory Number, page 64-25
- Synchronizing a Directory Number With Affected Devices, page 64-26
- Configuring Private Line Automatic Ringdown (PLAR), page 64-27
- Removing a Directory Number from a Phone, page 64-28
- Creating a Cisco Unity Connection Voice Mailbox, page 64-29
- Directory Number Configuration Settings, page 64-1
- Understanding Directory Numbers, *Cisco Unified Communications Manager System Guide*
- Directory Number Configuration Checklist, *Cisco Unified Communications Manager System Guide*
- Line Group Configuration, page 45-1
- Deleting Unassigned Directory Numbers, page 67-2
- Gateway Configuration, page 90-1
- Resetting a Phone, page 91-32
- Finding a Phone, page 91-26
- Configuring Cisco Unified IP Phones, page 91-27
- Cisco Unified IP Phones, *Cisco Unified Communications Manager System Guide*
- Phone Features, *Cisco Unified Communications Manager System Guide*
- Cisco Unity and Cisco Unity Connection Configuration Checklist, *Cisco Unified Communications Manager System Guide*
- *User Moves, Adds, and Changes Guide for Cisco Unity Connection*
- Presence, *Cisco Unified Communications Manager Features and Services Guide*

CHAPTER 65

Meet-Me Number/Pattern Configuration

This section contains information on the following topics:

Meet-Me Number/Pattern Configuration Settings

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.

Before You Begin

Make sure that the following prerequisites are met before you configure Meet-Me numbers/patterns:

- Configure the server(s). Refer to the "Server Configuration" section on page 2-1.
- Configure the device pools. Refer to the "Device Pool Configuration" section on page 9-1.

Table 65-1 describes the meet-me number/pattern configuration settings. For related procedures, see the "Related Topics" section on page 65-5.

Table 65-1 Meet-Me Number/Pattern Configuration 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	Enter up to 30 alphanumeric characters for a description of the meet-me number/pattern.

Table 65-1 Meet-Me Number/Pattern Configuration Settings (continued)

Field	Description
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. Refer to the "Partition Configuration" section on page 52-1 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 (see the "Finding a Partition" section on page 52-3). **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. Refer to the *Cisco Unified Communications Manager Security Guide* for more information.

Additional Topics

See the "Related Topics" section on page 65-5.

Finding a Meet-Me Number/Pattern

Because you might have several meet-me numbers/patterns in your network, Cisco Unified Communications Manager lets you locate specific meet-me numbers/patterns on the basis of specific criteria. Use the following procedure to locate meet-me numbers/patterns.

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

Procedure

Step 1 Choose **Call Routing** > **Meet-Me Number/Pattern**.

The Find and List Meet-Me Numbers 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.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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.

Additional Topics

See the "Related Topics" section on page 65-5.

Configuring a Meet-Me Number/Pattern

This section describes how to add, copy and update a Meet-Me Number/Pattern.

Before You Begin

Make sure that the following prerequisites are met before proceeding with the steps:

- Configure the server(s). Refer to the "Server Configuration" section on page 2-1.
- Configure the device pools. Refer to the "Device Pool Configuration" section on page 9-1.

Procedure

Step 1 Choose **Call Routing** > **Meet-Me Number/Pattern**.

Step 2 Perform one of the followings tasks:

- To copy an existing Meet-Me Number/Pattern, locate the appropriate Meet-Me Number/Pattern as described in "Finding a Meet-Me Number/Pattern" section on page 65-2. Click the Meet-Me Number/Pattern that you want to copy. The Meet-Me Number/Pattern Configuration window displays. Click **Copy** and continue with Step 3.
- To add a Meet-Me Number/Pattern, click the **Add New** button and continue with Step 3.
- To update an existing Meet-Me Number/Pattern, locate the appropriate Meet-Me Number/Pattern as described in "Finding a Meet-Me Number/Pattern" section on page 65-2. Click the Meet-Me Number/Pattern that you want to update, and continue with Step 3.

Note You can change the number or pattern as needed (example, changing 5000 to 500X).

Step 3 Enter the appropriate settings as described in Table 65-1.

Step 4 Click **Save**.

Additional Topics

See the "Related Topics" section on page 65-5.

Deleting a Meet-Me Number/Pattern

This section describes how to delete a Meet-Me Number/Pattern.

Before You Begin

Make sure that the following prerequisites are met before proceeding with the steps:

- Configure the servers.
- Configure the device pools.
- Configure the meet-me number/pattern.

Procedure

Step 1 Find the meet-me number/pattern by using the procedure in the "Finding a Meet-Me Number/Pattern" section on page 65-2.

Step 2 Click the Meet-Me Number/Pattern that you want to delete.

Step 3 Click **Delete**.

Additional Topics

See the "Related Topics" section on page 65-5.

Related Topics

- Meet-Me Number/Pattern Configuration Settings, page 65-1
- Finding a Meet-Me Number/Pattern, page 65-2
- Configuring a Meet-Me Number/Pattern, page 65-4
- Deleting a Meet-Me Number/Pattern, page 65-4
- Partition Configuration, page 52-1
- Configuring a Conference Device, page 73-16
- Synchronizing a Conference Device, page 73-17
- Deleting a Conference Device, page 73-17
- Conference Bridges, *Cisco Unified Communications Manager System Guide*

CHAPTER 66

Dial Plan Installer

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.

This chapter describes how to install a dial plan on a Cisco Unified Communications Manager server.

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 at the following URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/IDP50

For details on installing a COP file, see the *Cisco Unified Communications Manager Dial Plan Guide*.

For details on how to install a dial plan from this location, see "Installing a Dial Plan on Cisco Unified Communications Manager" section on page 66-3.

Use the following procedures to find and install dial plans on Cisco Unified Communications Manager.

- Finding a Dial Plan, page 66-2
- Editing a Dial Plan, page 66-3
- Installing a Dial Plan on Cisco Unified Communications Manager, page 66-3
- Configuring Route Pattern Details for a non-NANP Dial Plan, page 66-4
- Upgrading a Dial Plan, page 66-4
- Uninstalling a Dial Plan, page 66-6
- Restarting the Cisco CallManager Service, page 66-6
- Related Topics, page 66-7

Finding a Dial Plan

Use the following procedure to find a dial plan on a Cisco Unified Communications Manager system.

Note During your work in a browser session, 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 open a new browser window, the system retains your Cisco Unified Communications Manager search preferences until you modify your search.

Procedure

Step 1 From the Cisco Unified Communications Manager Administration window, choose **Call Routing** > **Dial Plan Installer**.

The Find and List Dial Plans window displays.

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records

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

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

Step 3 Click **Find**.

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

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

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

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

The window displays the item that you choose.

Additional Information

See the "Related Topics" section on page 66-7.

Editing a 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 by using the procedure defined in the "Finding a Dial Plan" section on page 66-2

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:

- To install a dial plan, see the "Installing a Dial Plan on Cisco Unified Communications Manager" section on page 66-3.
- To upgrade a dial plan, see the "Upgrading a Dial Plan" section on page 66-4.
- To uninstall a dial plan, see the "Uninstalling a Dial Plan" section on page 66-6.

Additional Information

See the "Related Topics" section on page 66-7.

Installing a Dial Plan on Cisco Unified Communications Manager

Use the following procedure to install a dial plan.

Procedure

Step 1 Find the Dial Plan that you want to install by using the procedure that is defined in the "Finding a Dial Plan" section on page 66-2.

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 The dial plan name and description display in the Dial Plan and Description fields.

Step 4 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.

Step 5 Choose the dial plan version that you want to install from the Available Version drop-down list box.

Step 6 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 7 Repeat Step 1 to Step 6 to install the dial plans on all the nodes Cisco Unified Communications Manager cluster.

Note After installation of the dial plans, restart the Cisco CallManager service to load the dial plan.

Additional Information

See the "Related Topics" section on page 66-7.

Configuring Route Pattern Details for a 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:
   a. Choose None in the Discard Digits field. Choosing None DDI in the Discard Digits field represents the same as not choosing a dial plan.
   b. Choose a non-NANP dial plan:No Digits in the Discard Digits field. (For Example, AMNP:No Digits.)
2. 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.

Additional Information

See the "Related Topics" section on page 66-7.

Upgrading a 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.

Use the following procedure to upgrade an existing dial plan.

Procedure

Step 1 Find the Dial Plan that you want to upgrade by using the procedure that is defined in the "Finding a Dial Plan" section on page 66-2

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 The dial plan name and description display in the Dial Plan and Description fields.

Step 4 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.

Step 5 Choose the dial plan version that you want to upgrade from the Available Version drop-down list box.

Step 6 Click **Install**.

The Status displays that the dial plan has been upgraded.

The Installed Version field displays the latest dial plan version.

Step 7 Repeat Step 1 to Step 6 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. See the "Restarting the Cisco CallManager Service" section on page 66-6.

Note When dial plans are migrated from 4.x to 6.0, all configurations, such as route patterns, get retained; the dial plans do not display in the Find and List Dial Plans window. 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. See the "Installing a Dial Plan on Cisco Unified Communications Manager" section on page 66-3.

Note When you upgrade from 4.x to 6.0, to retain the dial plan and the dial plan configurations, such as route pattern/route filter associated for a dial plan, install the latest dial plans that are available on CCO.

Additional Information

See the "Related Topics" section on page 66-7.

Uninstalling a 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.

Use the following procedure to uninstall a dial plan.

Procedure

Step 1 Find the Dial Plan that you want to delete by using the procedure that is defined in the "Finding a Dial Plan" section on page 66-2.

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 The dial plan name and description display in the Dial Plan and Description fields.

Step 4 The Installed Version displays the current version that is installed on the Cisco Unified Communications Manager server.

Step 5 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 6 Repeat Step 1 to Step 5 to uninstall the dial plans on all nodes of the Cisco Unified Communications Manager cluster.

Additional Information

See the "Related Topics" section on page 66-7.

Restarting the 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.

Additional Information

See the "Related Topics" section on page 66-7.

Related Topics

- Finding a Dial Plan, page 66-2
- Editing a Dial Plan, page 66-3
- Installing a Dial Plan on Cisco Unified Communications Manager, page 66-3
- Configuring Route Pattern Details for a non-NANP Dial Plan, page 66-4
- Upgrading a Dial Plan, page 66-4
- Uninstalling a Dial Plan, page 66-6
- Restarting the Cisco CallManager Service, page 66-6
- *Cisco Unified Communications Manager Dial Plan Guide*

CHAPTER 67

Route Plan Report

The route plan report lists all assigned and unassigned directory numbers (DN), call park numbers, call pickup numbers, conference numbers, route patterns, translation patterns, message-waiting indicators, voice-mail ports, attendant console, pilot numbers, domain routing, IP routing, hunt pilot, directed call park, and intercom directory numbers in the system. 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 Pattern/Directory Number, Partition, or Route Detail fields.

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, refer to the "Understanding Route Plans" section in *Cisco Unified Communications Manager System Guide*.

Note Refer to the "Local Route Groups" chapter in the *Cisco Unified Communications Manager Features and Services Guide* for a discussion of the route plan report and its format when the Local Route Group feature is configured.

Use the following procedures to view route plan records:

- Viewing Route Plan Records, page 67-1
- Deleting Unassigned Directory Numbers, page 67-2
- Viewing Route Plan Reports in a File, page 67-3

Viewing 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.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 67-4.

Deleting Unassigned Directory Numbers

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 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**.

Additional Information

See the "Related Topics" section on page 67-4.

Updating 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.

Additional Information

See the "Related Topics" section on page 67-4.

Viewing Route Plan Reports in a File

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.

Related Topics

- Route Plan Report, page 67-1
- Viewing Route Plan Records, page 67-1
- Deleting Unassigned Directory Numbers, page 67-2
- Configuring a Directory Number, page 64-25
- Understanding Route Plans, *Cisco Unified Communications Manager System Guide*
- Local Route Groups, *Cisco Unified Communications Manager Features and Services Guide*

CHAPTER 68

Calling Party Transformation Pattern Configuration

Use the following topics to find, add, update, copy, or delete a calling party transformation pattern:

Calling Party Transformation Pattern Configuration Settings

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, refer to Calling Party Normalization in the *Cisco Unified Communications Manager Features and Services Guide*.

Note Refer to the "Local Route Groups" chapter 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.

Table 68-1 describes the calling party transformation pattern configuration settings. For related procedures, see the "Related Topics" section on page 68-7.

Table 68-1 Calling Party Transformation Pattern Configuration 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 the "Wildcards and Special Characters in Route Patterns and Hunt Pilots" section 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. See the "Partition Configuration" section on page 52-1 for more information on how to use partitions. 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 Finding a Partition procedure in the *Cisco Unified Communications Manager Administration Guide*. **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.

Table 68-1 Calling Party Transformation Pattern Configuration Settings (continued)

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. Find and choose a route filter name by using the Finding a Route Filter procedure in the *Cisco Unified Communications Manager Administration Guide*. **Note** To set the maximum list box items, choose **System > Enterprise Parameters** and choose **CCMAdmin Parameters**.
Urgent Priority	Cisco Unified Communications Manager sets all calling party transformation patterns with urgent priority, and you cannot change the priority of the patterns.
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 Digits Instructions	Choose the discard digits 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 for the NANP include the digits 0 through 9; the wildcard characters X, asterisk (*), and octothorpe (#); and the international escape character +. If the Discard Digits 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 for the NANP 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.

Table 68-1 Calling Party Transformation Pattern Configuration Settings (continued)

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 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.

Table 68-1 Calling Party Transformation Pattern Configuration Settings (continued)

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.

Additional Topics

See the "Related Topics" section on page 68-7.

Finding a Calling Party Transformation Pattern

Because you might have several calling party transformation patterns in your network, Cisco Unified Communications Manager lets you locate specific calling party transformation patterns by using specific criteria as the basis. Use the following procedure to locate calling party transformation patterns.

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

Procedure

Step 1 Choose **Call Routing** > **Transformation Pattern** > **Calling Party Transformation Pattern**.

The Find and List Calling Party Transformation Patterns window displays.

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records

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

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

Step 3 Click **Find**.

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

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

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

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

The window displays the item that you choose.

Additional Topics

See the "Related Topics" section on page 68-7.

Configuring a Calling Party Transformation Pattern

To configure a calling party transformation pattern, perform the following procedure.

Procedure

Step 1 Choose **Call Routing** > **Transformation Pattern** > **Calling Party Transformation Pattern**.

The Find and List Calling Party Transformation Patterns window displays.

Step 2 Perform one of the followings tasks:

- To copy an existing calling party transformation pattern, locate the appropriate calling party transformation pattern as described in the "Finding a Calling Party Transformation Pattern" section on page 68-5, click the **Copy** button next to the calling party transformation pattern that you want to copy, and continue with Step 3.
- To add a new calling party transformation pattern, click the **Add New** button and continue with Step 3.

- To update an existing calling party transformation pattern, locate the appropriate transformation pattern as described in the "Finding a Calling Party Transformation Pattern" section on page 68-5, and continue with Step 3.

Step 3 In the Calling Party Transformation Pattern Configuration window that displays, enter the appropriate configuration settings as described in Table 68-1.

Step 4 Click **Save**.

Additional Topics

See the "Related Topics" section on page 68-7.

Deleting a Calling Party Transformation Pattern

To delete a calling party transformation pattern, perform the following procedure.

Procedure

Step 1 Locate the calling party transformation pattern that you want to delete, as described in the "Finding a Calling Party Transformation Pattern" section on page 68-5.

Step 2 Click **Delete**.

Step 3 Click **OK**.

Additional Topics

See the "Related Topics" section on page 68-7.

Related Topics

- Calling Party Transformation Pattern Configuration Settings, page 68-1
- Finding a Calling Party Transformation Pattern, page 68-5
- Configuring a Calling Party Transformation Pattern, page 68-6
- Deleting a Calling Party Transformation Pattern, page 68-7
- Finding a Route Filter, page 41-2
- Partition Configuration, page 52-1
- Calling Party Number Transformations Settings, *Cisco Unified Communications Manager System Guide*
- Wildcards and Special Characters in Route Patterns and Hunt Pilots, *Cisco Unified Communications Manager System Guide*
- Calling Party Normalization, *Cisco Unified Communications Manager Features and Services Guide*
- Local Route Groups, *Cisco Unified Communications Manager Features and Services Guide*

CHAPTER 69

Called Party Transformation Pattern Configuration

Use the following topics to find, add, update, copy, or delete a called party transformation pattern:

Called Party Transformation Pattern Configuration Settings

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 Refer to the Local Route Groups chapter 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.

Table 69-1 describes the called party transformation pattern configuration settings. For related procedures, see the "Related Topics" section on page 69-7.

Table 69-1 Called Party Transformation Pattern Configuration 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 the "Wildcards and Special Characters in Route Patterns and Hunt Pilots" section 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. See the "Partition Configuration" section on page 52-1 for more information on how to use partitions. 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 Finding a Partition procedure in the *Cisco Unified Communications Manager Administration Guide*. **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.
Numbering Plan	Choose a numbering plan.

Table 69-1 Called Party Transformation Pattern Configuration Settings (continued)

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. Find and choose a route filter name by using the Finding a Route Filter procedure in the *Cisco Unified Communications Manager Administration Guide*. **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 for the NANP 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 for the NANP 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.

Table 69-1 Called Party Transformation Pattern Configuration Settings (continued)

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.

Additional Topics

See the "Related Topics" section on page 69-7.

Finding a Called Party Transformation Pattern

Because you might have several called party transformation patterns in your network, Cisco Unified Communications Manager lets you locate specific called party transformation patterns by using specific criteria as the basis. Use the following procedure to locate called party transformation patterns.

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

Procedure

Step 1 Choose **Call Routing > Transformation Pattern > Called Party Transformation Pattern**.

The Find and List Called Party Transformation Patterns window displays.

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records

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

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

Step 3 Click **Find**.

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

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

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

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

The window displays the item that you choose.

Additional Topics

See the "Related Topics" section on page 69-7.

Configuring a Called Party Transformation Pattern

To configure a called party transformation pattern, perform the following procedure.

Procedure

Step 1 Choose **Call Routing** > **Transformation Pattern** > **Called Party Transformation Pattern**.

The Find and List Called Party Transformation Patterns window displays.

Step 2 Perform one of the followings tasks:

- To copy an existing called party transformation pattern, locate the appropriate called party transformation pattern as described in the "Finding a Called Party Transformation Pattern" section on page 69-5, click the **Copy** button next to the called party transformation pattern that you want to copy, and continue with Step 3.
- To add a new called party transformation pattern, click the **Add New** button, and continue with Step 3.
- To update an existing called party transformation pattern, locate the appropriate transformation pattern as described in the "Finding a Called Party Transformation Pattern" section on page 69-5, and continue with Step 3.

Step 3 In the Called Party Transformation Pattern Configuration window that displays, enter the appropriate configuration settings as described in Table 69-1.

Step 4 Click **Save**.

Additional Topics

See the "Related Topics" section on page 69-7.

Deleting a Called Party Transformation Pattern

To delete a called party transformation pattern, perform the following procedure.

Procedure

Step 1 Locate the called party transformation pattern that you want to delete, as described in the "Finding a Called Party Transformation Pattern" section on page 69-5.

Step 2 Click **Delete**.

Step 3 Click **OK**.

Additional Topics

See the "Related Topics" section on page 69-7.

Related Topics

- Called Party Transformation Pattern Configuration Settings, page 69-1
- Finding a Called Party Transformation Pattern, page 69-5
- Configuring a Called Party Transformation Pattern, page 69-6
- Deleting a Called Party Transformation Pattern, page 69-6
- Finding a Route Filter, page 41-2
- Calling Party Number Transformations Settings, *Cisco Unified Communications Manager System Guide*
- Wildcards and Special Characters in Route Patterns and Hunt Pilots, *Cisco Unified Communications Manager System Guide*
- Partition Configuration, page 52-1
- Local Route Groups, *Cisco Unified Communications Manager Features and Services Guide*

CHAPTER 70

Mobility Configuration

Mobile Connect 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 cellular phone.

For more information on Mobile Connect and how to configure mobility settings for dual-mode phones, refer to the Cisco Unified Mobility chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

CHAPTER 71

Logical Partitioning Policy Configuration

The **Call Routing > Logical Partitioning Policy Configuration** menu option in Cisco Unified Communications Manager Administration allows configuration of logical partitioning policies for use with geographic locations and geographic location filters to provision logical partitioning.

For more information on how to use the Logical Partitioning Policy Configuration window, refer to the "Logical Partitioning" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

PART 4

Media Resource Configuration

CHAPTER 72

Annunciator Configuration

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.

Use the following topics to find and update annunciators:

- Annunciator Configuration Settings, page 72-1
- Finding an Annunciator, page 72-3
- Updating an Annunciator, page 72-4
- Resetting an Annunciator, page 72-5
- Synchronizing an Annunciator, page 72-5
- Related Topics, page 72-6

Annunciator Configuration Settings

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.

Before You Begin

Verify that you have activated the Cisco IP Voice Media Streaming Application service on the server where you plan to configure the annunciator.

Tip When you add a Cisco Unified Communications Manager server, the annunciator for the server will automatically get added to the database. After you activate the Cisco IP Voice Media Streaming Application service, the annunciator device registers with Cisco Unified Communications Manager. Verify whether the annunciator exists by using the "Finding an Annunciator" section on page 72-3.

Verify that you have completed the following tasks:

- Configured the appropriate servers
- Configured device pools

Table 72-1 describes the annunciator configuration settings. For more information about related procedures, see the "Related Topics" section on page 72-6.

Table 72-1 Annunciator Configuration 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.
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 more details about locations, see the "Location Configuration" section on page 17-1. For an explanation of location-based CAC across intercluster trunks, see "Location-Based Call Admission Control Over Intercluster Trunk" in the *Cisco Unified Communications Manager System Guide*.

Table 72-1 Annunciator Configuration Settings (continued)

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: • 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 "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, 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. Refer to "Trusted Relay Point" and its subtopics in the "Media Resource Management" chapter of the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.

Finding an Annunciator

Perform the following procedure to find an annunciator:

Procedure

Step 1 Choose **Media Resources** > **Annunciator**.

The Find and List Annunciators window displays.

To find a specific annunciator quickly, specify the search criteria by performing the following procedure.

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records

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

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

Step 3 Click **Find**.

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

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

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

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

The window displays the item that you choose.

Additional Information

See the "Related Topics" section on page 72-6.

Updating an Annunciator

This section describes how to update an annunciator.

Before You Begin

Before you update an annunciator, verify that you have completed the following tasks:

- Configured the appropriate servers
- Configured device pools

Procedure

Step 1 Choose **Media Resources** > **Annunciator**.

The Find and List Annunciators window displays.

Step 2 To update an annunciator, locate the appropriate annunciator as described in the "Finding an Annunciator" section on page 72-3.

Tip When you add a Cisco Unified Communications Manager server, the annunciator for the sever will automatically get added to the database. After you activate the Cisco IP Voice Media Streaming Application service, the annunciator device registers with Cisco Unified Communications Manager.

Step 3 Click the annunciator that you want to update and continue with Step 4.

Step 4 Enter the appropriate settings as described in Table 72-1.

Step 5 Click **Save**.

Step 6 Be sure the Cisco IP Voice Media Streaming Application service has been activated. For information on activating services, refer to the *Cisco Unified Serviceability Administration Guide*.

Additional Information

See the "Related Topics" section on page 72-6.

Accessing Dependency Records

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. For more information about dependency records, see the "Accessing Dependency Records" section on page A-2.

Resetting an Annunciator

To reset an annunciator, perform the following procedure:

Procedure

Step 1 Locate the annunciator by using the procedure in the "Finding an Annunciator" section on page 72-3.

Step 2 Click the annunciator that you want to reset.

Step 3 Click the **Reset** button.

Step 4 The Device Reset Window displays. To continue, click **Reset**.

Additional Information

See the "Related Topics" section on page 72-6.

Synchronizing an Annunciator

To synchronize an annunciator with the most recent configuration changes, perform the following procedure, which will apply any outstanding configuration settings in the least-intrusive manner possible. (For example, a reset/restart may not be required on some affected devices.)

Procedure

Step 1 Choose **Media Resources** > **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**.

Additional Information

See the "Related Topics" section on page 72-6.

Related Topics

- Annunciator Configuration Settings, page 72-1
- Finding an Annunciator, page 72-3
- Updating an Annunciator, page 72-4
- Accessing Dependency Records, page 72-5
- Resetting an Annunciator, page 72-5
- Synchronizing an Annunciator, page 72-5
- Dependency Records, *Cisco Unified Communications Manager Administration Guide*
- Multilevel Precedence and Preemption, *Cisco Unified Communications Manager Features and Services Guide*
- Annunciator, *Cisco Unified Communications Manager System Guide*
- Trusted Relay Point, *Cisco Unified Communications Manager System Guide*

CHAPTER 73

Conference Bridge Configuration

Use the following topics to configure conference bridges:

Configuration Settings

Finding, Configuring, Synchronizing or Deleting a Conference Bridge

Software Conference Bridge Configuration 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 (see the "Configuring a Server" section on page 2-5 for more information). 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.

Refer to the "Conference Bridges" chapter of the *Cisco Unified Communications Manager System Guide* for more information about conference bridges.

Table 73-1 describes the software conference bridge configuration settings. For related procedures, see the "Related Topics" section on page 73-18.

Table 73-1 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. See Common Device Configuration for more information.
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 more details about locations, see the "Location Configuration" section on page 17-1. For an explanation of location-based CAC across intercluster trunks, see "Location-Based Call Admission Control Over Intercluster Trunk" in the *Cisco Unified Communications Manager System Guide*.

Table 73-1 Software Conference Bridge Configuration Settings (continued)

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 "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 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. Refer to "Trusted Relay Point" and its subtopics in the "Media Resource Management" chapter of the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.

Additional Information

See the "Related Topics" section on page 73-18.

Hardware Conference Bridge Configuration 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.

Refer to the "Conference Bridges" chapter of the *Cisco Unified Communications Manager System Guide* for more information about conference bridges.

Before you configure a conference bridge, configure the device pools. See the "Deleting a Device Pool" section on page 9-13.

Table 73-2 describes the hardware conference bridge configuration settings. For related procedures, see the "Related Topics" section on page 73-18.

Table 73-2 Hardware Conference Bridge Configuration Settings

Field	Description
Conference Bridge Type	Choose **Cisco Conference Bridge Hardware**. For a description of this type, refer to the "Conference Bridge Types in Cisco Unified Communications Manager Administration" section of 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. See Common Device Configuration for more information.

Table 73-2 Hardware Conference Bridge Configuration Settings (continued)

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 more details about locations, see the "Location Configuration" section on page 17-1. For an explanation of location-based CAC across intercluster trunks, see "Location-Based Call Admission Control Over Intercluster Trunk" in the *Cisco Unified Communications Manager System Guide*.

Table 73-2 Hardware Conference Bridge Configuration Settings (continued)

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 "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 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. Refer to "Trusted Relay Point" and its subtopics in the "Media Resource Management" chapter of 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.

Additional Information

See the "Related Topics" section on page 73-18.

Cisco IOS Conference Bridge Configuration 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.

Before you configure a conference bridge, configure the device pools. See the "Deleting a Device Pool" section on page 9-13.

Refer to the "Conference Bridges" chapter of the *Cisco Unified Communications Manager System Guide* for more information about conference bridges.

Table 73-3 describes the Cisco IOS conference bridge configuration settings. For related procedures, see the "Related Topics" section on page 73-18.

Table 73-3 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, refer to the "Conference Bridge Types in Cisco Unified Communications Manager Administration" section of the *Cisco Unified Communications Manager System Guide*.
Conference Bridge Name	Enter the same name that exists in the gateway Command Line Interface (CLI).
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. See Common Device Configuration for more information.
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 more details about locations, see the "Location Configuration" section on page 17-1. For an explanation of location-based CAC across intercluster trunks, see "Location-Based Call Admission Control Over Intercluster Trunk" in the *Cisco Unified Communications Manager System Guide*.

Table 73-3 Cisco IOS Conference Bridge Configuration Settings (continued)

Field	Description
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. Refer to the *Cisco Unified Communications Manager Security Guide* for secure conference bridge configuration procedures.
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 "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 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. Refer to "Trusted Relay Point" and its subtopics in the "Media Resource Management" chapter of the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.

Additional Information

See the "Related Topics" section on page 73-18.

Cisco Video Conference Bridge Configuration 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.

Before you configure a conference bridge, configure the device pools. See the "Deleting a Device Pool" section on page 9-13.

Refer to the "Conference Bridges" chapter of the *Cisco Unified Communications Manager System Guide* for more information about conference bridges.

Table 73-4 describes the Cisco video conference bridge configuration settings. For related procedures, see the "Related Topics" section on page 73-18.

Table 73-4 Cisco Video Conference Bridge Configuration Settings

Field	Description
Conference Bridge Type	Choose **Cisco Video Conference Bridge (IPVC-35xx)**. For a description of this type, refer to "Conference Bridge Types in Cisco Unified Communications Manager Administration" in 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. See Common Device Configuration for more information.

Table 73-4 Cisco Video Conference Bridge Configuration Settings (continued)

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 more details about locations, see the "Location Configuration" section on page 17-1. For an explanation of location-based CAC across intercluster trunks, see "Location-Based Call Admission Control Over Intercluster Trunk" in the *Cisco Unified Communications Manager System Guide*.

Table 73-4 Cisco Video Conference Bridge Configuration Settings (continued)

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 "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 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. Refer to "Trusted Relay Point" and its subtopics in the "Media Resource Management" chapter of 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, refer to the documentation for the specific device that you are configuring or contact the manufacturer.

Additional Information

See the "Related Topics" section on page 73-18.

Cisco Conference Bridge (WS-SVC-CMM) Configuration 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.

Before you configure a conference bridge, configure the device pools. See the "Deleting a Device Pool" section on page 9-13.

Refer to the "Conference Bridges" chapter of the *Cisco Unified Communications Manager System Guide* for more information about conference bridges.

Table 73-5 describes the Cisco Conference Bridge (WS-SVC-CMM) configuration settings. For related procedures, see the "Related Topics" section on page 73-18.

Table 73-5 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, refer to "Conference Bridge Types in Cisco Unified Communications Manager Administration" in 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.
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. See Common Device Configuration for more information.

Table 73-5 Cisco Conference Bridge (WS-SVC-CMM) Configuration Settings (continued)

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 more details about locations, see the "Location Configuration" section on page 17-1. For an explanation of location-based CAC across intercluster trunks, see "Location-Based Call Admission Control Over Intercluster Trunk" in the *Cisco Unified Communications Manager System Guide*.

Table 73-5 Cisco Conference Bridge (WS-SVC-CMM) Configuration Settings (continued)

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 "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 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. Refer to "Trusted Relay Point" and its subtopics in the "Media Resource Management" chapter of 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	
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, refer to the documentation for the specific device that you are configuring or contact the manufacturer.

Finding a Conference Bridge

Because you may have several conference bridges in your network, Cisco Unified Communications Manager lets you locate specific conference bridges on the basis of specific criteria. Use the following procedure to locate conference bridges.

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

Procedure

Step 1 Choose **Media Resources > Conference Bridge**.

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

Step 2 To find all records in the database, ensure the Find dialog box is empty; go to Step 3.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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 criteria.

Step 3 Click **Find**.

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

Note You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking **Delete Selected**. You can delete all conference bridge records in the database 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.

Additional Information

See the "Related Topics" section on page 73-18.

Configuring a Conference Device

This section describes how to configure a conference device.

Before You Begin

Make sure that the following prerequisites are met before you proceed with the steps:

- Configure the device pools. See the "Deleting a Device Pool" section on page 9-13.

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. See the "Software Conference Bridge Configuration Settings" section on page 73-1.

- For software conference bridges, activate the Cisco IP Voice Media Streaming Application service. Refer to the *Cisco Unified Serviceability Administration Guide*.

Procedure

Step 1 Choose **Media Resources** > **Conference Bridge**.

Step 2 Perform one of the following tasks:

- To add a conference device, click **Add New.**
- To update a conference device, locate the conference bridge by using the procedure in the "Finding a Conference Bridge" section on page 73-15.

The Conference Bridge Configuration window displays.

Step 3 Enter the appropriate settings as described in the following sections:

- Software Conference Bridge Configuration Settings, page 73-1
- Hardware Conference Bridge Configuration Settings, page 73-3
- Cisco IOS Conference Bridge Configuration Settings, page 73-6
- Cisco Video Conference Bridge Configuration Settings, page 73-9
- Cisco Conference Bridge (WS-SVC-CMM) Configuration Settings, page 73-12

Step 4 Click **Save**.

Note See the procedure described in "Synchronizing a Conference Device" section on page 73-17 before deciding on whether to proceed to Step 5.

Step 5 To reset the conference bridge device and apply your changes, click **Reset**.

The Device Reset window displays.

Step 6 Click **Reset** and close the window.

Additional Information

See the "Related Topics" section on page 73-18.

Synchronizing a Conference Device

To synchronize a conference device with the most recent configuration changes, perform the following procedure, which will apply any outstanding configuration settings in the least-intrusive manner possible. (For example, a reset/restart may not be required on some affected devices.)

Procedure

Step 1 Choose **Media Resources > 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**.

Additional Information

See the "Related Topics" section on page 73-18.

Deleting a Conference Device

This section describes how to delete a conference device. You cannot delete Cisco Unified Communications Manager Conference Bridge Software. See the "Configuring a Conference Device" section on page 73-16.

Before You Begin

Cisco Unified Communications Manager allows you to delete devices that may be associated with things 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. For more information about dependency records, see the "Accessing Dependency Records" section on page A-2.

Procedure

Step 1 Locate the conference bridge by using the procedure in the "Finding a Conference Bridge" section on page 73-15.

Step 2 Click the conference bridge that you want to delete.

Step 3 Click **Delete Selected**.

A message displays the following warning:

You are about to permanently delete this Conference Bridge. This action cannot be undone. Continue?

Step 4 To delete the conference device, click **OK**.

Additional Information

See the "Related Topics" section on page 73-18.

Related Topics

- Software Conference Bridge Configuration Settings, page 73-1
- Hardware Conference Bridge Configuration Settings, page 73-3
- Cisco IOS Conference Bridge Configuration Settings, page 73-6
- Cisco Video Conference Bridge Configuration Settings, page 73-9
- Cisco Conference Bridge (WS-SVC-CMM) Configuration Settings, page 73-12
- Finding a Conference Bridge, page 73-15
- Configuring a Conference Device, page 73-16
- Synchronizing a Conference Device, page 73-17
- Deleting a Conference Device, page 73-17
- Configuring a Meet-Me Number/Pattern, page 65-4
- Deleting a Meet-Me Number/Pattern, page 65-4
- Deleting a Meet-Me Number/Pattern, page 65-4
- Conference Bridges, *Cisco Unified Communications Manager System Guide*
- Conference Bridge Types in Cisco Unified Communications Manager Administration, *Cisco Unified Communications Manager System Guide*
- Trusted Relay Point, *Cisco Unified Communications Manager System Guide*

Other Information

- 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*

CHAPTER 74

Media Termination Point Configuration

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 App service on the server on which you configure the media termination point device. For information on activating and starting services, refer to the *Cisco Unified Serviceability Administration Guide*.

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. See the "Transcoder Configuration" section on page 78-1 for more information.

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.

Use the following topics to add, update, and delete media termination points:

- Cisco IOS Media Termination Point Configuration Settings, page 74-2
- Finding a Media Termination Point, page 74-2
- Configuring a Media Termination Point, page 74-3
- Synchronizing a Media Termination Point, page 74-4
- Deleting a Media Termination Point, page 74-5
- Related Topics, page 74-6

Cisco IOS Media Termination Point Configuration Settings

Table 74-1 describes Cisco IOS media termination point configuration settings. For related procedures, see the "Related Topics" section on page 74-6.

Table 74-1 Cisco IOS Media Termination Point Configuration Settings

Field	Description
Media Termination Point Type	Choose **Cisco IOS Enhanced Software Media Termination Point**. For specific information on this media termination point type, refer to "Media Termination Points" in 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. Refer to "Trusted Relay Point" in the "Media Resource Management" chapter in the *Cisco Unified Communications Manager System Guide* and its subtopics for a discussion of trusted relay points.

Additional Information

See the "Related Topics" section on page 74-6.

Finding a Media Termination Point

Because you might have several media termination points in your network, Cisco Unified Communications Manager lets you locate specific media termination points on the basis of specific criteria. Use the following procedure to locate media termination points.

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

Procedure

Step 1 Choose **Media Resources > Media Termination Point**.

The Find and List Media Termination Points 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.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 74-6.

Configuring a Media Termination Point

This section describes how to add, copy, or update a Media Termination Point.

Note To perform this procedure, you must activate the Cisco IP Voice Media Streaming App service by using Cisco Unified Serviceability. For information about activating services, refer to the *Cisco Unified Serviceability Administration Guide*.

Before You Begin

Make sure that the following prerequisites are met before you proceed with the steps:

- 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.

Procedure

Step 1 Perform one of the following tasks:

- To add a Media Termination Point, choose **Media Resources > Media Termination Point.** The Find and List Media Termination Point window displays. Click **Add New.**
- To copy a Media Termination Point, choose **Media Resources > Media Termination Point.** The Find and List Media Termination Point window displays. Click the **Copy** icon next to the media termination point that you want to copy.
- To update a Media Termination Point, locate the media termination point by using the procedure in the "Finding a Media Termination Point" section on page 74-2.

Step 2 Enter the appropriate settings as described in Table 74-1.

Step 3 Click **Save**.

Additional Information

See the "Related Topics" section on page 74-6.

Synchronizing a Media Termination Point

To synchronize a Media Termination Point with the most recent configuration changes, perform the following procedure, which will apply any outstanding configuration settings in the least-intrusive manner possible. (For example, a reset/restart may not be required on some affected devices.)

Procedure

Step 1 Choose **Media Resources** > **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**.

Additional Information

See the "Related Topics" section on page 74-6.

Deleting a Media Termination Point

This section describes how to delete a Media Termination Point.

Before You Begin

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. See the "Finding a Media Resource Group" section on page 79-2 section.
- Delete the media resource groups that are using the media termination point that you want to delete. See the "Deleting a Media Resource Group" section on page 79-4.

Procedure

Step 1 Locate the media termination point by using the procedure in the "Finding a Media Termination Point" section on page 74-2.

Step 2 Click the media termination point that you want to delete.

Step 3 Click **Delete Selected**.

A message displays the following warning:

You are about to permanently delete this Media Termination Point. This action cannot be undone.

Continue?

Step 4 To delete the media termination point, click **OK**.

If this is the last device in the Media Resource Group, the Media Resource Group will remain as an empty group.

Step 5 Click **OK**.

Additional Information

See the "Related Topics" section on page 74-6.

Related Topics

- Cisco IOS Media Termination Point Configuration Settings, page 74-2
- Finding a Media Termination Point, page 74-2
- Configuring a Media Termination Point, page 74-3
- Synchronizing a Media Termination Point, page 74-4
- Deleting a Media Termination Point, page 74-5
- Transcoders, *Cisco Unified Communications Manager System Guide*
- Media Termination Points, *Cisco Unified Communications Manager System Guide*
- Resource Reservation Protocol, *Cisco Unified Communications Manager System Guide*
- Media Resource Management, *Cisco Unified Communications Manager System Guide*

CHAPTER 75

Music On Hold Audio Source Configuration

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, refer to the Music On Hold chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

CHAPTER 76

Music On Hold Fixed Audio Source Configuration

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, refer to the Music On Hold chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

CHAPTER 77

Music On Hold Server Configuration

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, refer to the Music On Hold chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

CHAPTER 78

Transcoder Configuration

Use the following topics to configure transcoders:

Transcoder Configuration Settings

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.

Table 78-1 describes the transcoder configuration settings. For related procedures, see the "Related Topics" section on page 78-6.

Table 78-1 Transcoder Configuration 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, refer to the "Transcoders" chapter in 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).
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**.
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. Refer to "Trusted Relay Point" and its subtopics in the "Media Resource Management" chapter in 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.

Table 78-1 Transcoder Configuration Settings (continued)

Field	Description
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, refer to the documentation for the specific device that you are configuring or contact the manufacturer.

Additional Information

See the "Related Topics" section on page 78-6.

Finding a Transcoder

Because you might have several transcoders in your network, Cisco Unified Communications Manager lets you locate specific transcoders on the basis of specific criteria. Use the following procedure to locate transcoders.

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

Procedure

Step 1 Choose **Media Resources > Transcoder.**

The Find and List Transcoders 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.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 78-6.

Configuring a Transcoder

This section describes how to configure a transcoder.

Procedure

Step 1 Choose **Media Resources** > **Transcoder**.

The Find and List Transcoders window displays.

Step 2 Perform one of the following tasks:

- To copy an existing transcoder, locate the appropriate transcoder as described in the "Finding a Transcoder" section on page 78-3, click the **Copy** button next to the transcoder that you want to copy, and continue with Step 3.
- To add a new transcoder, click the **Add New** button and continue with Step 3.
- To update an existing transcoder, locate the appropriate transcoder as described in the "Finding a Transcoder" section on page 78-3 and continue with Step 3.

Step 3 Enter the appropriate settings as described in Table 78-1.

Step 4 Click **Save**.

The window refreshes and shows specific information, including the status, for the transcoder that you just configured.

Additional Information

See the "Related Topics" section on page 78-6.

Resetting a Transcoder

This section describes how to reset a Transcoder.

Procedure

Step 1 Choose **Media Resources** > **Transcoder**.

Step 2 From the Transcoders list, choose the transcoder that you want to reset.

The window refreshes and displays the transcoder that you chose.

Step 3 Click **Reset**.

The Reset dialog box displays.

Step 4 Click **Reset** again.

Additional Information

See the "Related Topics" section on page 78-6.

Synchronizing a Transcoder

To synchronize a transcoder with the most recent configuration changes, perform the following procedure, which will apply any outstanding configuration settings in the least-intrusive manner possible. (For example, a reset/restart may not be required on some affected devices.).

Procedure

Step 1 Choose **Media Resources** > **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**.

Additional Information

See the "Related Topics" section on page 78-6.

Deleting a Transcoder

This section describes how to delete a transcoder.

Before You Begin

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. For more information about dependency records, see the "Accessing Dependency Records" section on page A-2. 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.

Procedure

Step 1 Locate the transcoder by using the procedure in the "Finding a Transcoder" section on page 78-3.

Step 2 From the list of matching records, choose the transcoder that you want to delete.

The window refreshes and displays the transcoder that you chose.

Step 3 Click **Delete**.

A message displays that states that you are about to permanently delete this transcoder and that you cannot undo this action.

Step 4 If you want to continue, click **OK** or, to cancel the deletion, click **Cancel**.

After the window refreshes, the transcoder that you deleted no longer appears in the transcoder list.

Additional Information

See the "Related Topics" section on page 78-6.

Related Topics

- Transcoder Configuration Settings, page 78-1
- Finding a Transcoder, page 78-3
- Configuring a Transcoder, page 78-4
- Resetting a Transcoder, page 78-5
- Synchronizing a Transcoder, page 78-5
- Deleting a Transcoder, page 78-6
- Conference Bridge Configuration, page 73-1
- Media Termination Point Configuration, page 74-1
- Transcoders, *Cisco Unified Communications Manager System Guide*

- Transcoder Types in Cisco Unified Communications Manager Administration, *Cisco Unified Communications Manager System Guide*
- Media Resource Management, *Cisco Unified Communications Manager System Guide*

CHAPTER 79

Media Resource Group Configuration

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)

Use the following topics to configure media resource groups:

- Media Resource Group Configuration Settings, page 79-1
- Finding a Media Resource Group, page 79-2
- Configuring a Media Resource Group, page 79-4
- Deleting a Media Resource Group, page 79-4
- Understanding Media Resources, *Cisco Unified Communications Manager System Guide*
- Media Resource Group and Media Resource Group List Configuration Checklist, *Cisco Unified Communications Manager System Guide*

Media Resource Group Configuration Settings

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.

Table 79-1 describes the configuration settings that are used for configuring media resource groups. For more information about related procedures, see the "Related Topics" section on page 79-5.

Table 79-1 Media Resource Group Configuration 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. This description can comprise up to 50 characters. Ensure Description does not contain double quotes ("), less than (<), greater than (>), ampersand (&), or the percent sign (%).
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.
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.

Finding a Media Resource Group

Because you might have several media resource groups in your network, Cisco Unified Communications Manager lets you locate specific media resource groups on the basis of specific criteria. Use the following procedure to locate media resource groups.

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

Procedure

Step 1 Choose **Media Resources > Media Resource Group.**

The Find and List Media Resource Groups 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.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 79-5.

Configuring a Media Resource Group

Perform the following procedure to add, update, or copy a media resource group.

Note 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.

Procedure

Step 1 Choose **Media Resources** > **Media Resource Group**.

The Find and List Media Resource Group window displays.

Step 2 Perform one of the followings tasks:

- To copy a media resource group, locate the appropriate media resource group as described in "Finding a Media Resource Group" section on page 79-2. From the Search Results list, click the **Copy** icon that corresponds to the media resource group that you want to copy, and continue with Step 3.
- To add a new media resource group, click the **Add New** button. The Media Resource Group Configuration window displays. Continue with Step 3.
- To update an existing media resource group, locate the appropriate media resource group as described in "Finding a Media Resource Group" section on page 79-2, and continue with Step 3.

Step 3 Enter the appropriate settings as described in Table 79-1.

Step 4 Click **Save**.

If you are copying a media resource group, you should change at least the media resource group name.

If you are adding a media resource group, the Status changes from *Ready* to *Insert completed*. The list of media resource groups now includes the new media resource group.

If you are updating an existing media resource group, the Status changes from *Ready* to *Update completed.*

Additional Information

See the "Related Topics" section on page 79-5.

Deleting a Media Resource Group

Perform the following procedure to delete an existing media resource group.

Before You Begin

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. For more information about dependency records, see the "Accessing

Dependency Records" section on page A-2. 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. See the "Configuring a Media Resource Group List" section on page 80-3.
- Delete the media resource group lists that are using the media resource group that you want to delete. See the "Deleting a Media Resource Group List" section on page 80-4.

Procedure

Step 1 Locate the media resource group by using the procedure in the "Finding a Media Resource Group" section on page 79-2.

Step 2 From list of matching records, choose the media resource group that you want to delete.

Step 3 Click the **Delete** button.

A message displays that states that you are about to permanently delete this media resource group and that you cannot undo this action.

Step 4 If you want to continue, click **OK** or to cancel the deletion, click **Cancel**.

The chosen media resource group no longer appears in the Media Resource Groups List.

Additional Information

See the "Related Topics" section on page 79-5.

Related Topics

- Media Resource Group Configuration Settings, page 79-1
- Finding a Media Resource Group, page 79-2
- Configuring a Media Resource Group, page 79-4
- Deleting a Media Resource Group, page 79-4
- Accessing Dependency Records, page A-2
- Understanding Media Resources, *Cisco Unified Communications Manager System Guide*
- Media Resource Group and Media Resource Group List Configuration Checklist, *Cisco Unified Communications Manager System Guide*

Media Resource Group List

- Media Resource Group List Configuration, page 80-1
- Configuring a Media Resource Group List, page 80-3
- Deleting a Media Resource Group List, page 80-4

CHAPTER 80

Media Resource Group List Configuration

Use the following topics to configure Media Resource Group Lists:

- Media Resource Group List Configuration Settings, page 80-1
- Finding a Media Resource Group List, page 80-2
- Configuring a Media Resource Group List, page 80-3
- Deleting a Media Resource Group List, page 80-4

Media Resource Group List Configuration Settings

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.

Table 80-1 describes the configuration settings that are used for configuring Media Resource Group Lists. For more information about related procedures, see the "Related Topics" section on page 80-4

Table 80-1 Media Resource Group List Configuration 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.

Table 80-1 Media Resource Group List Configuration Settings (continued)

Field	Description
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.

Finding a Media Resource Group List

Because you might have several media resource group lists in your network, Cisco Unified Communications Manager lets you locate specific media resource group lists on the basis of specific criteria. Use the following procedure to locate media resource group lists.

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

Procedure

Step 1 Choose **Media Resources > Media Resource Group List.**

The Find and List Media Resource Group 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 Step 3.

To filter or search records

- From the drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 80-4.

Configuring a Media Resource Group List

Perform the following procedure to add, update, or copy a Media Resource Group List.

Note 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.

Procedure

Step 1 Choose **Media Resources > Media Resource Group List**.

The Find and List Media Resource Group Lists window displays.

Step 2 Perform one of the followings tasks:

- To copy a media resource group list, locate the appropriate media resource group list as described in "Finding a Media Resource Group List" section on page 80-2. From the Search Results list, click the **Copy** icon that corresponds to the media resource group list that you want to copy and continue with Step 3.
- To add a new media resource group list, click the **Add New** button. The Media Resource Group List Configuration window displays. Continue with Step 3.

- To update an existing media resource group list, locate the appropriate Media Resource Group List as described in "Finding a Media Resource Group List" section on page 80-2, and continue with Step 3.

Step 3 Enter the appropriate settings as described in Table 80-1.

Step 4 Click **Save**.

If you are adding a new media resource group list, the Status changes to from *Ready* to *Add successful*. The Media Resource Group Lists list now includes the new Media Resource Group List.

If you are copying a media resource group, you should change at least the media resource group name.

Additional Information

See the "Related Topics" section on page 80-4.

Deleting a Media Resource Group List

Perform the following procedure to delete an existing Media Resource Group List.

Note 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.

Procedure

Step 1 Locate the media resource group list by using the procedure in the "Finding a Media Resource Group List" section on page 80-2.

Step 2 From list of matching records, choose the media resource group list that you want to delete.

Step 3 Click the **Delete** button.

A message displays that states that you are about to permanently delete this media resource group list and that you cannot undo this action.

Step 4 If you want to continue, click **OK** or to cancel the deletion, click **Cancel**.

The chosen Media Resource Group List no longer appears in the Media Resource Groups List list.

Additional Information

See the "Related Topics" section on page 80-4.

Related Topics

- Media Resource Group List Configuration Settings, page 80-1
- Finding a Media Resource Group List, page 80-2
- Configuring a Media Resource Group List, page 80-3
- Deleting a Media Resource Group List, page 80-4

- Media Resource Group Configuration, page 79-1
- Understanding Media Resources, *Cisco Unified Communications Manager System Guide*
- Media Resource Group and Media Resource Group List Configuration Checklist, *Cisco Unified Communications Manager System Guide*

CHAPTER 81

MOH Audio File Management Configuration

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, refer to the Music On Hold chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

CHAPTER 82

Mobile Voice Access Configuration

Mobile Connect 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 Mobile Connect 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 Mobile Connect and Mobile Voice Access, refer to the Cisco Unified Mobility chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

PART 5

Voice Mail Configuration

CHAPTER 83

Cisco Voice-Mail Port Configuration

You can add and delete ports that are associated with a Cisco voice-mail server to the Cisco Unified Communications Manager database without using the Cisco Voice Mail Port Wizard. This section describes the procedures for doing so:

- Cisco Voice-Mail Port Configuration Settings, page 83-1
- Finding a Cisco Voice-Mail Port, page 83-6
- Configuring Cisco Voice-Mail Ports, page 83-7
- Synchronizing a Cisco Voice Mail Port with Affected Devices, page 83-8
- Deleting a Cisco Voice-Mail Port, page 83-9

Cisco Voice-Mail Port Configuration Settings

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, refer to the applicable *Cisco Unified Communications Manager Integration Guide for Cisco Unity*.

For more information on voice-messaging connectivity to Cisco Unified Communications Manager, refer to "Voice Mail Connectivity to Cisco Unified Communications Manager" in the *Cisco Unified Communications Manager System Guide*.

Table 83-1 describes the Cisco voice-mail port configuration settings. For more information about related procedures, see the "Related Topics" section on page 83-9.

Table 83-1 Cisco Voice-Mail Port Configuration Settings

Field	Description
Device Information	
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. See Common Device Configuration for more information.
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 ellipsis 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 **OK**. **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.

Table 83-1 Cisco Voice-Mail Port Configuration Settings (continued)

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 more details about locations, see the "Location Configuration" section on page 17-1. For an explanation of location-based CAC across intercluster trunks, see "Location-Based Call Admission Control Over Intercluster Trunk" in 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, refer to the *Cisco Unified Communications Manager Security Guide*.

Table 83-1 Cisco Voice-Mail Port Configuration Settings (continued)

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 "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 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. Refer to the "Trusted Relay Point" section and its subtopics in the Media Resource Management chapter of 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.

Table 83-1 Cisco Voice-Mail Port Configuration Settings (continued)

Field	Description
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. Find and choose a partition name (see the "Finding a Partition" section on page 52-3). **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 "Finding a Calling Search Space" section on page 53-3). **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.

Table 83-1 Cisco Voice-Mail Port Configuration Settings (continued)

Field	Description
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.

Finding a Cisco Voice-Mail Port

Because you will typically have a number of Cisco voice-mail ports in your network, Cisco Unified Communications Manager lets you locate specific Cisco voice-mail ports on the basis of specific criteria. Use the following procedure to locate Cisco voice-mail ports.

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

Procedure

Step 1 Choose **Voice Mail >Cisco Voice Mail Port**.

The Find and List Voice Mail Ports 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.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 83-9.

Configuring Cisco Voice-Mail Ports

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. See Cisco Voice Mail Port Wizard, page 84-1 for more information.

Perform this procedure to add individual Cisco voice-mail ports to the Cisco Unified Communications Manager database, or update or copy an existing voice-mail port.

Procedure

Step 1 Choose **Voice Mail** > **Cisco Voice Mail Port**.

The Find and List Voice Mail Ports window displays.

Step 2 Perform one of the followings tasks:

- To copy Cisco voice-mail port and its settings, locate the appropriate Cisco voice-mail port as described in "Finding a Cisco Voice-Mail Port" section on page 83-6. From the Search Results list, click the **Copy** icon that corresponds to the voice-mail port that you want to copy, and continue with Step 3.
- To add a new voice-mail port, click the **Add New** button. The Voice Mail Port Configuration window displays. Continue with Step 3.
- To update an existing Cisco voice-mail port, locate the appropriate voice-mail port as described in "Finding a Cisco Voice-Mail Port" section on page 83-6. Click the voice-mail port that you want to update and continue with Step 3.

Step 3 Enter the appropriate settings as described in Table 83-1.

Step 4 Click **Save**.

If you are copying the basic settings of an existing Cisco voice-mail port to apply to another Cisco voice-mail port, you must change the Port Name and Directory Number fields.

Additional Information

See the "Related Topics" section on page 83-9.

Synchronizing a Cisco Voice Mail Port with Affected Devices

To synchronize devices with a voice mail port that has undergone configuration changes, perform the following procedure, which will apply any outstanding configuration settings in the least-intrusive manner possible. (For example, a reset/restart may not be required on some affected devices.)

Procedure

Step 1 Choose **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**.

Additional Information

See the "Related Topics" section on page 83-9.

Deleting a Cisco Voice-Mail Port

To delete a single Cisco voice-mail port from Cisco Unified Communications Manager, follow these procedures.

Before You Begin

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. For more information about dependency records, see the "Accessing Dependency Records" section on page A-2.

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. See the "Configuring a Directory Number" section on page 64-25.

After you delete the voice-mail port, you can delete the directory number that was using the voice-mail port. See the "Deleting Unassigned Directory Numbers" section on page 67-2.

Tip Instead of using the procedure that is described here, you can use the Cisco Voice Mail Port Wizard to delete ports from an existing server. See "Cisco Voice Mail Port Wizard" section on page 84-1 for more information.

Procedure

Step 1 Choose **Voice Mail** > **Cisco Voice Mail Port**.

Step 2 Find the Cisco voice-mail port by using the procedure in the "Finding a Cisco Voice-Mail Port" section on page 83-6.

Step 3 Click the Cisco voice-mail port that you want to delete.

Step 4 Click **Delete**.

Additional Information

See the "Related Topics" section on page 83-9.

Related Topics

- Cisco Voice-Mail Port Configuration Settings, page 83-1
- Finding a Cisco Voice-Mail Port, page 83-6
- Configuring Cisco Voice-Mail Ports, page 83-7
- Synchronizing a Cisco Voice Mail Port with Affected Devices, page 83-8
- Deleting a Cisco Voice-Mail Port, page 83-9

- Cisco Voice Mail Port Wizard, page 84-1
- Cisco Unity and Cisco Unity Connection Configuration Checklist, *Cisco Unified Communications Manager System Guide*

CHAPTER 84

Cisco Voice Mail Port Wizard

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, refer to 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, refer to 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, refer to "Voice Mail Connectivity to Cisco Unified Communications Manager" in 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. The following sections describes the procedures.

This chapter includes the following configuration information:

Adding a New Cisco Voice-Mail Server and Ports

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 **Voice Mail** > **Cisco Voice Mail Port Wizard**.

From the display, choose one of the following options:

- Create a new Cisco Voice Mail Server and add ports to it. Click **Next** and continue with Step 2.
- Add ports to an existing Cisco Voice Mail server. Click **Next** and continue with the "Adding Ports to an Existing Cisco Voice-Mail Server" section on page 84-6.
- Delete ports from an existing Cisco Voice Mail server. Click **Next** and continue with the "Deleting Ports from an Existing Cisco Voice-Mail Server" section on page 84-7.

Step 2 Choose **Add ports to a new Cisco Voice Mail server using this name**.

Step 3 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 4 Click **Next**.

The Cisco Voice Mail Ports window displays.

Step 5 From the drop-down list box, choose the number of ports to add.

Step 6 Click **Next**.

The Cisco Voice Mail Device Information window displays.

Step 7 Enter the appropriate configuration settings, as described in Table 84-1. The wizard applies these configuration settings to all the new ports.

Table 84-1 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.
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. See Common Device Configuration for more information.

Table 84-1 Voice Mail Port Wizard Device Information Configuration Settings (continued)

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. 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 "Finding a Calling Search Space" section on page 53-3). **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 more details about locations, see the "Location Configuration" section on page 17-1. For an explanation of location-based CAC across intercluster trunks, see "Location-Based Call Admission Control Over Intercluster Trunk" in 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, refer to the *Cisco Unified Communications Manager Security Guide*.

Step 8 Click **Next**.

The Cisco Voice Mail Directory Numbers window displays.

Step 9 Enter the directory number settings for the new Cisco voice-mail server as described in Table 84-2.

Table 84-2 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 (see the "Finding a Partition" section on page 52-3). **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 "Finding a Calling Search Space" section on page 53-3). **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 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.

Table 84-2 Voice Mail Port Wizard Directory Number Configuration Settings (continued)

Field	Description
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 +.

Step 10 Click **Next**.

A window that asks whether you want to add these directory numbers to a line group displays.

Step 11 Choose one of the options that display:

- If you choose to add directory numbers to a new line group, skip to Step 12.
- If you choose to add directory numbers to an existing line group, skip to Step 14.
- If you choose to add directory numbers to a line group later, skip to Step 16.

Step 12 Choose the “Yes. Add directory numbers to a **new** Line Group” option and click **Next**.

Step 13 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 17.

Step 14 Choose the “Yes. Add directory numbers to an **existing** Line Group” option and click **Next**.

Step 15 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 17.

Step 16 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 17 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 18 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.

Next Steps

- Make sure that you set up the message-waiting indicator (MWI) device. For more information, refer to the "Cisco Unity and Cisco Unity Connection Configuration Checklist" section in the *Cisco Unified Communications Manager System Guide*.

Additional Topics

See the "Related Topics" section on page 84-7.

Adding Ports to an Existing Cisco Voice-Mail Server

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 **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 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.

Additional Topics

See the "Related Topics" section on page 84-7.

Deleting Ports from an Existing Cisco Voice-Mail Server

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 **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**.

Additional Topics

See the "Related Topics" section on page 84-7.

Related Topics

- Cisco Voice Mail Port Wizard, page 84-1
- Adding a New Cisco Voice-Mail Server and Ports, page 84-1
- Adding Ports to an Existing Cisco Voice-Mail Server, page 84-6
- Deleting Ports from an Existing Cisco Voice-Mail Server, page 84-7
- Message Waiting Configuration, page 85-1
- Cisco Unity and Cisco Unity Connection Configuration Checklist, *Cisco Unified Communications Manager System Guide*

CHAPTER 85

Message Waiting Configuration

The following topics provide information on message waiting configuration:

Message Waiting Configuration Settings

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.

Table 85-1 describes the Message Waiting configuration settings. For related procedures, see the "Related Topics" section on page 85-5.

Table 85-1 Message Waiting Configuration 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**.

Table 85-1 Message Waiting Configuration Settings (continued)

Field Name	Description
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. Find and choose a partition name (see the "Finding a Partition" section on page 52-3). **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 "Finding a Calling Search Space" section on page 53-3). **Note** To set the maximum list box items, choose **System > Enterprise Parameters** and choose **CCMAdmin Parameters**.

Additional Information

See the "Related Topics" section on page 85-5.

Finding a Message Waiting Number

Because you might have several message-waiting numbers in your network, Cisco Unified Communications Manager lets you locate specific message-waiting numbers on the basis of specific criteria. Use the following procedure to locate message-waiting numbers.

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

Procedure

Step 1 Choose **Voice Mail** > **Message Waiting**.

The Find and List Message Waiting Numbers 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.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- Specify the appropriate search text, if applicable.
- From the third drop-down list box, select Both, On, or Off.

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.

Additional Information

See the "Related Topics" section on page 85-5.

Configuring Message Waiting

To configure message waiting for use with voice-messaging systems, use the following procedure.

Procedure

Step 1 Choose **Voice Mail** > **Message Waiting**.

Step 2 Click the **Add New.**

The Message Waiting Number Configuration window displays.

Step 3 Enter the appropriate settings as described in Table 85-1.

Note 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.

Step 4 To add this device to the system, click **Save**.

Additional Information

See the "Related Topics" section on page 85-5.

Deleting a Message Waiting Number

To delete the message-waiting number, perform these procedures.

Procedure

Step 1 Choose **Voice Mail** > **Message Waiting**.

Step 2 Find the message-waiting number by using the procedure in the "Finding a Message Waiting Number" section on page 85-2.

Step 3 Click the message-waiting number that you want to delete.

Step 4 Click **Delete**.

A confirmation window displays.

Step 5 To delete the message-waiting number, click **OK** or to cancel the deletion process, click **Cancel**.

Additional Information

See the "Related Topics" section on page 85-5.

Related Topics

- Message Waiting Configuration Settings, page 85-1
- Finding a Message Waiting Number, page 85-2
- Configuring Message Waiting, page 85-4
- Voice Mail Connectivity to Cisco Unified Communications Manager, *Cisco Unified Communications Manager System Guide*
- Cisco Unity and Cisco Unity Connection Configuration Checklist, *Cisco Unified Communications Manager System Guide*
- Voice-Mail Profile Configuration, page 87-1
- Directory Number Configuration Settings, page 64-1

CHAPTER 86

Cisco Voice-Mail Pilot Configuration

The following topics provide information on voice-mail pilot configuration:

- Voice-Mail Pilot Configuration Settings, page 86-1
- Finding a Cisco Voice-Mail Pilot, page 86-2
- Configuring the Voice-Mail Pilot Number, page 86-3
- Deleting a Voice-Mail Pilot Number, page 86-4
- Voice Mail Connectivity to Cisco Unified Communications Manager, *Cisco Unified Communications Manager System Guide*
- Cisco Unity and Cisco Unity Connection Configuration Checklist, *Cisco Unified Communications Manager System Guide*

Voice-Mail Pilot Configuration Settings

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.

Table 86-1 describes the voice-mail pilot configuration settings.

Table 86-1 Voice-Mail Pilot Configuration Settings

Field	Description
Voice Mail Pilot Number	Enter a number to identify the voice mail pilot number.
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. Find and choose a calling search space name (see the "Finding a Calling Search Space" section on page 53-3). **Note** To set the maximum list box items, choose **System > Enterprise Parameters** and choose **CCMAdmin Parameters**.
Description	Enter the description of the pilot number.
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.

Additional Information

See the "Related Topics" section on page 86-5.

Finding a Cisco Voice-Mail Pilot

Because you may have several Cisco voice-mail pilots in your network, Cisco Unified Communications Manager lets you locate specific Cisco voice-mail pilots on the basis of specific criteria. Use the following procedure to locate Cisco voice-mail pilots.

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

Procedure

Step 1 Choose **Voice Mail > Voice Mail Pilot**.

The Find and List Voice Mail Pilots 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.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 86-5.

Configuring the Voice-Mail Pilot Number

To configure the voice-mail pilot number, perform these procedures.

Procedure

Step 1 Choose **Voice Mail** > **Voice Mail Pilot**.

Step 2 Click the **Add New** link.

Step 3 Configure the appropriate settings as described in Table 86-1.

Step 4 To add the new voice-mail pilot number or to update the settings for an existing voice-mail pilot number, click **Save**.

Additional Information

See the "Related Topics" section on page 86-5.

Deleting a Voice-Mail Pilot Number

To delete the voice-mail pilot number, perform these procedures. You cannot delete the default or the *No Voice Mail* profile numbers.

Before You Begin

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. For more information about dependency records, see the "Accessing Dependency Records" section on page A-2. 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. See the "Configuring a Voice-Mail Profile" section on page 87-3.
- Delete the voice-mail profiles that are using the voice-mail pilot that you want to delete. See the "Deleting a Voice-Mail Profile" section on page 87-5.

Procedure

Step 1 Choose **Voice Mail** > **Voice Mail Pilot**.

Step 2 Find the voice-mail pilot by using the procedure in the "Finding a Cisco Voice-Mail Pilot" section on page 86-2.

Step 3 Click the Cisco voice-mail pilot that you want to delete.

Step 4 Click **Delete**.

A confirmation window displays.

Note If you choose the default or the *No Voice Mail* pilot numbers, the Delete button does not display.

Step 5 To delete the voice-mail pilot, click **OK** or to cancel the deletion process, click **Cancel**.

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.

Additional Information

See the "Related Topics" section on page 86-5.

Related Topics

- Voice-Mail Pilot Configuration Settings, page 86-1
- Finding a Cisco Voice-Mail Pilot, page 86-2
- Configuring the Voice-Mail Pilot Number, page 86-3
- Deleting a Voice-Mail Pilot Number, page 86-4
- Voice Mail Connectivity to Cisco Unified Communications Manager, *Cisco Unified Communications Manager System Guide*
- Cisco Unity and Cisco Unity Connection Configuration Checklist, *Cisco Unified Communications Manager System Guide*
- Message Waiting Configuration, page 85-1
- Voice-Mail Profile Configuration, page 87-1

CHAPTER 87

Voice-Mail Profile Configuration

The following topics provide information on voice-mail profiles:

Voice-Mail Profile Configuration Settings

The Voice Mail Profile Configuration window of Cisco Unified Communications Manager Administration allows you to define any line-related voice-messaging information.

Note A voice-mail profile gets assigned to a directory number, not a device.

Table 87-1 describes the voice-mail profile configuration settings. For more information about related procedures, see the "Related Topics" section on page 87-5.

Table 87-1 Voice Mail Profile Configuration Settings

Field	Description
Voice Mail Profile Information	
Voice Mail Profile Name	Enter a name to identify the voice-mail profile.
Description	Enter the description of the profile.
Voice Mail Pilot	Choose the appropriate voice-mail pilot number that is defined in the Voice Mail Pilot Configuration or **Use Default**.

Table 87-1 Voice Mail Profile Configuration Settings (continued)

Field	Description
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 Communications Manager 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. See the "Directory Number Configuration" section on page 64-1 for more information. **Note** When a call gets redirected from a DN to a voice-mail server/service that is integrated with Cisco Unified Communications Manager 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 Communications Manager server to choose a mailbox.
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.

Finding Voice-Mail Profiles

Because you may have several voice-mail profiles in your network, Cisco Unified Communications Manager lets you locate specific voice-mail profiles on the basis of specific criteria. Use the following procedure to locate voice-mail profiles.

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

Procedure

Step 1 Choose **Voice Mail** > **Voice Mail Profile**.

The Find and List Voice Mail Profiles 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.

To filter or search records

- From the drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 87-5.

Configuring a Voice-Mail Profile

To configure a voice-mail profile for a directory number, to copy a voice-mail profile, or to update an existing voice-mail profile use the following procedure.

Procedure

Step 1 In the menu bar, choose **Voice Mail** > **Voice Mail Profile**.

The Find and List Voice Mail Profiles window displays.

Step 2 Perform one of the followings tasks:

- To copy a voice-mail profile, locate the appropriate voice-mail profile as described in "Finding Voice-Mail Profiles" section on page 87-2. From the Search Results list, click the **Copy** icon that corresponds to the voice-mail profile that you want to copy and continue with Step 3.
- To configure a voice-mail profile for a directory number, click the **Add New** button. The Voice Mail Profile Configuration window displays. Continue with Step 3.

- To update an existing voice-mail profile, locate the appropriate voice-mail profile as described in "Finding Voice-Mail Profiles" section on page 87-2 and continue with Step 3.

Step 3 Configure the appropriate settings as described in Table 87-1.

Step 4 Click **Save**.

If you are updating an existing voice-mail profile, click **Apply Config** to synchronize all devices that are associated with the voice-mail profile. For more information about the **Apply Config** button, see the "Synchronizing a Voice Mail Profile With Affected Devices" section on page 87-4.

Additional Information

See the "Related Topics" section on page 87-5.

Synchronizing a Voice Mail Profile With Affected Devices

To synchronize devices with a voice mail profile that has undergone configuration changes, perform the following procedure, which will apply any outstanding configuration settings in the least-intrusive manner possible. (For example, a reset/restart may not be required on some affected devices.)

Procedure

Step 1 Choose **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**.

Additional Information

See the "Related Topics" section on page 87-5.

Deleting a Voice-Mail Profile

To delete a voice-mail profile, use the following procedure. You cannot delete the default profile or the No Voice Mail profile.

Before You Begin

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. For more information about dependency records, see the "Accessing Dependency Records" section on page A-2. 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.

Procedure

Step 1 Choose **Voice Mail** > **Voice Mail Profile**.

Step 2 To locate the voice-mail profile that you want to delete, follow the procedure on "Finding Voice-Mail Profiles" section on page 87-2.

Step 3 Check the check box next to the voice-mail profiles that you want to delete. To select all the voice-mail profiles in the window, check the check box in the matching records title bar.

Step 4 Click **Delete Selected**.

Additional Information

See the "Related Topics" section on page 87-5.

Related Topics

- Voice-Mail Profile Configuration Settings, page 87-1
- Finding Voice-Mail Profiles, page 87-2
- Configuring a Voice-Mail Profile, page 87-3
- Synchronizing a Voice Mail Profile With Affected Devices, page 87-4
- Deleting a Voice-Mail Profile, page 87-5
- Voice Mail Connectivity to Cisco Unified Communications Manager, *Cisco Unified Communications Manager System Guide*
- Cisco Unity and Cisco Unity Connection Configuration Checklist, *Cisco Unified Communications Manager System Guide*

PART 6

Device Configuration

CHAPTER 88

CTI Route Point Configuration

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, refer to the documentation and online help that is included with these applications.

This section describes the following basic procedure:

CTI Route Point Configuration Settings

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, refer to the documentation and online help that is included with these applications.

Table 88-1 describes the CTI route point configuration settings. For more information about related procedures, see the "Related Topics" section on page 88-10.

Table 88-1 CTI Route Point Configuration 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.
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. See the "Common Device Configuration" section on page 102-1 for more information.

Table 88-1 CTI Route Point Configuration Settings (continued)

Field	Description
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. Find and choose a calling search space name (see the "Finding a Calling Search Space" section on page 53-3). **Note** To set the maximum list box items, choose **System** > **Enterprise Parameters** and choose **CCMAdmin Parameters**.
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 more details about locations, see the "Location Configuration" section on page 17-1. For an explanation of location-based CAC across intercluster trunks, see "Location-Based Call Admission Control Over Intercluster Trunk" in 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. Refer to the Cisco Unified Communications Manager locale installer that is in the *Cisco Unified Communications Operating System Administration Guide*.

Table 88-1 CTI Route Point Configuration Settings (continued)

Field	Description
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 the "Media Resource Management" section 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**.
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**.

Table 88-1 CTI Route Point Configuration Settings (continued)

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 "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 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. Refer to the "Trusted Relay Point" section and its subtopics in the "Media Resource Management" chapter of the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.
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.

Table 88-1 CTI Route Point Configuration Settings (continued)

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, refer to "Introducing Geolocations" and "Geolocation Configuration" in the "Geolocations and Location Conveyance" chapter in the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocations, refer to the "Logical Partitioning" chapter in 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.

Finding CTI Route Points

To find and list CTI route points, perform the following procedure.

Procedure

Step 1 Choose **Device > CTI Route Point**.

The Find and List Route Points 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.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 88-10.

Configuring a CTI Route Point

To add or update a CTI route point, perform the following procedure.

Procedure

Step 1 Choose **Device** > **CTI Route Point**.

The Find and List Route Points window displays.

Step 2 Perform one of the followings tasks:

- To copy a CTI route point, locate the appropriate route point as described in "Finding CTI Route Points" section on page 88-6. From the Search Results list, click the **Copy** icon that corresponds to the CTI route point that you want to copy and continue with Step 3.
- To add a new CTI route point, click the **Add New** button. The CTI Route Point Configuration window displays. Continue with Step 3.
- To update a CTI route point, locate the appropriate CTI route point as described in "Finding CTI Route Points" section on page 88-6 and continue with Step 3.

Step 3 Enter the appropriate settings, as defined in Table 88-1.

Step 4 Click **Save**.

For instructions on how to add and configure directory numbers, see the "Configuring a Directory Number" section on page 64-25.

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.

Additional Information

See the "Related Topics" section on page 88-10.

Deleting a CTI Route Point

To delete a CTI route point, perform the following procedure.

Before You Begin

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. For more information about dependency records, see the "Accessing Dependency Records" section on page A-2. 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.

Procedure

Step 1 Choose **Device** > **CTI Route Point**.

The Find/List CTI Route Points window displays.

Step 2 Specify the search criteria that are needed to locate the CTI route point that you want to delete.

Step 3 Click **Find**.

The window refreshes to display a list of the CTI route points that match the specified search criteria.

Step 4 Perform one of the following actions:

- Check the check boxes next to the CTI route points that you want to delete and click **Delete Selected**.
- Delete all the CTI route points in the window by clicking **Select All** and click **Delete Selected**.
- Choose the name of the CTI route point that you want to delete from the list to display its current settings and click **Delete**.

Step 5 To permanently delete the CTI route point, click **OK**.

Additional Information

See the "Related Topics" section on page 88-10.

Resetting a CTI Route Point

To reset a CTI route point, perform the following procedure.

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 reset. To choose all CTI route points in the window, check the check box in the matching records title bar.

Step 5 Click **Reset Selected**.

The Reset Device dialog displays.

Step 6 Click one of the following buttons:

- **Restart**—Restarts a device without shutting it down.
- **Reset**—Shuts down a device and brings it back up.
- **Close**—Closes the Reset Device dialog without performing any action.

Additional Information

See the "Related Topics" section on page 88-10.

Synchronizing a CTI Route Point

To synchronize a CTI route point with the most recent configuration changes, perform the following procedure, which will apply any outstanding configuration settings in the least-intrusive manner possible. (For example, a reset/restart may not be required on some affected devices.)

Procedure

Step 1 Choose **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**.

Additional Information

See the "Related Topics" section on page 88-10.

Related Topics

- CTI Route Point Configuration Settings, page 88-2
- Configuring a CTI Route Point, page 88-7
- Finding CTI Route Points, page 88-6
- Deleting a CTI Route Point, page 88-8
- Resetting a CTI Route Point, page 88-8
- Synchronizing a CTI Route Point, page 88-9
- Computer Telephony Integration, *Cisco Unified Communications Manager System Guide*
- Trusted Relay Point, *Cisco Unified Communications Manager System Guide*

CHAPTER 89

Gatekeeper Configuration

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. Refer to Cisco Multimedia Conference Manager (MCM) documentation for alternate gatekeeper configuration details.

Gatekeeper configuration comprises two 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. See the "Trunk Configuration" section on page 92-1.
- 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. Refer to 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.

The following topics cover gatekeeper configuration in Cisco Unified Communications Manager Administration:

- Gatekeeper Configuration Settings, page 89-1
- Finding a Gatekeeper, page 89-3
- Configuring a Gatekeeper, page 89-4
- Deleting a Gatekeeper, page 89-5
- Resetting a Gatekeeper, page 89-5
- Synchronizing a Gatekeeper, page 89-6
- Related Topics, page 89-6

Gatekeeper Configuration Settings

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. Refer to Cisco Multimedia Conference Manager (MCM) documentation and the *Cisco Unified Communications Solution Reference Network Design (SRND)* for alternate gatekeeper configuration details.

Gatekeeper configuration comprises two 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. See the "Trunk Configuration" section on page 92-1.
- 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. Refer to 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.

Table 89-1 describes the gatekeeper configuration settings. For related procedures, see the "Related Topics" section on page 89-6.

Table 89-1 Gatekeeper Configuration 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.
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.

Table 89-1 Gatekeeper Configuration Settings (continued)

Field	Description
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.

Finding a Gatekeeper

Because you might have several gatekeepers in your network, Cisco Unified Communications Manager Administration lets you locate specific gatekeepers on the basis of specific criteria. Use the following procedure to locate gatekeepers.

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

Procedure

Step 1 Choose **Device** > **Gatekeeper**.

The Find and List Gatekeeper 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.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 89-6.

Configuring a Gatekeeper

Perform the following procedure to add or update a gatekeeper.

Note You can configure multiple gatekeeper devices per Cisco Unified Communications Manager cluster.

Procedure

Step 1 Choose **Device** > **Gatekeeper**.

The Find and List Gatekeepers window displays.

Step 2 Perform one of the followings tasks:

- To add a new gatekeeper, click the **Add New** button and continue with Step 3.
- To update an existing gatekeeper, locate the appropriate gatekeeper as described in "Finding a Gatekeeper" section on page 89-3 and continue with Step 3.

Step 3 Enter the appropriate settings as described in Table 89-1.

Step 4 Click **Save**.

Additional Information

See the "Related Topics" section on page 89-6.

Deleting a Gatekeeper

Perform the following steps to delete a gatekeeper.

Before You Begin

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, see the "Accessing Dependency Records" section on page A-2. 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. See the "Configuring a Trunk" section on page 92-48.
- Delete the trunks that are using the gatekeeper that you want to delete. See the "Deleting a Trunk" section on page 92-49.

Procedure

Step 1 Locate the gatekeeper by using the procedure in the "Finding a Gatekeeper" section on page 89-3.

Step 2 From the list of matching records, choose the gatekeeper that you want to delete.

Step 3 Click **Delete Selected**.

A confirmation dialog box displays.

Step 4 To delete the gatekeeper, click **OK**.

Additional Information

See the "Related Topics" section on page 89-6.

Resetting a Gatekeeper

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. Perform the following procedure to reset a gatekeeper.

Note Resetting a gatekeeper does not cause all active calls that this gatekeeper controls to be dropped; however, new call attempts fail.

Procedure

Step 1 Locate the gatekeeper by using the procedure in the "Finding a Gatekeeper" section on page 89-3.

Step 2 From the list of matching records, choose the gatekeeper that you want to reset.

Step 3 If you changed any settings for the Gatekeeper Device, click **Reset**.

The Reset Device dialog displays.

Step 4 Click one of the following choices:

- **Restart—**Restarts the chosen devices without shutting them down (reregisters the phones and trunks with Cisco Unified Communications Manager).
- **Reset**—Shuts down, then restarts, the internal gatekeeper device. The Cisco Unified Communications Manager cluster unregisters (URQ) and then reregisters (RRQ) with the gatekeeper.
- **Close**—Closes the Reset Device dialog without performing any action.

Additional Information

See the "Related Topics" section on page 89-6.

Synchronizing a Gatekeeper

To synchronize a gatekeeper with the most recent configuration changes, perform the following procedure, which will apply any outstanding configuration settings in the least-intrusive manner possible. (For example, a reset/restart may not be required on some affected devices.)

Procedure

Step 1 Choose **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**.

Additional Information

See the "Related Topics" section on page 89-6.

Related Topics

- Gatekeeper Configuration Settings, page 89-1
- Gatekeeper Configuration, page 89-1

- Finding a Gatekeeper, page 89-3
- Configuring a Gatekeeper, page 89-4
- Deleting a Gatekeeper, page 89-5
- Resetting a Gatekeeper, page 89-5
- Synchronizing a Gatekeeper, page 89-6
- Trunk Configuration, page 92-1
- Gatekeepers and Trunks, *Cisco Unified Communications Manager System Guide*

Additional Cisco Documentation

- *Cisco Unified Communications Solution Reference Network Design (SRND)*
- Cisco IOS Multimedia Conference Manager (Command Reference) documentation

CHAPTER 90

Gateway Configuration

Cisco Unified Communications gateways enable Cisco Unified Communications Manager to communicate with non-IP telecommunications devices. Cisco Unified Communications Manager supports several gateway types as described in the *Cisco Unified Communications Manager System Guide*.

These sections provide information about using Cisco Unified Communications Manager for working with and configuring Cisco gateways.

Gateway Configuration Settings

Cisco Unified Communications gateways enable Cisco Unified Communications Manager to communicate with non-IP telecommunications devices. See the following sections for tables that list detailed descriptions for all gateway configuration fields:

- MGCP Gateway Configuration Settings, page 90-2
- H.323 Gateway Configuration Settings, page 90-4
- Analog Access Gateway Configuration Settings, page 90-22
- Cisco VG248 Gateway Configuration Settings, page 90-27
- Cisco IOS SCCP Gateway Configuration Settings, page 90-28

For detailed information about port configuration settings, see the "Port Configuration Settings" section on page 90-30.

MGCP Gateway Configuration Settings

Table 90-1 provides detailed descriptions for MGCP gateway configuration settings.

Table 90-1 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.
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.

Table 90-1 MGCP Gateway Configuration Settings (continued)

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). **Note** The correct number of slots displays for each model of MGCP gateway. (The VG200 gateway has only one slot.) **Note** To begin configuring ports on a module, select the module first; then, click **Save**.	
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 chosen 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.

Table 90-1 MGCP Gateway Configuration Settings (continued)

Field	Description
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, refer to the documentation for the specific gateway that you are configuring or contact the manufacturer.

Additional Information

See the "Related Topics" section on page 90-104.

H.323 Gateway Configuration 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.

Table 90-2 lists configuration settings for H.323 gateways.

Table 90-2 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.
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.

Table 90-2 H.323 Gateway Configuration Settings (continued)

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, refer to 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, refer to 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 more details about locations, see the "Location Configuration" section on page 17-1. For an explanation of location-based CAC across intercluster trunks, see "Location-Based Call Admission Control Over Intercluster Trunk" in the *Cisco Unified Communications Manager System Guide*.

Table 90-2 H.323 Gateway Configuration Settings (continued)

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	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** Refer to the *Cisco Unified Communications Manager 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 more information, refer to Chapter 25, “Service Parameters Configuration.” • For information on QSIG support with Cisco Unified Communications Manager, refer to “Q.Signaling (QSIG)” in the “Understanding IP Telephony Protocols” chapter of the *Cisco Unified Communications Manager System Guide*.

Table 90-2 H.323 Gateway Configuration Settings (continued)

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 more information, refer to Chapter 25, “Service Parameters Configuration.” • For information on QSIG support with Cisco Unified Communications Manager, refer to “Q.Signaling (QSIG)” in the “Understanding IP Telephony Protocols” chapter of the *Cisco Unified Communications Manager System Guide*.

Table 90-2 H.323 Gateway Configuration Settings (continued)

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 "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 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. Refer to the "Trusted Relay Point" section and its subtopics in the "Media Resource Management" chapter of 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.

Table 90-2 H.323 Gateway Configuration Settings (continued)

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.

Table 90-2 H.323 Gateway Configuration Settings (continued)

Field	Description
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, refer to 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.
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 device type does not have this setting.
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.

Table 90-2 H.323 Gateway Configuration Settings (continued)

Field	Description
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. Find and choose a calling search space name (see the "Finding a Calling Search Space" section on page 53-3). **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.
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.

Table 90-2 H.323 Gateway Configuration Settings (continued)

Field	Description
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 Table 17-8 in the "Calling Party Number Transformations Settings" section in the *Cisco Unified Communications Manager System Guide*.

Table 90-2 H.323 Gateway Configuration Settings (continued)

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.

Table 90-2 H.323 Gateway Configuration Settings (continued)

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.

Table 90-2 H.323 Gateway Configuration Settings (continued)

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 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.

Table 90-2 H.323 Gateway Configuration Settings (continued)

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 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 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 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 H.323 Gateway Configuration window.

Table 90-2 H.323 Gateway Configuration Settings (continued)

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, refer to "Introducing Geolocations" and "Geolocation Configuration" in the "Geolocations and Location Conveyance" chapter in the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocations, refer to the "Logical Partitioning" chapter 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 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, refer to "Introducing Geolocation Filters" and "Geolocation Filter Configuration" in the "Geolocations and Location Conveyance" chapter in the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocation filters, refer to the "Logical Partitioning" chapter in 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**.

Table 90-2 H.323 Gateway Configuration Settings (continued)

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 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, 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 "Configuring the Incoming Calling Party Settings in the Device Pool, Gateway, or Trunk Configuration Windows" in the *Cisco Unified Communications Manager Features and Services Guide*.

Table 90-2 H.323 Gateway Configuration Settings (continued)

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 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, 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 "Configuring the Incoming Calling Party Settings in the Device Pool, Gateway, or Trunk Configuration Windows" in the *Cisco Unified Communications Manager Features and Services Guide*.

Table 90-2 H.323 Gateway Configuration Settings (continued)

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 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 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 "Configuring the Incoming Calling Party Settings in the Device Pool, Gateway, or Trunk Configuration Windows" in the *Cisco Unified Communications Manager Features and Services Guide*.

Table 90-2 H.323 Gateway Configuration Settings (continued)

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 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 "Configuring the Incoming Calling Party Settings in the Device Pool, Gateway, or Trunk Configuration Windows" in the *Cisco Unified Communications Manager Features and Services Guide*.

Additional Information

See the "Related Topics" section on page 90-104.

Analog Access Gateway Configuration Settings

Table 90-3 lists configuration settings for Analog Access gateways (Cisco Catalyst 6000 24 port FXS Gateway).

Table 90-3 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.
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. Find and choose a calling search space name (see the "Finding a Calling Search Space" section on page 53-3). **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.

Table 90-3 Analog Access Gateway Configuration Settings (continued)

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 "Location Configuration" section on page 17-1. For an explanation of location-based CAC across intercluster trunks, see "Location-Based Call Admission Control Over Intercluster Trunk" 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.
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.

Table 90-3 Analog Access Gateway Configuration Settings (continued)

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 "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 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. Refer to the "Trusted Relay Point" section and its subtopics in the "Media Resource Management" chapter of 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.

Table 90-3 Analog Access Gateway Configuration Settings (continued)

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.

Table 90-3 Analog Access Gateway Configuration Settings (continued)

Field	Description
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, refer to 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, refer to "Introducing Geolocations" and "Geolocation Configuration" in the "Geolocations and Location Conveyance" chapter in the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocations, refer to the "Logical Partitioning" chapter 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 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, refer to "Introducing Geolocation Filters" and "Geolocation Filter Configuration" in the "Geolocations and Location Conveyance" chapter in the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocation filters, refer to the "Logical Partitioning" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Additional Information

See the "Related Topics" section on page 90-104.

Cisco VG248 Gateway Configuration Settings

Table 90-4 lists configuration settings for the Cisco VG248 Gateways.

Table 90-4 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.
	`EXAMPLE`
	`MAC Address for the Cisco VG248 is`
	`0039A44218`
	`the MAC address for registered port 12 in`
	`Cisco Unified Communications Manager is`
	`VGC0039A4421812`

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.

Additional Information

See the "Related Topics" section on page 90-104.

Cisco IOS SCCP Gateway Configuration Settings

Table 90-5 lists configuration settings for the Cisco IOS SCCP gateways.

Table 90-5 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).
	`EXAMPLE`
	`MAC Address for the gateway is`
	`0006D7E5C7`
	`The MAC address in Cisco Unified Communications Manager is`
	`0006D7E5C7281`
	`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.

Table 90-5 Cisco IOS SCCP Gateway Configuration Settings (continued)

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), 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**.	
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 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

Table 90-5 Cisco IOS SCCP Gateway Configuration Settings (continued)

Field	Description
	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	
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, refer to the documentation for the specific gateway that you are configuring or contact the manufacturer.

Additional Information

- See the "Related Topics" section on page 90-104.

Port Configuration Settings

See the following sections for tables that list detailed descriptions for all port type configuration fields:

- FXS/FXO Port Configuration Settings, page 90-31
- Digital Access PRI Port Configuration Settings, page 90-39
- Digital Access T1 Port Configuration Settings, page 90-62
- BRI Port Configuration Settings, page 90-69
- POTS Port Configuration Settings, page 90-82
- Loop-Start Port Configuration Settings, page 90-84

- Ground-Start Port Configuration Settings, page 90-85
- E & M Port Configuration Settings, page 90-86

For detailed information about gateway configuration settings, see the "Gateway Configuration Settings" section on page 90-2.

FXS/FXO Port Configuration Settings

Table 90-6 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 90-6 FXS/FXO Port Configuration Settings

Field	Description
Device Information	
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/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, refer to 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, refer to the *Cisco Unified Communications Manager Security Guide*.

Table 90-6 FXS/FXO Port Configuration Settings (continued)

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 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. Find and choose a calling search space name (see the "Finding a Calling Search Space" section on page 53-3). **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.
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 Configuration" section on page 17-1. For an explanation of location-based CAC across intercluster trunks, see "Location-Based Call Admission Control Over Intercluster Trunk" 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.

Table 90-6 FXS/FXO Port Configuration Settings (continued)

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 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.

Table 90-6 FXS/FXO Port Configuration Settings (continued)

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 "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 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. Refer to the "Trusted Relay Point" section and its subtopics in the "Media Resource Management" chapter of the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.

Table 90-6 FXS/FXO Port Configuration Settings (continued)

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, refer to "Introducing Geolocations" and "Geolocation Configuration" in the "Geolocations and Location Conveyance" chapter in the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocations, refer to the "Logical Partitioning" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
Transmit UTF-8 for Calling Party Name	This device uses the user locale setting of the device pool for the device o 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.
Calling Party Transformation CSS	This setting, which displays for FXS ports (not FXO ports), 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.

Table 90-6 FXS/FXO Port Configuration Settings (continued)

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 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.
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*.

Table 90-6 FXS/FXO Port Configuration Settings (continued)

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*.
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 +.
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.

Table 90-6 FXS/FXO Port Configuration Settings (continued)

Field	Description
SMDI Port Number (0-4096)	Use this field for analog access ports that connect to a voice-messaging system. Set the SMDI Port Number equal to the actual port number on the voice-messaging system to which the analog access port connects. **Note** Voice-mail logical ports typically must match physical ports for the voice-messaging system to operate correctly.
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, refer to 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, refer to "Introducing Geolocations" and "Geolocation Configuration" in the "Geolocations and Location Conveyance" chapter in the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocations, refer to the "Logical Partitioning" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Table 90-6 FXS/FXO Port Configuration Settings (continued)

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, refer to "Introducing Geolocation Filters" and "Geolocation Filter Configuration" in the "Geolocations and Location Conveyance" chapter in the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocation filters, refer to the "Logical Partitioning" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Additional Information

See the "Related Topics" section on page 90-104.

Digital Access PRI Port Configuration Settings

Table 90-7 provides detailed descriptions for Digital Access PRI port configuration settings.

Note To determine whether your gateway supports the QSIG protocol, refer to the gateway product documentation. For information on QSIG support with Cisco Unified Communications Manager, refer to "Q.Signaling (QSIG)" in the "Understanding IP Telephony Protocols" chapter of the *Cisco Unified Communications Manager System Guide*.

Table 90-7 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.

Table 90-7 Digital Access PRI Port Configuration Settings (continued)

Field	Description
Description	Enter a description that clarifies the purpose of the device.
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.
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, refer to 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, refer to 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.

Table 90-7 Digital Access PRI Port Configuration Settings (continued)

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 "Location Configuration" section on page 17-1. For an explanation of location-based CAC across intercluster trunks, see "Location-Based Call Admission Control Over Intercluster Trunk" 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.
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.

Table 90-7 Digital Access PRI Port Configuration Settings (continued)

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 "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 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. Refer to the "Trusted Relay Point" section and its subtopics in the "Media Resource Management" chapter of the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.

Table 90-7 Digital Access PRI Port Configuration Settings (continued)

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 v150 (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.) The default value specifies unchecked.
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*.

Table 90-7 Digital Access PRI Port Configuration Settings (continued)

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*.

Table 90-7 Digital Access PRI Port Configuration Settings (continued)

Field	Description
Interface Information	
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

Table 90-7 Digital Access PRI Port Configuration Settings (continued)

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 more information, refer to Chapter 25, "Service Parameters Configuration." • For information on QSIG support with Cisco Unified Communications Manager, refer to "Q.Signaling (QSIG)" in the "Understanding IP Telephony Protocols" chapter of the *Cisco Unified Communications Manager System Guide*.

Table 90-7 Digital Access PRI Port Configuration Settings (continued)

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) 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 more information, refer to Chapter 25, "Service Parameters Configuration." • For information on QSIG support with Cisco Unified Communications Manager, refer to "Q.Signaling (QSIG)" in the "Understanding IP Telephony Protocols" chapter of the *Cisco Unified Communications Manager System Guide*.
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.

Table 90-7 Digital Access PRI Port Configuration Settings (continued)

Field	Description
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.
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.

Table 90-7 Digital Access PRI Port Configuration Settings (continued)

Field	Description
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.
	`EXAMPLE`
	`Digits 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.

Table 90-7 Digital Access PRI Port Configuration Settings (continued)

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. Find and choose a calling search space name (see the "Finding a Calling Search Space" section on page 53-3). **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 Table 17-8 in the "Calling Party Number Transformations Settings" section in the *Cisco Unified Communications Manager System Guide*.

Table 90-7 Digital Access PRI Port Configuration Settings (continued)

Field	Description
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.
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.

Table 90-7 Digital Access PRI Port Configuration Settings (continued)

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 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 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.

Table 90-7 Digital Access PRI Port Configuration Settings (continued)

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: • 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.
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 +.
SMDI Base Port	Enter the first SMDI port number of the T1 span. If you set this parameter to a nonzero value and this gateway belongs to an unknown type of route list, route group, or route list, hunting does not continue past this span.

Table 90-7 Digital Access PRI Port Configuration Settings (continued)

Field	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. **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 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.
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.
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.

Table 90-7 Digital Access PRI Port Configuration Settings (continued)

Field	Description
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).
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.

Table 90-7 Digital Access PRI Port Configuration Settings (continued)

Field	Description
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.
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. For more information about this field, see Table 17-11 in the “Connected Party Presentation and Restriction Settings” section in the *Cisco Unified Communications Manager System Guide*.
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**.

Table 90-7 Digital Access PRI Port Configuration Settings (continued)

Field	Description
Default Prefix Setting	To enter the default value for all prefix fields at the same time, click **Default Prefix Settings**.
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, 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 "Configuring the Incoming Calling Party Settings in the Device Pool, Gateway, or Trunk Configuration Windows" in the *Cisco Unified Communications Manager Features and Services Guide*.

Table 90-7 Digital Access PRI Port Configuration Settings (continued)

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 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, 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 "Configuring the Incoming Calling Party Settings in the Device Pool, Gateway, or Trunk Configuration Windows" in the *Cisco Unified Communications Manager Features and Services Guide*.

Table 90-7 Digital Access PRI Port Configuration Settings (continued)

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 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 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 "Configuring the Incoming Calling Party Settings in the Device Pool, Gateway, or Trunk Configuration Windows" in the *Cisco Unified Communications Manager Features and Services Guide*.

Table 90-7 Digital Access PRI Port Configuration Settings (continued)

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 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 "Configuring the Incoming Calling Party Settings in the Device Pool, Gateway, or Trunk Configuration Windows" in the *Cisco Unified Communications Manager Features and Services Guide*.

Table 90-7 Digital Access PRI Port Configuration Settings (continued)

Field	Description
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, refer to 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, refer to "Introducing Geolocations" and "Geolocation Configuration" in the "Geolocations and Location Conveyance" chapter in the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocations, refer to the "Logical Partitioning" chapter 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 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, refer to "Introducing Geolocation Filters" and "Geolocation Filter Configuration" in the "Geolocations and Location Conveyance" chapter in the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocation filters, refer to the "Logical Partitioning" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Additional Information

See the "Related Topics" section on page 90-104.

Digital Access T1 Port Configuration Settings

Table 90-8 provides detailed descriptions for Digital Access T1 port configuration settings.

Table 90-8 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.
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.
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, refer to the *Cisco Unified Communications Manager Security Guide*.

Table 90-8 Digital Access T1 Port Configuration Settings (continued)

Field	Description
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, refer to 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 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. Find and choose a calling search space name (see the "Finding a Calling Search Space" section on page 53-3). **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 Configuration" section on page 17-1. For an explanation of location-based CAC across intercluster trunks, see "Location-Based Call Admission Control Over Intercluster Trunk" in the *Cisco Unified Communications Manager System Guide*.

Table 90-8 Digital Access T1 Port Configuration Settings (continued)

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.
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	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*.

Table 90-8 Digital Access T1 Port Configuration Settings (continued)

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.
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

Table 90-8 Digital Access T1 Port Configuration Settings (continued)

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.
SMDI Base Port	Enter the first SMDI port number of the T1 span. If you set this parameter to a nonzero value and this gateway belongs to an unknown type of route list, route group, or route list, hunting does not continue past this span.

Table 90-8 Digital Access T1 Port Configuration Settings (continued)

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 "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 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. Refer to the "Trusted Relay Point" section and its subtopics in the "Media Resource Management" chapter of the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.
V150 (subset)	Check this box to enable v150 (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) The default value specifies unchecked.

Table 90-8 Digital Access T1 Port Configuration Settings (continued)

Field	Description
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, refer to 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, refer to "Introducing Geolocations" and "Geolocation Configuration" in the "Geolocations and Location Conveyance" chapter in the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocations, refer to the "Logical Partitioning" chapter 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 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, refer to "Introducing Geolocation Filters" and "Geolocation Filter Configuration" in the "Geolocations and Location Conveyance" chapter in the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocation filters, refer to the "Logical Partitioning" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Additional Information

See the "Related Topics" section on page 90-104.

BRI Port Configuration Settings

Table 90-9 provides detailed descriptions for BRI port configuration settings.

Table 90-9 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.
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/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 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, refer to the *Cisco Unified Communications Manager Security Guide*.

Table 90-9 BRI Port Configuration Settings (continued)

Field	Description
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, refer to 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 more details about locations, see the "Location Configuration" section on page 17-1. For an explanation of location-based CAC across intercluster trunks, see "Location-Based Call Admission Control Over Intercluster Trunk" 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.
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.

Table 90-9 BRI Port Configuration Settings (continued)

Field	Description
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.
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.

Table 90-9 BRI Port Configuration Settings (continued)

Field	Description
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.
	`EXAMPLE`
	`Digits 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.
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 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 PRI Port Gateway Configuration window.

Table 90-9 BRI Port Configuration Settings (continued)

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, refer to "Introducing Geolocations" and "Geolocation Configuration" in the "Geolocations and Location Conveyance" chapter in the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocations, refer to the "Logical Partitioning" chapter in 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 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.

Table 90-9 BRI Port Configuration Settings (continued)

Field	Description
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.

Table 90-9 BRI Port Configuration Settings (continued)

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.

Table 90-9 BRI Port Configuration Settings (continued)

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**.

Table 90-9 BRI Port Configuration Settings (continued)

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 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, 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 "Configuring the Incoming Calling Party Settings in the Device Pool, Gateway, or Trunk Configuration Windows" in the *Cisco Unified Communications Manager Features and Services Guide*.

Table 90-9 BRI Port Configuration Settings (continued)

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 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, 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 "Configuring the Incoming Calling Party Settings in the Device Pool, Gateway, or Trunk Configuration Windows" in the *Cisco Unified Communications Manager Features and Services Guide*.

Table 90-9 BRI Port Configuration Settings (continued)

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 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 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 "Configuring the Incoming Calling Party Settings in the Device Pool, Gateway, or Trunk Configuration Windows" in the *Cisco Unified Communications Manager Features and Services Guide*.

Table 90-9 BRI Port Configuration Settings (continued)

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 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 "Configuring the Incoming Calling Party Settings in the Device Pool, Gateway, or Trunk Configuration Windows" in the *Cisco Unified Communications Manager Features and Services Guide*.

Table 90-9 BRI Port Configuration Settings (continued)

Field	Description
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.
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.

Table 90-9 BRI Port Configuration Settings (continued)

Field	Description
Product-Specific Configuration	
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, refer to the documentation for the specific gateway that you are configuring or contact the manufacturer.

Additional Information

See the "Related Topics" section on page 90-104.

POTS Port Configuration Settings

Table 90-10 describes the POTS port configuration settings.

Table 90-10 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).

Table 90-10 POTS Port Configuration Settings (continued)

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.
SMDI Port Number (0-4096)	Use this field for analog access ports that connect to a voice-messaging system. Set the SMDI Port Number equal to the actual port number on the voice-messaging system to which the analog access port connects. **Note** Voice-mail logical ports typically must match physical ports for the voice-messaging system to operate correctly.
Unattended Port	Check this check box to indicate an unattended port on this device.

Table 90-10 POTS Port Configuration Settings (continued)

Field	Description
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, refer to the documentation for the specific gateway that you are configuring or contact the manufacturer.

Additional Information

See the "Related Topics" section on page 90-104.

Loop-Start Port Configuration Settings

Table 90-11 describes the loop-start port configuration settings.

Table 90-11 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.

Table 90-11 Loop-Start Port Configuration Settings (continued)

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, refer to the documentation for the specific gateway that you are configuring or contact the manufacturer.

Additional Information

See the "Related Topics" section on page 90-104.

Ground-Start Port Configuration Settings

Table 90-12 describes the ground-start port configuration settings.

Table 90-12 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.
Unattended Port	Check this check box to indicate an unattended port on this device.

Table 90-12 Ground-Start Port Configuration Settings (continued)

Field	Description
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, refer to the documentation for the specific gateway that you are configuring or contact the manufacturer.

Additional Information

See the "Related Topics" section on page 90-104.

E & M Port Configuration 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.

Table 90-13 describes the E & M port configuration settings.

Table 90-13 E & 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	
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.

Table 90-13 E & M Port Configuration Settings (continued)

Field	Description
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 +.
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.

Table 90-13 E & M Port Configuration Settings (continued)

Field	Description
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, refer to the documentation for the specific gateway that you are configuring or contact the manufacturer.

Additional Information

See the "Related Topics" section on page 90-104.

Finding Specific Gateways

Because you might have hundreds of gateways in your network, Cisco Unified Communications Manager lets you use specific criteria to locate specific gateways. Use the following procedure to find specific gateways.

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

Procedure

Step 1 Choose **Device** > **Gateway**.

The Find and List Gateway 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.

To filter or search records

- From the first drop-down list box, choose a search parameter.
- From the second drop-down list box, choose a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 90-104.

Adding Gateways 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 90-14, 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.

Table 90-14 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	Adding a Cisco IOS MGCP Gateway, page 90-90
Cisco IOS 269X, 3725, 3745 Gateways	Adding a Cisco IOS SCCP Gateway, page 90-96
Cisco Catalyst 6000 E1 VoIP Gateway Cisco Catalyst 6000 T1 VoIP Gateway	Adding a Non-IOS MGCP Gateway, page 90-97
Other Cisco IOS Gateway that is configured in H.323 mode	Adding a Cisco IOS H.323 Gateway, page 90-98
Cisco Catalyst 6000 24 Port FXS Gateway	Adding an Analog Access Gateway and Ports, page 90-99
Cisco VG248 Gateway	Adding a Cisco VG248 Analog Phone Gateway, page 90-100

Adding a 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, refer to 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:

- Cisco VG200
- VG224
- Cisco 362X, 364X, 366X
- Cisco 3725 and 3745
- Cisco 26XX and 269X
- Cisco 2801, 2811, 2821, 2851, 3825, 3845
- Cisco Catalyst 4000 Access Gateway Module
- Cisco Catalyst 4224 Voice Gateway Switch
- Communication Media Module
- Cisco IAD2400

Note The Cisco Catalyst 6000 gateways also support MGCP but are configured differently. See the "Adding a Non-IOS MGCP Gateway" section on page 90-97.

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.

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 "MGCP Gateway Configuration Settings" section on page 90-2, 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.

For detailed instructions, see the following procedures:

- Adding FXS Ports to an MGCP Gateway, page 90-92
- Adding FXO Ports to an MGCP Gateway, page 90-93
- Adding Digital Access T1 Ports to an MGCP Gateway, page 90-94
- Adding a Digital Access PRI Device to an MGCP Gateway, page 90-95
- Adding a BRI Port to an MGCP Gateway, page 90-95

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.

Adding Ports to an MGCP Gateway

The device protocols and port types that can be configured on MGCP gateways vary by the type of installed voice interface cards. This section contains the following procedures:

- Adding FXS Ports to an MGCP Gateway, page 90-92
- Adding FXO Ports to an MGCP Gateway, page 90-93
- Adding Digital Access T1 Ports to an MGCP Gateway, page 90-94
- Adding a Digital Access PRI Device to an MGCP Gateway, page 90-95
- Adding a BRI Port to an MGCP Gateway, page 90-95

Adding FXS Ports to an 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. See the "Adding a Cisco IOS MGCP Gateway" section on page 90-90 for instructions.

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 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 sections for details about these fields:

- FXS/FXO Port Configuration Settings, page 90-31
- POTS Port Configuration Settings, page 90-82

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.

Note See the "Configuring a Directory Number" section on page 64-25 and "Directory Number Configuration Settings" section on page 64-1 for information about adding and configuring DNs.

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 through Step 8 to add additional FXS ports.

Additional Information

See the "Related Topics" section on page 90-104.

Adding FXO Ports to an 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. See the "Adding a Cisco IOS MGCP Gateway" section on page 90-90 for instructions.

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 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 as described in the following sections:

- FXS/FXO Port Configuration Settings, page 90-31
- Loop-Start Port Configuration Settings, page 90-84
- Ground-Start Port Configuration Settings, page 90-85

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 though Step 7.

Additional Information

See the "Related Topics" section on page 90-104.

Adding Digital Access T1 Ports to an MGCP Gateway

Use this procedure to add Digital Access T1 (T1-CAS) ports to an MGCP gateway.

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 "Finding Specific Gateways" section on page 90-88 for the appropriate settings for the port type that you choose.

Step 5 Enter the appropriate Gateway Configuration settings. See the "Digital Access T1 Port Configuration Settings" section on page 90-62 for details.

Step 6 Click **Save**.

Step 7 To reset the gateway and apply the changes, click **Reset**.

Additional Information

See the "Related Topics" section on page 90-104.

Adding a Digital Access PRI Device to an MGCP Gateway

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 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 "Digital Access PRI Port Configuration Settings" section on page 90-39 for detailed field descriptions.

Step 6 Click **Save**.

Step 7 To reset the gateway and apply the changes, click **Reset**.

Additional Information

See the "Related Topics" section on page 90-104.

Adding a BRI Port to an 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.

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 "BRI Port Configuration Settings" section on page 90-69 for detailed field descriptions.

Step 6 Click **Save**.

Step 7 To apply the changes, reset the gateway.

Additional Information

See the "Related Topics" section on page 90-104.

Adding a 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, refer to 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:

- Cisco IOS 269x
- 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 the "Cisco IOS SCCP Gateway Configuration Settings" section on page 90-28, 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 "Cisco Unified IP Phone Configuration" section on page 91-1 and the "Configuring Speed-Dial Buttons or Abbreviated Dialing" section on page 91-34 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.

Adding a 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**:

- Cisco Catalyst 6000 E1 VoIP Gateway
- 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:

- Cisco Catalyst 6000 T1 VoIP Gateway—Choose either **Digital Access PRI** or **Digital Access T1**.
- 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.

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 Configuration Settings, page 90-39
- Digital Access T1 Port Configuration Settings, page 90-62

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.

See the "Adding Digital Access T1 Ports to an MGCP Gateway" section on page 90-94.

Step 9 To reset the gateway and apply the changes, click **Reset**.

Additional Information

See the "Related Topics" section on page 90-104.

Adding a 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, refer to 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 "H.323 Gateway Configuration Settings" section on page 90-4.

Step 6 Click **Save**.

Step 7 To reset the gateway and apply the changes, click **Reset**.

Additional Information

See the "Related Topics" section on page 90-104.

Adding an 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 "Analog Access Gateway Configuration Settings" section on page 90-22.

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 "POTS Port Configuration Settings" section on page 90-82.

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**.

For information about adding and configuring directory numbers, see the "Configuring a Directory Number" section on page 64-25 and the "Directory Number Configuration Settings" section on page 64-1.

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**.

Additional Information

See the "Related Topics" section on page 90-104.

Adding a 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 "Cisco VG248 Gateway Configuration Settings" section on page 90-27.

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, as described in the "Configuring Speed-Dial Buttons or Abbreviated Dialing" section on page 91-34.

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 "Configuring a Directory Number" section on page 64-25.

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 through Step 11.

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**.

Additional Information

See the "Related Topics" section on page 90-104.

Modifying Gateways and Ports

Using Cisco Unified Communications Manager, you perform the following tasks identically regardless of the gateway type:

- Using Dependency Records, page 90-101
- Deleting Gateways, page 90-101
- Resetting and Restarting Gateways, page 90-102
- Updating Gateways and Ports, page 90-104

Using Dependency Records

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**. For more information about this link, see the "Dependency Records" appendix.

Deleting Gateways

Complete the following steps to delete a gateway from Cisco Unified Communications Manager.

Before You Begin

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. For more information about dependency records, see the "Accessing Dependency Records" section on page A-2. 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. See the "Adding Devices to a Route Group" section on page 42-5.
- Delete the route groups that are using the gateway that you want to delete. See the "Deleting a Route Group" section on page 42-6.

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 gateways that matches your search criteria displays.

Step 4 Check the check box next to the gateway that you want to delete.

Step 5 Click **Delete Selected**.

A message displays that states that you cannot undo this action.

Step 6 To delete the gateway, click **OK** or to cancel the operation, click **Cancel**.

Tip You can delete all the gateways in the window by clicking **Select All** and then clicking **Delete Selected**.

Additional Information

See the "Related Topics" section on page 90-104.

Resetting and Restarting Gateways

Complete the following steps to reset or restart a gateway by using Cisco Unified Communications Manager.

Procedure

Step 1 Choose **Device > Gateway**.

The Find and List Gateway window displays.

Step 2 To locate a specific gateway, enter search criteria.

Step 3 Click **Find**.

A list of discovered gateways that matches your search criteria displays.

Step 4 Check the check box next to the gateway that you want to reset.

Step 5 Click **Reset Selected**.

The Device Reset window displays.

Step 6 Click one of the following choices:

- **Restart**—Restarts a device without shutting it down.
- **Reset**—Shuts down a device and brings it back up.
- **Close**—Returns to the previous window without performing any action.

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.

Additional Information

See the "Related Topics" section on page 90-104.

Synchronizing a Gateway

To synchronize a gateway with the most recent configuration changes, perform the following procedure, which will apply any outstanding configuration settings in the least-intrusive manner possible. (For example, a reset/restart may not be required on some affected devices.)

Procedure

Step 1 Choose **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**.

Additional Information

See the "Related Topics" section on page 90-104.

Updating 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 following sections.

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.

- MGCP Gateway Configuration Settings, page 90-2
- FXS/FXO Port Configuration Settings, page 90-31
- Digital Access PRI Port Configuration Settings, page 90-39
- Digital Access T1 Port Configuration Settings, page 90-62.
- Analog Access Gateway Configuration Settings, page 90-22
- Finding Specific Gateways, page 90-88

Step 6 Click **Save**.

Step 7 To apply the changes, click **Reset** to reset the gateway.

Additional Information

See the "Related Topics" section on page 90-104.

Related Topics

All Gateway Types

- Adding Gateways to Cisco Unified Communications Manager, page 90-89
- Gateway Configuration Settings, page 90-2
- Finding Specific Gateways, page 90-88
- Using Dependency Records, page 90-101
- Modifying Gateways and Ports, page 90-101
- Deleting Gateways, page 90-101
- Resetting and Restarting Gateways, page 90-102

- Synchronizing a Gateway, page 90-103
- Updating Gateways and Ports, page 90-104
- Trusted Relay Point, *Cisco Unified Communications Manager System Guide*
- Local Route Groups, *Cisco Unified Communications Manager Features and Services Guide*

IOS MGCP Gateways

- Adding a Cisco IOS MGCP Gateway, page 90-90
- MGCP Gateway Configuration Settings, page 90-2
- Finding Specific Gateways, page 90-88
- Where to Find More Information, *Cisco Unified Communications Manager System Guide*

SCCP Gateways

- Adding a Cisco IOS SCCP Gateway, page 90-96
- Cisco IOS SCCP Gateway Configuration Settings, page 90-28

Non-IOS MGCP Gateways

- Adding a Non-IOS MGCP Gateway, page 90-97

H.323 Gateways

- Adding a Cisco IOS H.323 Gateway, page 90-98
- H.323 Gateway Configuration Settings, page 90-4

Analog Access Gateways

- Adding an Analog Access Gateway and Ports, page 90-99
- Analog Access Gateway Configuration Settings, page 90-22
- Adding a Cisco VG248 Analog Phone Gateway, page 90-100
- Cisco VG248 Gateway Configuration Settings, page 90-27
- *Cisco VG248 Analog Phone Gateway Software Configuration Guide*

BRI Gateways

- BRI Port Configuration Settings, page 90-69
- MGCP BRI Call Connections, *Cisco Unified Communications Manager System Guide*
- MGCP BRI Gateway Configuration Checklist, *Cisco Unified Communications Manager System Guide*

Ports

- Adding FXS Ports to an MGCP Gateway, page 90-92
- Adding FXO Ports to an MGCP Gateway, page 90-93
- Adding Digital Access T1 Ports to an MGCP Gateway, page 90-94
- Adding a Digital Access PRI Device to an MGCP Gateway, page 90-95
- Adding a BRI Port to an MGCP Gateway, page 90-95
- FXS/FXO Port Configuration Settings, page 90-31
- Digital Access PRI Port Configuration Settings, page 90-39

- Digital Access T1 Port Configuration Settings, page 90-62
- POTS Port Configuration Settings, page 90-82
- Loop-Start Port Configuration Settings, page 90-84
- Ground-Start Port Configuration Settings, page 90-85
- E & M Port Configuration Settings, page 90-86

Phones and Directory Numbers

- Cisco Unified IP Phone Configuration, page 91-1
- Configuring Speed-Dial Buttons or Abbreviated Dialing, page 91-34
- Directory Number Configuration, page 64-1
- Directory Number Configuration Settings, page 64-1

CHAPTER 91

Cisco Unified IP Phone Configuration

Cisco Unified IP Phones as full-featured telephones can plug directly into your IP network. You 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 IP Video Phone 7985
- Cisco Unified IP SIP Phone 3951
- 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. The following procedures apply to update or delete for this phone type. See the "Gateway Configuration" section on page 90-1 for Cisco VG248 analog phone gateway and VG224 analog phone gateway configuration information.

The following topics provide information about working with and configuring Cisco Unified IP Phones in Cisco Unified Communications Manager Administration:

Configuration Settings

- Phone Configuration Settings, page 91-2
- Phone Migration Settings, page 91-24
- Speed-Dial and Abbreviated-Dial Configuration Settings, page 91-25
- BLF/Speed Dial Configuration Settings, page 91-26
- BLF/Directed Call Park Configuration Settings, page 91-26

Procedures

- Finding a Phone, page 91-26
- Configuring Cisco Unified IP Phones, page 91-27
- Resetting a Phone, page 91-32
- Synchronizing a Phone, page 91-32
- Migrating Existing Phone Configuration to a Different Phone, page 91-30
- Deleting a Phone, page 91-33
- Configuring Speed-Dial Buttons or Abbreviated Dialing, page 91-34
- Configuring IP Phone Services, page 91-35
- Configuring Service URL Buttons, page 91-37
- Copy to a Remote Destination Profile, page 91-38
- Modifying Phone Button Template Button Items, page 91-39
- Finding an Actively Logged-In Device, page 91-40
- Displaying the MAC Address of a Phone, page 91-41

Table 44-2 in the "Cisco Unified IP Phones" chapter of the *Cisco Unified Communications Manager System Guide* lists the configuration steps for Cisco Unified IP Phones that support SIP.

For third-party phones that run SIP, see the "Configuration Checklist for Third-Party Phones That Are Running SIP" section on page B-1 in the "Configuring Non-Cisco Phones That Are Running SIP" appendix.

Additional Information

See the "Related Topics" section on page 91-42.

Phone Configuration Settings

Table 91-1 describes the available settings in the Phone Configuration window. For related procedures, see the "Related Topics" section on page 91-42.

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, refer to the documentation for the specific phone that you are configuring or contact the manufacturer.

Table 91-1 Phone Configuration Settings

Field	Description
Device Information	

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, refer to 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. See the "Gateway Configuration" section on page 90-1 for configuration information.
	Only one MAC address exists for the Cisco VG248 Analog Phone Gateway. All 48 ports share the same MAC address. Cisco Unified Communications Manager 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)
	`EXAMPLE`
	`MAC Address for the Cisco VG248 is`
	`000039A44218`
	`the MAC address for registered port 12 in the`
	`Cisco Unified Communications Manager is`
	`0039A4421812`
	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.

Device Name	Enter a name to identify software-based telephones, H.323 clients, and CTI ports. The value can include 1 to 15 characters, including alphanumeric characters, dot, dash, and underscores.
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>.

Table 91-1 Phone Configuration Settings (continued)

Field	Description
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, softkey template, and MLPP information.
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. See "Common Device Configuration" for more information. 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 Communications Manager does not make this field available for H.323 clients or CTI ports.
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, refer to "Partitions and Calling Search Spaces" in the *Cisco Unified Communications Manager System Guide*. For configuration information about calling search space for phones, see the "Calling Search Space" section on page 64-23.
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. For configuration information about calling search space for phones, see the "Calling Search Space" section on page 64-23.
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 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*.

Table 91-1 Phone Configuration Settings (continued)

Field	Description
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 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**.
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 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**.
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 more details about locations, see the "Location Configuration" section on page 17-1. For an explanation of location-based CAC across intercluster trunks, see "Location-Based Call Admission Control Over Intercluster Trunk" 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. If no AAR group is specified, Cisco Unified Communications Manager 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 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 that information be displayed (on the phone) in any language other than English, verify that the locale installer is installed before configuring user locale. Refer to the Cisco Unified Communications Manager Locale Installer documentation.

Table 91-1 Phone Configuration Settings (continued)

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 Communications Manager makes this field available only for phone models that support localization. **Note** If no network locale is specified, Cisco Unified Communications Manager uses the network locale that is associated with the device pool. **Note** If users require that country-specific tones be played (on the phone), verify that the locale is installed before configuring the network locale. Refer to 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, refer to "Barge and Privacy" in the *Cisco Unified Communications Manager Features and Services Guide*. You can also refer to 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, refer to "Barge and Privacy" in the *Cisco Unified Communications Manager Features and Services Guide*.
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, refer to "Device Mobility" in the *Cisco Unified Communications Manager Features and Services Guide*.

Table 91-1 Phone Configuration Settings (continued)

Field	Description
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.
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. **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 Mobile Connect and Mobile Voice Access features for dual-mode phones. **Note** 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, refer to the Phone Designer documentation.
Services Provisioning	From the drop-down list box, choose whether the phone will use the services that are provisioned in the phone configuration file (Internal), services received from an external URL (External URL), or both. The default specifies Internal. Select **External URL** if you are using an external provisioning server or **Both** if are using an external server but also want to allow users to subscribe to services in Cisco Unified Communications Manager.
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 “Licensing” in the *Cisco Unified Communications Manager System Guide*.

Table 91-1 Phone Configuration Settings (continued)

Field	Description
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.
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, see the "Device Defaults Configuration" section on page 94-1. For more information about Cisco Unified IP Phone software and configuration, refer to the Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager 6.1, which is specific to the phone model.
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, refer to "Barge and Privacy" in 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.

Table 91-1 Phone Configuration Settings (continued)

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 "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 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. Refer to the "Trusted Relay Point" section and its subtopics in the "Media Resource Management" chapter of 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.

Table 91-1 Phone Configuration Settings (continued)

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 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.
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.
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 chose in the Phone Configuration window.

Table 91-1 Phone Configuration Settings (continued)

Field	Description
Is Active	Cisco Unified Communications Manager uses the Is Active check box for licensing and registration of phones. For a phone that uses a real MAC address, not for a phone that uses a dummy MAC address that was created via BAT, the check box displays as checked and disabled. For a dummy phone that uses a dummy MAC address that was created via BAT, the Is Active check box displays as unchecked and enabled. If you manually convert the dummy MAC address to a real MAC address in the Phone Configuration window, check this check box, which ensures that the phone can register with Cisco Unified Communications Manager and that licensing consumes device license units for the phone. If you use the Cisco Unified Communications Manager Auto-Register Phone Tool (TAPS), the tool updates the Is Active check box in the Phone Configuration window to display as checked and disabled after the Cisco Unified Communications Manager Auto-Register Phone Tool applies the device name to the phone that uses the dummy MAC address. If the Is Active check box displays as checked and disabled, licensing consumes device license units for the phone, and the phone can register with Cisco Unified Communications Manager.
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.
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 Communications Manager 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 Table 60-1 in the "Translation Pattern Configuration Settings" section on page 60-1 for more information about the calling line ID presentation and the connected line ID presentation parameters. For more information about call display restrictions, refer to the "Call Display Restrictions" chapter in 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.

Table 91-1 Phone Configuration Settings (continued)

Field	Description
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 Communications Manager 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 Communications Manager 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. Refer to the "Synchronizing a Phone" section on page 91-32.
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 tone to play. For a detailed description of the secure-tone feature and the configuration requirements, see the *Cisco Unified Communications Manager Security Guide*.
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 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. For more information on packet capturing, refer to the *Troubleshooting Guide for Cisco Unified Communications Manager*.

Table 91-1 Phone Configuration Settings (continued)

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, refer to 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, refer to 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. Refer to the "Presence" chapter in 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). Refer to 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.

Table 91-1 Phone Configuration Settings (continued)

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 Communications Manager 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 Communications Manager 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. For information on how to configure a calling search space, see the “Calling Search Space Configuration” section on page 53-1

Table 91-1 Phone Configuration Settings (continued)

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 Across Different DNs—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 that is assigned to both Line 8 and 9 and 1508 that is 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 (refer to the “Synchronizing a Phone” section on page 91-32), the digest credentials for the user get added to the phone configuration file. For more information on digest authentication, refer to 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.

Table 91-1 Phone Configuration Settings (continued)

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 Communications Manager 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, refer to the *Cisco Unified Communications Manager Security Guide*.

Table 91-1 Phone Configuration Settings (continued)

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.

Table 91-1 Phone Configuration Settings (continued)

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	
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.
External Data Locations Information (Leave blank to use default)	
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.
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 CM User Options window that was configured during installation. Leave this field blank to accept the default setting.

Table 91-1 Phone Configuration Settings (continued)

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 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.
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	
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 Communications Manager rejects the value. Cisco Unified Communications Manager 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 (refer to the "Synchronizing a Phone" section on page 91-32). For more information on symmetric key operations for encrypted configuration file downloads, refer to the *Cisco Unified Communications Manager Security Guide*.

Table 91-1 Phone Configuration Settings (continued)

Field	Description
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 Communications Manager transmits or blocks caller ID. If you want the Cisco Unified Communications Manager to send caller ID, choose *Allowed.* If you do not want the Cisco Unified Communications Manager to send caller ID, choose *Restricted.* *Default* specifies that caller ID does not get sent.
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 Communications Manager 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 Communications Manager. (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 Communications Manager. 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.

Table 91-1 Phone Configuration Settings (continued)

Field	Description
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 Communications Manager 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.
Gatekeeper Controlled H.323 Client	This check box enables the gatekeeper control of the H.323 client.
Associated Mobility Identity	
(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.
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. **Note** This field displays only after a Cisco Unified Mobile Communicator device has been added.
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. **Note** This field displays only after a Cisco Unified Mobile Communicator device has been added.
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 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.

Table 91-1 Phone Configuration Settings (continued)

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 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*. **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.
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 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*.
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.

Table 91-1 Phone Configuration Settings (continued)

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 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	
Secure Shell User	Enter a user ID for the secure shell user. 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. Refer to 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. Refer to 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.
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. See the "Modifying Phone Button Template Button Items" section on page 91-39 for a detailed procedure.
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. See the "Configuring a Directory Number" section on page 64-25 for a detailed procedure.

Table 91-1 Phone Configuration Settings (continued)

Field	Description
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. See the "Configuring Speed-Dial Buttons or Abbreviated Dialing" section on page 91-34 for a detailed procedure.
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. See the "Configuring Service URL Buttons" section on page 91-37 for a detailed procedure.
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 Configuration window displays for this phone. See the "BLF/Speed Dial Configuration Settings" section on page 91-26 for more information.
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 Configuration window displays for this phone. For more information on configuring BLF/Directed Call Park buttons, refer to the "Call Park and Directed Call Park" chapter in 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, refer to the documentation for the specific device that you are configuring or contact the manufacturer.

Phone Migration Settings

For information on migrating existing phone settings to a different phone, see the "Migrating Existing Phone Configuration to a Different Phone" section on page 91-30.

Speed-Dial and Abbreviated-Dial Configuration Settings

Table 91-2 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 Table 91-2 apply to both sections.

The system provides a total of 99 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 99 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. Refer to the phone user guide for information.

Table 91-2 Speed-Dial and Abbreviated-Dial Configuration Settings

Field	Description
(number from 1 to 99 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.
Label	Enter the text that you want to display for the speed-dial button or abbreviated-dial number. Cisco Unified Communications Manager does not make this field available for the Cisco Unified IP Phone 7910.
ASCII Label	This field provides the same information as the *Label* field, but you must limit input to ASCII characters. Devices that do not support unicode (internationalized) characters display the content of the *ASCII Label* field.

Additional Information

See the "Related Topics" section on page 91-42.

BLF/Speed Dial Configuration Settings

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, refer to the "Presence" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

BLF/Directed Call Park Configuration Settings

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, refer to the "Call Park and Directed Call Park" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Finding a Phone

Because you might have thousands of Cisco Unified IP Phones in your network, Cisco Unified Communications Manager lets you search for phones on the basis of specified criteria. Follow these steps to search for a specific Cisco Unified IP Phone in the Cisco Unified Communications Manager database.

Note 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. See the "Gateway Configuration" section on page 90-1 for configuration information on the Cisco VG248 and VG224 Gateways.

Tip For methods to limit your search, refer to the "Phone Search" section in the *Cisco Unified Communications Manager System Guide*. To search for devices to which users are actively logged in, see the "Finding an Actively Logged-In Device" section on page 91-40.

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

Tip For phones that have an IPv4 address only or both IPv4 and IPv6 addresses, the IPv4 address displays in the Find and List Phones window; for phones that have an IPv6 address only, the IPv6 address displays in the Find and List Phones window.

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 To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 91-42.

Configuring Cisco Unified IP Phones

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.

Note Add the Cisco VG248 and VG224 Phone Ports from the Gateway Configuration window of Cisco Unified Communications Manager Administration. See the "Gateway Configuration" section on page 90-1 for configuration information.

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. See the "Configuring Phone Button Templates" section on page 98-3 and the "Creating Nonstandard Softkey Templates" section on page 99-2 for configuration information.

Procedure

Step 1 Choose **Device** > **Phone**.

The Find and List Phones window displays.

Step 2 Perform one of the followings tasks:

Note For information on obtaining the MAC address, see the "Displaying the MAC Address of a Phone" section on page 91-41.

- To copy an existing phone, locate the appropriate phone as described in "Finding a Phone" section on page 91-26, click the **Copy** button next to the phone that you want to copy, and continue with Step 5.
- 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 as described in "Finding a Phone" section on page 91-26, click the **Super Copy** button next to the phone that you want to copy, and continue with Step 5.

  Note The lines that get copied become shared lines between the original phone and the new phone.

- To add a new phone, click the **Add New** button and continue with Step 3.
- To update an existing phone, locate the appropriate phone as described in "Finding a Phone" section on page 91-26 and continue with Step 5.

Step 3 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.

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.

The Phone Configuration window displays.

Step 5 Enter the appropriate settings as described in Table 91-1.

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 with the "Directory Number Configuration Settings" section on page 64-1.

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. For more information about the **Apply Config** button, see the "Synchronizing a Phone" section on page 91-32.

Next Steps

To configure speed-dial buttons on this phone, see the "Configuring Speed-Dial Buttons or Abbreviated Dialing" section on page 91-34. To configure services for this phone, see the "Configuring IP Phone Services" section on page 91-35. To configure service URL buttons for this phone, see the "Adding an IP Phone Service to a Phone Button" section on page 100-9. To configure busy lamp field/speed-dial settings for this phone, see the "BLF/Speed Dial Configuration Settings" section on page 91-26.

Additional Information

For more information on phone configuration, as well as H.323 clients, CTI ports, and other devices from Cisco Unified Communications Manager Administration, see the "Related Topics" section on page 91-42.

Migrating Existing Phone Configuration to a Different 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 following topics:

- Before You Begin, page 91-30—information to review before you migrate the settings.
- Procedure, page 91-31—procedure to perform for migrating the settings.
- Table 91-3—configuration settings that display in the Phone Migration Configuration window

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, refer to 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 Find the phone configuration that you want to migrate, as described in the "Finding a Phone" section on page 91-26.

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 91-3.

Step 5 Click **Save**.

Step 6 If a warning displays that the new phone may lose feature functionality, click **OK**.

Table 91-3 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, refer to the Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager that supports your phone model.
Description	If you want to do so, enter a description for the new phone.

Additional Information

See the "Related Topics" section on page 91-42.

Resetting a Phone

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 You can also refer to the "Synchronizing a Phone" section on page 91-32 for instructions on updating the phone with the latest configuration changes by using the least-intrusive method.

Note If a call is in progress, the phone does not reset until the call completes.

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 Check the check boxes next to the phones that you want to reset. To choose all the phones in the window, click **Select All**.

Step 4 Click **Reset Selected**.

The Device Reset window displays.

Step 5 Click one of the following buttons:

- **Restart**—Restarts the chosen devices without shutting them down (reregisters the phones with Cisco Unified Communications Manager).
- **Reset**—Shuts down the chosen devices and brings them back up (performs a complete shutdown and reinitialization of the phones).
- **Close**—Returns you to the previous window without restarting or resetting the chosen devices.

Additional Information

See the "Related Topics" section on page 91-42.

Synchronizing a 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**.

Additional Information

See the "Related Topics" section on page 91-42.

Deleting a Phone

To delete a Cisco Unified IP Phone by using Cisco Unified Communications Manager Administration, perform the following procedure.

Before You Begin

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, see the "Removing a Directory Number from a Phone" section on page 64-28; otherwise, the directory number remains in the Cisco Unified Communications Manager database when the phone gets deleted. To delete a directory number from the database, see the "Deleting Unassigned Directory Numbers" section on page 67-2.

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, see the "Accessing Dependency Records" section on page A-2.

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 Perform one of the following actions:

- Check the check boxes next to the phones that you want to delete and click **Delete Selected**.
- Delete all the phones in the window by clicking **Select All** and clicking **Delete Selected**.
- Choose the name of the phone that you want to delete from the list to display its current settings and click **Delete**.

A confirmation dialog displays.

Step 4 Click **OK**.

Additional Information

See the "Related Topics" section on page 91-42.

Configuring 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 CM User Options to change the speed-dial buttons on their phones.

Table 91-2 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 91-2 apply to both sections.

The system provides a total of 99 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 99 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. Refer to 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 91-2.

Step 3 To apply the changes, click **Save**.

Step 4 To close the window, click **Close**.

Additional Information

See the "Related Topics" section on page 91-42.

Configuring IP Phone Services

From certain phones, such as Cisco Unified IP Phone 7970, 7960, and 7940, 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 set up the available services for phones. Users use the Cisco Unified CM User Options menu to modify the services. For information about the Cisco Unified CM User Options menu, refer to the Cisco Unified IP Phone User Guide that is specific to your phone model. For more information on maintaining services in Cisco Unified Communications Manager Administration, see the "IP Phone Services Configuration" section on page 100-1.

See the following sections for details of subscribing to a phone service, updating a phone service, and unsubscribing from a phone service:

- Subscribing to a Service, page 91-35
- Updating Services, page 91-36
- Unsubscribing from a Service, page 91-37

Subscribing to a Service

To subscribe to new services for a phone, perform the following steps.

Before You Begin

Add the phone services to Cisco Unified Communications Manager. For more information, see the "Configuring an IP Phone Service" section on page 100-5.

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.

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 through Step 8.

Additional Information

See the "Related Topics" section on page 91-42.

Updating Services

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**.

Additional Information

See the "Related Topics" section on page 91-42.

Unsubscribing from a 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.

Additional Information

See the "Related Topics" section on page 91-42.

Configuring Service URL Buttons

From Cisco Unified IP Phones 7970, 7960, and 7940, 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 and then configure that button for the phone. Users use the Cisco Unified CM User Options menu to modify the services. For information about the Cisco Unified CM User Options menu, refer to the Cisco Unified IP Phone User Guide that is specific for your phone model. For more information on maintaining services in Cisco Unified Communications Manager Administration, see the "IP Phone Services Configuration" section on page 100-1.

Adding a 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. For more information, see the "Configuring an IP Phone Service" section on page 100-5.

- Configure the service URL button on the phone button template. For more information, see the "Configuring Phone Button Templates" section on page 98-3.
- Subscribe to the service. See the "Configuring IP Phone Services" section on page 91-35.

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 values in the Label and ASCII Label fields.

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 Step 5 through Step 7.

Step 9 To close this window and return to the Phone Configuration window, click **Close**.

Additional Information

See the "Related Topics" section on page 91-42.

Copy to a Remote Destination Profile

You can copy information from a phone record to a new remote destination profile, which is used for Mobile Connect and Mobile Voice Access. See Cisco Unified Mobility in 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 "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**.

Additional Information

- See the "Related Topics" section on page 91-42.
- Cisco Unified Mobility, *Cisco Unified Communications Manager Features and Services Guide*

Modifying 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 "SEP*999999999999*-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 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 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 To continue, click **OK**.

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 To change the order of the associated items, select an item in the Associated Items pane and click the up or down arrows to change its order.

Step 7 To move an item from the Associated Items pane to the Unassigned Associated Items pane or vice versa, select the item in either pane and click the left or right arrows to move the item to the other pane.

Step 8 To move an item from the Associated Items or Unassigned Associated Items pane to the Dissociate These Items pane or vice versa, select the item in any pane and click the up or down arrows that are located between the two panes that you want to affect.

Step 9 After you have finished moving items among the panes and all items are in the desired order, click **Save**.

Step 10 To close the Reorder Phone Button Configuration window, click **Close**.

Additional Information

See the "Related Topics" section on page 91-42.

Finding an Actively Logged-In Device

The Cisco Extension Mobility feature keeps a record of the devices to which users are actively logged in. 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 logged in.

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

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 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 Device 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.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 91-42.

Displaying the MAC Address of a Phone

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, refer to 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. See the "Gateway Configuration" section on page 90-1 for configuration information.
- 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. See the "Gateway Configuration" section on page 90-1 for configuration information.
- 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.

Additional Information

See the "Related Topics" section on page 91-42.

Related Topics

- Phone Configuration Settings, page 91-2
- Phone Migration Settings, page 91-24
- Speed-Dial and Abbreviated-Dial Configuration Settings, page 91-25
- BLF/Speed Dial Configuration Settings, page 91-26
- BLF/Directed Call Park Configuration Settings, page 91-26
- Finding a Phone, page 91-26
- Configuring Cisco Unified IP Phones, page 91-27
- Migrating Existing Phone Configuration to a Different Phone, page 91-30
- Resetting a Phone, page 91-32
- Synchronizing a Phone, page 91-32
- Deleting a Phone, page 91-33
- Configuring Speed-Dial Buttons or Abbreviated Dialing, page 91-34
- Configuring IP Phone Services, page 91-35
- Configuring Service URL Buttons, page 91-37
- Modifying Phone Button Template Button Items, page 91-39
- Finding an Actively Logged-In Device, page 91-40
- Displaying the MAC Address of a Phone, page 91-41
- Directory Number Configuration, page 64-1
- Gateway Configuration, page 90-1
- Phone Button Template Configuration, page 98-1
- IP Phone Services Configuration, page 100-1
- Cisco Unified IP Phones, *Cisco Unified Communications Manager System Guide*
- Programmable Line Keys, *Cisco Unified Communications Manager System Guide*
- Phone Features, *Cisco Unified Communications Manager System Guide*
- Understanding Directory Numbers, *Cisco Unified Communications Manager System Guide*
- Presence, *Cisco Unified Communications Manager Features and Services Guide*
- Cisco Unified Mobility, *Cisco Unified Communications Manager Features and Services Guide*
- Trusted Relay Point, *Cisco Unified Communications Manager System Guide*

CHAPTER 92

Trunk Configuration

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

The following topics cover Cisco Unified Communications Manager trunk configuration:

- Trunk Configuration Settings, page 92-1
- Finding a Trunk, page 92-46
- Configuring a Trunk, page 92-48
- Deleting a Trunk, page 92-49
- Resetting a Trunk, page 92-49
- Synchronizing a Trunk, page 92-50
- Related Topics, page 92-51

Trunk Configuration Settings

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 “Configuring SIP Profiles” section on page 101-10, SIP Trunk Security Profile Configuration, and 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.

Table 92-1 describes the trunk configuration settings for gatekeeper-controlled H.225 trunks, gatekeeper-controlled intercluster trunks, and non-gatekeeper-controlled intercluster trunks.

Table 92-2 describes the trunk configuration settings for SIP trunks.

For more information about related procedures, see the "Related Topics" section on page 92-51.

Table 92-1 Trunk Configuration Settings for H.225 and Intercluster Trunks

Field	Description
Device Information	
Device Name	Enter a unique identifier for the trunk.
Description	Enter a descriptive name for the trunk.
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.
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.

Table 92-1 Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)

Field	Description
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 more details about locations, see the "Location Configuration" section on page 17-1. For an explanation of location-based CAC across intercluster trunks, see "Location-Based Call Admission Control Over Intercluster Trunk" in 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.

Table 92-1 Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)

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 more information, refer to Chapter 25, "Service Parameters Configuration." • For information on QSIG support with Cisco Unified Communications Manager, refer to "Q.Signaling (QSIG)" in the "Understanding IP Telephony Protocols" chapter of the *Cisco Unified Communications Manager System Guide*.

Table 92-1 Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)

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 more information, refer to Chapter 25, "Service Parameters Configuration." • For information on QSIG support with Cisco Unified Communications Manager, refer to "Q.Signaling (QSIG)" in the "Understanding IP Telephony Protocols" chapter of the *Cisco Unified Communications Manager System Guide*.

Table 92-1 Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)

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, refer to 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, refer to the *Cisco Unified Communications Manager Troubleshooting Guide*.

Table 92-1 Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)

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.

Table 92-1 Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)

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, refer to 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.

Table 92-1 Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)

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 "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 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. Refer to the "Trusted Relay Point" section and its subtopics in the "Media Resource Management" chapter of the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.
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**.

Table 92-1 Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)

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 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, 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 "Configuring the Incoming Calling Party Settings in the Device Pool, Gateway, or Trunk Configuration Windows" in the *Cisco Unified Communications Manager Features and Services Guide*.

Table 92-1 Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)

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 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, 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 "Configuring the Incoming Calling Party Settings in the Device Pool, Gateway, or Trunk Configuration Windows" in the *Cisco Unified Communications Manager Features and Services Guide*.

Table 92-1 Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)

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 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 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 "Configuring the Incoming Calling Party Settings in the Device Pool, Gateway, or Trunk Configuration Windows" in the *Cisco Unified Communications Manager Features and Services Guide*.

Table 92-1 Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)

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 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 "Configuring the Incoming Calling Party Settings in the Device Pool, Gateway, or Trunk Configuration Windows" in the *Cisco Unified Communications Manager Features and Services Guide*.
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.

Table 92-1 Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)

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. Find and choose a calling search space name by using the Finding a Calling Search Space procedure in the *Cisco Unified Communications Manager Administration Guide*. **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.

Table 92-1 Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)

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.
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 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.

Table 92-1 Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)

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.
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 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.

Table 92-1 Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)

Field	Description
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.

Table 92-1 Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)

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.

Table 92-1 Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)

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.

Table 92-1 Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)

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 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.
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.

Table 92-1 Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)

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. **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.
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.

Table 92-1 Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)

Field	Description
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.
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. Refer to the command reference documentation for your gatekeeper for more information.

Table 92-1 Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)

Field	Description
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.
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.

Table 92-1 Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)

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, refer to "Introducing Geolocations" and "Geolocation Configuration" in the "Geolocations and Location Conveyance" chapter in the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocations, refer to the "Logical Partitioning" chapter 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 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, refer to "Introducing Geolocation Filters" and "Geolocation Filter Configuration" in the "Geolocations and Location Conveyance" chapter in the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocation filters, refer to the "Logical Partitioning" chapter in 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, refer to the "Logical Partitioning" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Table 92-2 describes the trunk configuration settings for SIP trunks.

Table 92-2 Trunk Configuration Settings for SIP Trunks

Field	Description
Device Information	
Device Name	Enter a unique identifier for the trunk.
Description	Enter a descriptive name for the trunk.

Table 92-2 Trunk Configuration Settings for SIP Trunks (continued)

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.

Table 92-2 Trunk Configuration Settings for SIP Trunks (continued)

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 more details about locations, see the "Location Configuration" section on page 17-1. For an explanation of location-based CAC across intercluster trunks, see "Location-Based Call Admission Control Over Intercluster Trunk" in 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.

Table 92-2 Trunk Configuration Settings for SIP Trunks (continued)

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, refer to 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, refer to the *Cisco Unified Communications Manager Troubleshooting Guide*.

Table 92-2 Trunk Configuration Settings for SIP Trunks (continued)

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.

Table 92-2 Trunk Configuration Settings for SIP Trunks (continued)

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.
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.
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, refer to the *Cisco Unified Communications Manager Security Guide*.

Table 92-2 Trunk Configuration Settings for SIP Trunks (continued)

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 "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 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. Refer to the "Trusted Relay Point" section and its subtopics in the "Media Resource Management" chapter of the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.
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**.

Table 92-2 Trunk Configuration Settings for SIP Trunks (continued)

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 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 "Configuring the Incoming Calling Party Settings in the Device Pool, Gateway, or Trunk Configuration Windows" in the *Cisco Unified Communications Manager Features and Services Guide*.

Table 92-2 Trunk Configuration Settings for SIP Trunks (continued)

Field	Description
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.

Table 92-2 Trunk Configuration Settings for SIP Trunks (continued)

Field	Description
Call Routing Information	
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. **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.

Table 92-2 Trunk Configuration Settings for SIP Trunks (continued)

Field	Description
Asserted Identity	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.

Table 92-2 Trunk Configuration Settings for SIP Trunks (continued)

Field	Description
Asserted Identity (continued)	**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 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.

Table 92-2 Trunk Configuration Settings for SIP Trunks (continued)

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.

Table 92-2 Trunk Configuration Settings for SIP Trunks (continued)

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.
Connected Name Presentation	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.
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 by using the Finding a Calling Search Space procedure in the *Cisco Unified Communications Manager Administration Guide*. **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.
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.

Table 92-2 Trunk Configuration Settings for SIP Trunks (continued)

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 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.
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 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.
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.

Table 92-2 Trunk Configuration Settings for SIP Trunks (continued)

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 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.
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.

Table 92-2 Trunk Configuration Settings for SIP Trunks (continued)

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 +.
Caller Name	Enter a caller name to override the caller name that is received from the originating SIP Device.
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.

Table 92-2 Trunk Configuration Settings for SIP Trunks (continued)

Field	Description
SIP Information	
Destination Address	The Destination Address represents the remote SIP peer with which this trunk will communicate. The allowed values for this field specify a valid V4 dotted IP address, fully qualified domain name (FQDN), or DNS SRV record only if the *Destination Address is an SRV* field is checked. **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.

Table 92-2 Trunk Configuration Settings for SIP Trunks (continued)

Field	Description
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 valid IPv6 address (global unicast, unique local, or a host name) • 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.
Destination Port	Choose the destination port. Ensure that the value that you enter specifies any port from 1024 - 65535. **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.

Table 92-2 Trunk Configuration Settings for SIP Trunks (continued)

Field	Description
MTP Preferred Originating Codec	Indicate the preferred outgoing codec: • 711ulaw • 711alaw • G729/G729a • G729b/G729ab **Note** To configure G.79 codecs for use with a SIP trunk, you must use a hardware MTP or transcoder that supports the G.79 codec. For more information, see Chapter 26, "Transcoders," in 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. Refer to the "Presence" chapter in 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.

Table 92-2 Trunk Configuration Settings for SIP Trunks (continued)

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, refer to 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.

Table 92-2 Trunk Configuration Settings for SIP Trunks (continued)

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. For information on how to configure a calling search space, see the "Calling Search Space Configuration" section on page 53-1.
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).

Table 92-2 Trunk Configuration Settings for SIP Trunks (continued)

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, refer to "Introducing Geolocations" and "Geolocation Configuration" in the "Geolocations and Location Conveyance" chapter in the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocations, refer to the "Logical Partitioning" chapter 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 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, refer to "Introducing Geolocation Filters" and "Geolocation Filter Configuration" in the "Geolocations and Location Conveyance" chapter in the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocation filters, refer to the "Logical Partitioning" chapter in 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, refer to the "Logical Partitioning" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Finding a 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.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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.

Additional Topics

See the "Related Topics" section on page 92-51.

Configuring a 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 "Configuring SIP Profiles" section on page 101-10, SIP Trunk Security Profile Configuration, 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:

- To add a new trunk device, click the **Add New** button. The Trunk Configuration window displays. Continue with Step 3.
- To update trunk settings, locate the appropriate trunk as described in "Finding a Trunk" section on page 92-46. Click the name of the trunk that you want to update. Continue with Step 6.

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 Click **Next**.

Step 6 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 92-1. For SIP trunks, enter the appropriate settings as described in Table 92-2.

Step 7 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). For more information about the **Apply Config** button, see the "Synchronizing a Trunk" section on page 92-50.

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

Additional Topics

See the "Related Topics" section on page 92-51.

Deleting a 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. For more information about dependency records, see the "Accessing Dependency Records" section on page A-2. 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. See the "Configuring a Route Pattern" section on page 44-11.
- Delete the route patterns that are using the trunk that you want to delete. See the "Deleting a Route Pattern" section on page 44-12.

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:

- Check the check boxes next to the trunks that you want to delete and click **Delete Selected**.
- Delete all trunks in the window by clicking **Select All** and then clicking **Delete Selected**.
- 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**.

Additional Topics

See the "Related Topics" section on page 92-51.

Resetting a 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 Trunk.**

The Device Reset dialog displays.

Step 5 Click one of the following choices:

- **Restart**—Restarts the trunk device without shutting it down first.
- **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.
- **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.

Additional Topics

See the "Related Topics" section on page 92-51.

Synchronizing a Trunk

To synchronize a trunk with the most recent configuration changes, perform the following procedure, which will apply any outstanding configuration settings in the least-intrusive manner possible. (For example, a reset/restart may not be required on some affected devices.)

Procedure

Step 1 Choose **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.

Additional Topics

See the "Related Topics" section on page 92-51.

Related Topics

- Trunk Configuration Settings, page 92-1
- Finding a Trunk, page 92-46
- Configuring a Trunk, page 92-48
- Deleting a Trunk, page 92-49
- Resetting a Trunk, page 92-49
- Synchronizing a Trunk, page 92-50
- Configuring SIP Profiles, page 101-10
- SIP Trunk Security Profile Configuration
- Call Admission Control, *Cisco Unified Communications Manager System Guide*
- Gatekeepers and Trunks, *Cisco Unified Communications Manager System Guide*
- Gatekeeper and Trunk Configuration in Cisco Unified Communications Manager, *Cisco Unified Communications Manager System Guide*
- Trusted Relay Point, *Cisco Unified Communications Manager System Guide*
- Local Route Groups, *Cisco Unified Communications Manager Features and Services Guide*
- *Cisco Unified Communications Manager Security Guide*
- *Cisco Unified Communications Solution Reference Network Design (SRND)*

CHAPTER 93

Remote Destination Configuration

The Cisco Unified Mobility Mobile Connect 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 Mobile Connect 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 Mobile Connect, Mobile Voice Access, and other Cisco Unified Mobility features, as well as how to configure remote destinations, refer to the Cisco Unified Mobility chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

CHAPTER 94

Device Defaults Configuration

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.

This section covers the following topics:

- Device Defaults Configuration Settings, page 94-1
- Updating Device Defaults, page 94-2
- Related Topics, page 94-3

Device Defaults Configuration Settings

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.

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. See the "Configuring a Device Pool" section on page 9-11.
- If the device is a phone, configure new phone templates. See the "Configuring Phone Button Templates" section on page 98-3.

Table 94-1 describes the configuration settings for device defaults. For more information about related procedures, see the "Related Topics" section on page 94-3.

Table 94-1 Device Defaults Configuration 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.

Updating 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. See the "Configuring a Device Pool" section on page 9-11.
- If the device is a phone, configure new phone templates. See the "Configuring Phone Button Templates" section on page 98-3.

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 94-1.

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.

Additional Information

See the "Related Topics" section on page 94-3.

Related Topics

- Device Defaults Configuration Settings, page 94-1
- Updating Device Defaults, page 94-2
- Finding Devices With Non-Default Firmware Loads, page 95-1
- Device Firmware Loads, *Cisco Unified Communications Manager System Guide*

CHAPTER 95

Device Firmware Load Information

Use device firmware load information to locate devices that are not using the default firmware load for their device type.

Finding 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.

Related Topics

- Updating Device Defaults, page 94-2
- Related Topics, page 94-3

CHAPTER 96

Default Device Profile Configuration

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. Device profiles include device type, user locale, phone button template, softkey template, Join Across Lines and Single Button Barge feature settings, multilevel precedence and preemption (MLPP) information, and IP phone services.

This chapter contains information on the following topics:

- Default Device Profile Configuration Settings, page 96-1
- Configuring a Default Device Profile, page 96-6
- Deleting a Default Device Profile, page 96-7
- Related Topics, page 96-7

Default Device Profile Configuration Settings

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, phone template, user locale, expansion modules, softkey template, Join Across Lines and Single Button Barge feature settings, and MLPP information.

Table 96-1 describes the fields that are available in the Default Device Profile Configuration window. For related procedures, see the "Related Topics" section on page 96-7.

Table 96-1 Default Device Profile Configuration Settings

Field	Description
Default Device Profile Information	
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. Refer to 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, refer to "Barge and Privacy" in the *Cisco Unified Communications Manager Features and Services Guide*.

Table 96-1 Default Device Profile Configuration Settings (continued)

Field	Description
Single Button Barge/cBarge	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, refer to "Barge and Privacy" in 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, refer to "Understanding Directory Numbers" in 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.

Table 96-1 Default Device Profile Configuration Settings (continued)

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, refer to "Call Display Restrictions" in 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.

Table 96-1 Default Device Profile Configuration Settings (continued)

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.

Table 96-1 Default Device Profile Configuration Settings (continued)

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.

Configuring a Default Device Profile

The default device profile contains attributes such as device type, phone template, user locale, expansion modules, softkey template, Join Across Lines and Single Button Barge feature settings, and MLPP information. Perform the following procedure to add or update a default device profile.

Procedure

Step 1 Choose **Device** > **Device Settings** > **Default Device Profile**.

The Default Device Profile Configuration window displays.

Step 2 Perform one of the followings tasks:

- To add a new profile, choose the type of device that you want to add from the Device Profile Type drop-down list box; then, click **Next** and continue with Step 3.
- To update an existing profile, click the device profile that you want to update from the Device Profile Defaults pane. The Default Device Profile Configuration window displays the profile information of the profile that you chose; continue with Step 3

Step 3 Enter the appropriate settings in the profile as described in Table 96-1.

Step 4 Click **Save**.

Additional Topics

See the "Related Topics" section on page 96-7.

Deleting a Default Device Profile

This section describes how to delete a default device profile.

Procedure

Step 1 Choose **Device** > **Device Settings** > **Default Device Profile**.

Step 2 From the Default Device Profile pane, click the device profile that you want to delete.

The Default Device Profile Configuration window displays the profile information of the profile that you chose.

Step 3 Click **Delete**.

A message displays that states that this action cannot be undone.

Step 4 To delete the default device profile, click **OK** or, to cancel the deletion, click **Cancel**.

Additional Topics

See the "Related Topics" section on page 96-7.

Related Topics

- Default Device Profile Configuration Settings, page 96-1
- Configuring a Default Device Profile, page 96-6
- Deleting a Default Device Profile, page 96-7

CHAPTER 97

Device Profile Configuration

A device profile comprises the set of attributes (services and/or features) that are associated with a particular device. Device profiles include name, description, phone template, add-on modules, softkey templates, feature settings, multilevel precedence and preemption (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 Communications Manager 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. For more information about the device profile default, see the "Default Device Profile Configuration" section on page 96-1.

Use the following topics to configure and locate device profiles:

- Device Profile Configuration Settings, page 97-1
- Finding a Device Profile, page 97-8
- Configuring a Device Profile, page 97-8
- Deleting a Device Profile, page 97-11

Device Profile Configuration Settings

A device profile comprises the set of attributes (services and/or features) that are associated with a particular device. Device profiles include name, description, phone template, add-on modules, softkey templates, feature settings, multilevel precedence and preemption (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 Communications Manager 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. For more information about the device profile default, see the "Default Device Profile Configuration" section on page 96-1.

Before You Begin

Make sure that phone button template(s) are already configured before you configure the device profile. See the "Configuring Phone Button Templates" section on page 98-3 for more information.

Table 97-1 describes the available settings in the Device Profile Configuration window. For more information about related procedures, see the "Related Topics" section on page 97-11.

Table 97-1 Device Profile Configuration 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.
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**.

Table 97-1 Device Profile Configuration Settings (continued)

Field	Description
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. Refer to 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, refer to "Presence" in 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, refer to "Barge and Privacy" in the *Cisco Unified Communications Manager Features and Services Guide*.

Table 97-1 Device Profile Configuration Settings (continued)

Field	Description
Single Button Barge/cBarge	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, refer to "Barge and Privacy" in 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, refer to "Understanding Directory Numbers" in 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.

Table 97-1 Device Profile Configuration Settings (continued)

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, refer to the Call Display Restrictions chapter in 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.

Table 97-1 Device Profile Configuration Settings (continued)

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.
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**.

Table 97-1 Device Profile Configuration Settings (continued)

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: • **Default**—This device profile inherits its MLPP indication setting from the device pool of the associated device. • **Off**—This device does not handle nor process indication of an MLPP precedence call. • **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: • **Default**—This device profile inherits its MLPP preemption setting from the device pool of the associated device. • **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 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.

Finding a Device Profile

Procedure

Step 1 Choose **Device** > **Device Settings** > **Device Profile.**

The Find and List Device Profiles 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.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 97-11.

Configuring a Device Profile

The user device profile contains attributes such as device profile name, description, phone template, user locale, expansion modules, softkey template, feature settings, MLPP information, directory numbers, subscribed services, and speed-dial information. Perform the following procedure to add or update a user device profile.

Before You Begin

Make sure that phone button template(s) are already configured before proceeding with the steps. See the "Configuring Phone Button Templates" section on page 98-3 for more information.

Procedure

Step 1 Choose **Device** > **Device Settings** > **Device Profile**.

The Find and List Device Profile window displays.

Step 2 Perform one of the followings tasks:

- To copy an existing device profile, locate the appropriate device profile as described in "Finding a Device Profile" section on page 97-8, click the **Copy** button next to the device profile that you want to copy and continue with Step 5.
- To add a new device profile, click the **Add New** button. The Device Profile Configuration window displays. Continue with Step 3.
- To update an existing device profile, locate the appropriate device profile as described in "Finding a Device Profile" section on page 97-8, and continue with Step 5.

Note Before updating a device profile, make sure that the device profile that you want to update is configured in Cisco Unified Communications Manager.

Step 3 From the Device Profile Type drop-down list box, choose a device type. Click **Next**.

Step 4 If the Select the device profile protocol drop-down list box displays, choose the protocol for the device profile. Click **Next**.

Step 5 Enter the appropriate settings as described in Table 97-1.

Step 6 Click **Save**.

Step 7 From the Association Info pane, you can configure directory numbers, speed dials, and intercom directory numbers for the device profile. Refer to the "Directory Number Configuration" section on page 64-1, the "Cisco Unified IP Phone Configuration" section on page 91-1, and the "Intercom Directory Number Configuration" section on page 56-1 for the appropriate settings as described in these sections.

Step 8 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. Refer to the "Modifying Phone Button Template Button Items" section on page 91-39 for the appropriate settings for this window.

Note You must log in to a device for changes to a user device profile to take effect.

Additional Configuration

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. See "Directory Number Configuration Settings" section on page 64-1 for the details of the fields in this window.
- **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. See "Configuring Speed-Dial Buttons or Abbreviated Dialing" section on page 91-34 for configuration details of this window.
- **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 "Configuring BLF/SpeedDial Buttons" in 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 "BLF/Directed Call Park Configuration Settings" in 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. See the "Configuring Service URL Buttons" section on page 91-37 for configuration details of this window.
- **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. See the "Configuring IP Phone Services" section on page 91-35 for configuration details of this window.

Additional Information

See the "Related Topics" section on page 97-11.

Deleting a Device Profile

This section describes how to delete a user device profile.

Before You Begin

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. For more information about dependency records, see the "Accessing Dependency Records" section on page A-2. 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.

Procedure

Step 1 Locate the user device profile that you want to delete. See the "Finding a Device Profile" section on page 97-8.

Step 2 From the User Device Profile Configuration window, click **Delete**.

A message displays that states that you cannot undo this action.

Step 3 To delete the device profile, click **OK** or, to cancel the deletion, click **Cancel**.

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.

Additional Information

See the "Related Topics" section on page 97-11.

Related Topics

- Device Profile Configuration Settings, page 97-1
- Finding a Device Profile, page 97-8
- Configuring a Device Profile, page 97-8
- Deleting a Device Profile, page 97-11

Directory Numbers

- Directory Number Configuration, page 64-1
- Directory Number Configuration Settings, page 64-1

Join Across Lines

- Understanding Directory Numbers, *Cisco Unified Communications Manager System Guide*

Single Button Barge/cBarge

- Barge and Privacy, *Cisco Unified Communications Manager Features and Services Guide*

Presence

- Presence, *Cisco Unified Communications Manager Features and Services Guide*

Directed Call Park

- Call Park and Directed Call Park, *Cisco Unified Communications Manager Features and Services Guide*

Phone Configuration

- Cisco Unified IP Phone Configuration, page 91-1

CHAPTER 98

Phone Button Template Configuration

Cisco Unified Communications Manager includes several default phone button templates. When adding phones, you can assign one of these templates to the phones or create a new template.

Creating and using templates provides a fast way 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.

This chapter contains information on the following topics:

Phone Button Template Configuration Settings

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. See the "Updating Device Defaults" section on page 94-2.

Before You Begin

If you are creating a custom, nonstandard phone button template, refer to the guidelines for creating new phone button templates. Refer to the "Guidelines for Customizing Phone Button Templates" section in the *Cisco Unified Communications Manager System Guide*.

Table 98-1 describes the phone button template configuration settings.

Table 98-1 Phone Button Template Configuration 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.

Finding a Phone Button Template

Because you may have several phone button templates in your network, Cisco Unified Communications Manager Administration lets you locate specific phone button templates on the basis of specific criteria. Use the following procedure to locate phone button templates.

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

Procedure

Step 1 Choose **Device > Device Settings > Phone Button Template.**

The Find and List Phone Button 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; go to Step 3.

To filter or search records

- From the first drop-down list box, select a search pattern.
- Specify the appropriate search text, if applicable.

- From the second drop-down list box, select whether to search for standard, non-standard, or both types of phone button 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.

Additional Topics

See the "Related Topics" section on page 98-6.

Configuring 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.

Use the following procedures to add, rename, or update custom, nonstandard templates or to add or remove features, lines, or speed dials.

If you create a template for a Cisco Unified IP Phone, you can change the default template for that phone during auto-registration. See the "Updating Device Defaults" section on page 94-2.

Before You Begin

If you are creating a custom, nonstandard phone button template, refer to the guidelines for creating new phone button templates. See the "Guidelines for Customizing Phone Button Templates" section in the *Cisco Unified Communications Manager System Guide*.

Procedure

Step 1 Choose **Device** > **Device Settings** > **Phone Button Template**.

The Find and List Phone Button Templates window displays.

Step 2 Perform one of the followings tasks:

- To rename an existing phone button template, locate the appropriate phone button template as described in "Finding a Phone Button Template" section on page 98-2. The Phone Button Template Configuration page displays. In the Button Template Name field, enter the new name. Click **Save.** The template redisplays with the new name.

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.

- To add a new phone button template, click the **Add New** button. The Phone Button Template Configuration window displays. Continue with Step 3.
- To update an existing phone button template, locate the appropriate phone as described in "Finding a Phone Button Template" section on page 98-2. From the list of matching records, choose the phone button template that you want to update. The Phone Button Template Configuration window displays. Continue with Step 4.

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 updating the template, you must restart devices that are using the template by clicking **Restart Devices**

Step 3 From the Phone Button Template drop-down list box, choose a template and click **Copy** to create a new template.

The new template exactly duplicates the existing template. You must assign a new name for the new template. Update this new template if you want it to differ from the original.

Step 4 Update the appropriate settings as described in Table 98-1.

Step 5 Click **Save**.

Additional Topics

See the "Related Topics" section on page 98-6.

Configuring a Cisco Unified IP Phone Expansion Module Phone Button Template

You can create a phone button template for a Cisco Unified IP Phone Expansion Module by using the Standard Cisco IP Phone 7960 phone button template as described in the following procedure.

Procedure

Step 1 Find the phone button template by using the procedure in the "Finding a Phone Button Template" section on page 98-2.

Step 2 From the list of matching records, locate the Standard 7960 (for SCCP or SIP) phone button template 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 98-1 (the button template name that you just created will already display).

Step 6 Click **Save**.

Additional Topics

See the "Related Topics" section on page 98-6.

Deleting a Phone Button Template

Use this procedure to delete a phone button template.

Before You Begin

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. For more information about dependency records, see the "Accessing Dependency Records" section on page A-2. 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. See the "Deleting a Phone" section on page 91-33.
- Delete the devices that are using the phone button template that you want to delete. See the "Deleting a Phone" section on page 91-33.

Procedure

Step 1 Find the phone button template by using the procedure in the "Finding a Phone Button Template" section on page 98-2.

Step 2 From the list of matching records, choose 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.

The Phone Button Template Configuration window displays.

Step 3 Click **Delete**.

Note You can delete multiple nonstandard phone button templates from the Find and List Phone Button Templates window by checking the check boxes next to the appropriate phone button templates and clicking **Delete Selected**. You can delete all phone button templates in the window by clicking **Select All** and **Delete Selected**. 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

A message verifies that you want to delete the template.

Step 4 To delete the template, click **OK**.

A message verifies that the template was deleted.

Step 5 To continue, click **OK**.

Additional Topics

See the "Related Topics" section on page 98-6.

Related Topics

- Phone Button Template Configuration Settings, page 98-1
- Cisco Unified IP Phone Configuration, page 91-1
- Updating Device Defaults, page 94-2
- Finding a Phone Button Template, page 98-2
- Configuring Phone Button Templates, page 98-3
- Configuring a Cisco Unified IP Phone Expansion Module Phone Button Template, page 98-5
- Deleting a Phone Button Template, page 98-5
- Cisco Unified IP Phones, *Cisco Unified Communications Manager System Guide*
- Guidelines for Customizing Phone Button Templates, *Cisco Unified Communications Manager System Guide*

- Phone Button Templates, *Cisco Unified Communications Manager System Guide*
- Programmable Line Keys, *Cisco Unified Communications Manager System Guide*

CHAPTER 99

Softkey Template Configuration

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.

The administrator can copy, update, or delete nonstandard softkey templates by using softkey template configuration.

The following sections provide details about softkey template configuration:

- Finding a Softkey Template, page 99-1
- Creating Nonstandard Softkey Templates, page 99-2
- Adding Application Softkeys to Nonstandard Softkey Templates, page 99-3
- Configuring Softkey Positions in a Nonstandard Softkey Template, page 99-4
- Modifying Softkey Templates, page 99-5
- Assigning Softkey Templates to IP Phones, page 99-8

Finding a 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; go to Step 3.

To filter or search records

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

Additional Information

See the "Related Topics" section on page 99-9.

Creating 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.

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 If you want to add additional application softkeys to the nonstandard softkey template, see the "Adding Application Softkeys to Nonstandard Softkey Templates" section on page 99-3.

Step 9 To configure the positions of the softkeys on the Cisco Unified IP Phone LCD screen, see the "Configuring Softkey Positions in a Nonstandard Softkey Template" section on page 99-4.

Step 10 To save your configuration, click **Save**.

Additional Information

See the "Related Topics" section on page 99-9.

Adding 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 by using the procedure in the "Finding a Softkey Template" section on page 99-1.

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 on the phone, click **Apply Config.** For more information about the Apply Config button, see the "Synchronizing a Softkey Template Configuration With Affected Devices" section on page 99-8.

Additional Information

See the "Related Topics" section on page 99-9.

Configuring Softkey Positions in a Nonstandard Softkey Template

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 "Finding a Softkey Template" section on page 99-1.

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 on the phone, click **Apply Config.** For more information about the Apply Config button, see the "Synchronizing a Softkey Template Configuration With Affected Devices" section on page 99-8.

Additional Information

See the "Related Topics" section on page 99-9.

Modifying Softkey Templates

You can make changes to custom, nonstandard softkey templates that you created:

- Renaming a Softkey Template, page 99-6
- Deleting a Softkey Template, page 99-6
- Updating a Softkey Template, page 99-7
- Synchronizing a Softkey Template Configuration With Affected Devices, page 99-8

Additional Information

See the "Related Topics" section on page 99-9.

Renaming a Softkey Template

Use this procedure to rename a nonstandard softkey template that you created.

Procedure

Step 1 Find the softkey template by using the procedure in the "Finding a Softkey Template" section on page 99-1.

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.

Additional Information

See the "Related Topics" section on page 99-9.

Deleting a 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. For more information about dependency records, see the "Accessing Dependency Records" section on page A-2. 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. See the "Deleting a Phone" section on page 91-33.
- Delete the devices that are using the nonstandard softkey template that you want to delete. See the "Deleting a Phone" section on page 91-33.

Procedure

Step 1 Find the softkey template by using the procedure in the "Finding a Softkey Template" section on page 99-1.

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.

Additional Information

See the "Related Topics" section on page 99-9.

Updating a 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 by using the procedure in the "Finding a Softkey Template" section on page 99-1.

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). See the "Adding Application Softkeys to Nonstandard Softkey Templates" section on page 99-3 and the "Configuring Softkey Positions in a Nonstandard Softkey Template" section on page 99-4.

Step 4 Click **Save**.

The Softkey Template Configuration window redisplays with the softkey template updated.

Step 5 To apply the updated softkey template to affected devices, click **Apply Config.** For more information about the Apply Config button, see the "Synchronizing a Softkey Template Configuration With Affected Devices" section on page 99-8.

Additional Information

See the "Related Topics" section on page 99-9.

Synchronizing a Softkey Template Configuration With Affected Devices

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

Procedure

Step 1 Choose **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**.

Additional Information

See the "Related Topics" section on page 99-9.

Assigning Softkey Templates to IP Phones

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.

For more information about configuring a common device configuration and phones, refer to the "Configuring a Common Device Configuration" section on page 102-7and the "Configuring Cisco Unified IP Phones" section on page 91-27.

Related Topics

- Finding a Softkey Template, page 99-1
- Creating Nonstandard Softkey Templates, page 99-2
- Modifying Softkey Templates, page 99-5
- Renaming a Softkey Template, page 99-6
- Deleting a Softkey Template, page 99-6
- Synchronizing a Softkey Template Configuration With Affected Devices, page 99-8
- Assigning Softkey Templates to IP Phones, page 99-8
- Softkey Templates, *Cisco Unified Communications Manager System Guide*

CHAPTER 100

IP Phone Services Configuration

Using Cisco Unified Communications Manager Administration, you define and maintain the list of IP phone services to which users can subscribe at their site. IP phone services comprise XML applications that enable the display of interactive content with text and graphics on Cisco Unified IP Phones 7970, 7960, 7940, 7912, and 7905.

Note Cisco Unified IP Phones 7912 and 7905 only support text-based XML applications.

Cisco Unified Communications Manager provides sample IP phone services applications. You can also create customized Cisco Unified IP Phone applications for your site.

After you configure the list of services, you can add services to the phones in the database and assign them to phone buttons. In Cisco Unified Communications Manager Administration, you can view and modify settings for phones and device profiles. Users can log on to the Cisco Unified CM User Options application and subscribe to these services for their Cisco Unified IP Phones.

This section covers the following topics:

IP Phone Service Configuration Settings

Using Cisco Unified Communications Manager Administration, you define and maintain the list of IP phone services to which users can subscribe at their site. IP phone services comprise XML applications that enable the display of interactive content with text and graphics on Cisco Unified IP Phones 7970, 7960, 7940, 7912, and 7905.

Note Cisco Unified IP Phones 7912 and 7905 only support text-based XML applications.

Cisco Unified Communications Manager provides sample IP phone services applications. You can also create customized Cisco Unified IP Phone applications for your site.

After you configure the list of services, you can add services to the phones in the database and assign them to phone buttons. In Cisco Unified Communications Manager Administration, you can view and modify settings for phones and device profiles. Users can log on to Cisco Unified CM User Options and subscribe to these services for their Cisco Unified IP Phones.

Table 100-1 describes the IP phone service configuration settings. See Table 100-2 for information about the IP phone service parameter settings. For more information about related procedures, see the "Related Topics" section on page 100-9.

Table 100-1 IP Phone Service Configuration Settings

Field	Description
Service Information	
Service Name	Enter the name of the service as it will display on the menu of available services in Cisco Unified CM User Options. Enter up to 32 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.
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.
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.
Service Category	Select a service application type (XML or Java MIDlet).
Service Type	Select whether the service will be provisioned to the Services, Directories, or Messages button.
Service Vendor	For Java MIDlet services, enter the service vendor that exactly matches the vendor that is defined in the JAD file. For XML services, you can leave this field blank.
Service Version	You can leave this field blank for XML and Java MIDlet services. If you enter a value for a Java MIDlet service, the value must exactly match the version that is defined in the JAD file; otherwise, the MIDlet will not install or execute.

Table 100-1 IP Phone Service Configuration Settings (continued)

Field	Description
Enable	Select this check box to enable the service, or deselect the check box to disable the service without deleting it. **Note** You cannot delete default services. Use this field if a default service exists, but you do not want to make it available for subscription.
Enterprise Subscriptions	Select this check box to automatically provision the new service to all devices in the enterprise without requiring individual subscription. If this option is selected, the service automatically gets provisioned and does not get presented for user subscription. **Note** Be aware that this check box is available for selection only when the service is created. You cannot modify it.

IP Phone Service Parameter Settings

Add the phone service before you configure IP phone service parameters. Refer to 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 a phone service for a 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.

Table 100-2 describes the IP phone service parameter settings. For more information about related procedures, see the "Related Topics" section on page 100-9.

Table 100-2 IP Phone Service Parameter Settings

Field	Description
Service Parameter Information	
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 CM User Options; 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.

Table 100-2 IP Phone Service Parameter Settings (continued)

Field	Description
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.
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 CM User Options, 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.

Finding an IP Phone Service

Because you might have several IP phone services in your network, Cisco Unified Communications Manager lets you locate specific IP phone services on the basis of specific criteria. Use the following procedure to locate IP phone services.

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

Procedure

Step 1 Choose **Device >Device Settings > Phone Services.**

The Find and List IP Phone Services 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.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 100-9.

Configuring an IP Phone Service

Perform the following steps to add or update an IP phone service.

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 directory database publisher 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.

Procedure

Step 1 Choose **Device >Device Settings > Phone Services**.

The Find and List IP Phone Services window displays.

Step 2 Perform one of the followings tasks:

- To add an IP phone service, click the **Add New** button. The IP phone services Configuration window displays. Continue with Step 3.
- To update an existing IP phone service (for example, to change the service URL or other information), locate the appropriate IP phone service as described in "Finding an IP Phone Service" section on page 100-4. Click the name of the IP phone service that you want to update and continue with Step 3.

Step 3 Enter the appropriate settings as described in Table 100-1.

Step 4 Click **Save**.

You can add, update, or delete parameters as needed as described in "Configuring an IP Phone Service Parameter" section on page 100-7 and "Deleting an IP Phone Service Parameter" section on page 100-8.

Step 5 To apply the changes, update the IP phone services Configuration window:

- 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 a 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.

- If the service is new and you do not need to rebuild user subscriptions, click **Save**.

Additional Information

See the "Related Topics" section on page 100-9.

Deleting an IP Phone Service

Perform the following steps to delete an IP phone service.

Before You Begin

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. For more information about dependency records, see the "Accessing Dependency Records" section on page A-2. 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. See the "Deleting a Phone" section on page 91-33.
- Delete the devices that are using the IP phone service that you want to delete. See the "Deleting a Phone" section on page 91-33.

Procedure

Step 1 Find the IP phone service by using the procedure in the "Finding an IP Phone Service" section on page 100-4.

Step 2 Click the name of the IP phone service that you want to delete.

The IP phone services Configuration window displays.

Step 3 Click **Delete**.

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

Step 4 Click **OK**.

The window refreshes, and the IP phone service gets deleted from the database.

Additional Information

See the "Related Topics" section on page 100-9.

Configuring an IP Phone Service Parameter

Use the following procedure to add and configure or update IP phone service parameters. Add the phone service before you configure parameters. Refer to 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 by using the procedure in the "Finding an IP Phone Service" section on page 100-4.

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:

- To add a new 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.
- 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.

Step 4 Enter the appropriate settings as described in Table 100-2.

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 and Step 4.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:

- 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 name for a phone service parameter.

Note If you remove an IP phone service parameter or change the parameter name of a phone service for a 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.

- If the service is new and you do not need to rebuild user subscriptions, click **Save**.

Additional Information

See the "Related Topics" section on page 100-9.

Deleting an IP Phone Service Parameter

Perform the following steps to delete an IP phone service parameter.

Note If you remove a phone service parameter or modify the Parameter Name of a phone service parameter for a 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 the procedure in the "Finding an IP Phone Service" section on page 100-4.

Step 2 From the IP phone services list, choose the 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:

- 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.

  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.

- If the service is new and you do not need to rebuild user subscriptions, click **Save**.

Additional Information

See the "Related Topics" section on page 100-9.

Adding an IP Phone Service to a Phone Button

In addition to adding an IP phone service, so it is available to users on their phones, you can assign the service to a phone button that is configured as a service URL. This gives the user one-button access to the service without using the services button on the IP phone.

Perform the following steps to add a service to a service URL button:

Procedure

Step 1 Add the service to Cisco Unified Communications Manager (see Configuring an IP Phone Service, page 100-5).

Step 2 Customize a phone button template by configuring a Service URL button (refer to the "Configuring Phone Button Templates" section on page 98-3).

Step 3 Add the customized phone button template to the phone (refer to the "Configuring Cisco Unified IP Phones" section on page 91-27).

Step 4 Subscribe the service to the phone (refer to the "Configuring IP Phone Services" section on page 91-35).

Step 5 Add the service URL to a phone button (refer to the "Configuring Service URL Buttons" section on page 91-37).

Additional Information

See the "Related Topics" section on page 100-9.

Related Topics

- IP Phone Service Configuration Settings, page 100-1
- IP Phone Service Parameter Settings, page 100-3
- Finding an IP Phone Service, page 100-4
- Configuring an IP Phone Service, page 100-5
- Deleting an IP Phone Service, page 100-6
- Configuring an IP Phone Service Parameter, page 100-7
- Deleting an IP Phone Service Parameter, page 100-8
- Adding an IP Phone Service to a Phone Button, page 100-9
- Cisco Unified IP Phone Services, *Cisco Unified Communications Manager System Guide*

CHAPTER 101

SIP Profile Configuration

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.

Use the following topics to configure and locate SIP profiles:

- SIP Profile Configuration Settings, page 101-1
- Finding SIP Profiles, page 101-9
- Configuring SIP Profiles, page 101-10
- Deleting SIP Profiles, page 101-11
- Resetting a SIP Profile, page 101-11
- Synchronizing a SIP Profile With Affected SIP Devices, page 101-12
- Related Topics, page 101-13

SIP Profile Configuration Settings

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.

Table 101-1 describes the available settings in the SIP Profile Configuration window. For more information about related procedures, see the "Related Topics" section on page 101-13.

Table 101-1 SIP Profile Configuration 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.

Table 101-1 SIP Profile Configuration Settings (continued)

Field	Description
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 Network Domain list from the drop-down menu. Configure the lists in the Resource Priority Namespace Network Domain menu that is accessed from the System menu.
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
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 will cause the call to be routed instead of being blocked. This represents the behavior that you will get if the Redirect by Application check box is unchecked. See the "Redirection" section on page 42-17.

Table 101-1 SIP Profile Configuration Settings (continued)

Field	Description
Disable Early Media on 180	By default, Cisco Unified Communications Manager will signal 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 will connect media, and the calling phone will play 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. See the "Use of Early Media" section on page 42-11.
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 92, "Trunk Configuration." **Note** The parameter applies to SIP trunks only, not phones that are running SIP or other endpoints.

Table 101-1 SIP Profile Configuration Settings (continued)

Field	Description
Enable ANAT	This option allows a dual-stack SIP trunk to offer both IPv4 and IPv6 media. When you check both the Enable ANAT and the 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.
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)	Use this parameter in conjunction with the Timer Register Expires setting. The phone will reregister 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 range from 32767 to 0. Default specifies 5.
Timer Register Expires (seconds)	This field specifies the value that the phone that is running SIP will send in the Expires header of the REGISTER message. Valid values include any positive number; however, 3600 (1 hour) specifies the default value. In the 200OK response to REGISTER, Cisco Unified Communications Manager will include an Expires header with the configured value of the SIP Station KeepAlive Interval service parameter. This value in the 200OK determines the time, in seconds, after which the registration expires. The phone will refresh the registration Timer Register Delta seconds before the end of this interval.

Table 101-1 SIP Profile Configuration Settings (continued)

Field	Description
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 will be 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 will be retransmitted. Valid values include any positive number. Default specifies 10.
Start Media Port	This field designates the start real-time protocol (RTP) port for media. Media port ranges from 16384 to 32766. Default specifies 16384.
Stop Media Port	This field designates the stop real-time protocol (RTP) port for media. Media port ranges from 16384 to 32766. Default specifies 32766.
Call Pickup URI	This URI provides a unique address that the phone that is running SIP will send 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 will send 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 will send 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 will send 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

Table 101-1 SIP Profile Configuration Settings (continued)

Field	Description
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.
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)
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.

Table 101-1 SIP Profile Configuration Settings (continued)

Field	Description
Timer Subscribe Delta (seconds)	Use this parameter in conjunction with the Timer Subscribe Expires setting. The phone will resubscribe 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 will allow 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 will send 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 will send to Cisco Unified Communications Manager to invoke the abbreviated dial feature. Speed dials that are not associated with a line key (abbreviated dial indices) will not download to the phone. The phone will use the feature indication mechanism (INVITE with Call-Info header) to indicate when an abbreviated dial number has been entered. The request URI will contain the abbreviated dial digits (for example, 14), and the Call-Info header will indicate the abbreviated dial feature. Cisco Unified Communications Manager will translate 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.

Table 101-1 SIP Profile Configuration Settings (continued)

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.
Call Stats	Check this check box if you want RTP statistics in BYE requests and responses enabled; leave unchecked if you want RTP statistics in BYE requests and responses disabled. If this check box is checked, the phone inserts the headers RTP-RxStat and RTP-TxStat as follows: • RTP-RxStat:Dur=a,Pkt=b,Oct=c,LatePkt=d,LostPkt=e,AvgJit=f • RTP-TxStat: Dur=g,Pkt=h,Oct=i where: • Dur—Total number of seconds since the beginning of reception or transmission. • Pkt—Total number of RTP packets that are received or transmitted. • Oct—Total number of RTP payload octets that are received or transmitted (not including RTP header). • LatePkt—Total number of late RTP packets that are received. • LostPkt—Total number of lost RTP packets that are received (not including the late RTP packets). • AvgJit—Average jitter, which is an estimate of the statistical variance of the RTP packet interarrival time, measured in timestamp unit and calculated according to RFC 1889. • a, b, c, d, e, f, g, h, and i—Integers

Table 101-1 SIP Profile Configuration Settings (continued)

Field	Description
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.

Finding SIP Profiles

This topic describes how to use the Find and List SIP Profile window. The function searches every type of SIP profile against the following categories:

- Profile name
- Description

Procedure

Step 1 Choose **Device** > **Device Settings** > **SIP Profile.**

The Find and List SIP Profiles 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.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 101-13.

Configuring SIP Profiles

Perform the following procedure to add, copy, or update a SIP profile.

Procedure

Step 1 Choose **Device** > **Device Settings** > **SIP Profile**.

The Find and List SIP Profile window displays.

Step 2 Perform one of the followings tasks:

- To copy an existing SIP profile, locate the appropriate SIP profile as described in "Finding SIP Profiles" section on page 101-9, click the **Copy** button next to the SIP profile that you want to copy and continue with Step 3.
- To add a new SIP profile, click the **Add New** button and continue with Step 3.
- To update an existing SIP profile, locate the appropriate SIP profile as described in "Finding SIP Profiles" section on page 101-9 and continue with Step 3.

Step 3 Enter the appropriate settings as described in Table 101-1.

Step 4 Click **Save**.

Additional Information

See the "Related Topics" section on page 101-13.

Deleting SIP Profiles

This section describes how to delete a SIP profile.

Before You Begin

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 "Accessing Dependency Records" section on page A-2.

Procedure

Step 1 Locate the SIP profile that you want to delete. See the "Finding SIP Profiles" section on page 101-9.

Step 2 From the SIP Profile Configuration window, click **Delete**.

A message displays that states that you cannot undo this action.

Step 3 To delete the SIP profile, click **OK** or, to cancel the deletion, click **Cancel**.

Additional Information

See the "Related Topics" section on page 101-13.

Resetting a SIP Profile

Perform the following procedure to reset a SIP profile.

Procedure

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

Step 2 Locate the SIP profile that you want to reset. See the "Finding SIP Profiles" section on page 101-9.

Step 3 Click the SIP profile that you want to reset.

The SIP Profile Configuration window displays.

Step 4 Click **Reset**.

The Device Reset dialog displays.

Step 5 Click one of the following choices:

- **Restart—**Restarts the chosen devices without shutting them down (reregisters the phones and trunks with Cisco Unified Communications Manager).
- **Reset**—Shuts down, then restarts, the device.
- **Close**—Closes the Reset Device dialog without performing any action.

Additional Information

See the "Related Topics" section on page 101-13.

Synchronizing a SIP Profile With Affected SIP Devices

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

Procedure

Step 1 Choose **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**.

Additional Information

See the "Related Topics" section on page 101-13.

Related Topics

- SIP Profile Configuration Settings, page 101-1
- Finding SIP Profiles, page 101-9
- Configuring SIP Profiles, page 101-10
- Deleting SIP Profiles, page 101-11
- Resetting a SIP Profile, page 101-11
- Synchronizing a SIP Profile With Affected SIP Devices, page 101-12
- Configuring Cisco Unified IP Phones, page 91-27
- Configuring a Trunk, page 92-48
- Configuring a Resource Priority Namespace Network Domain, page 21-3
- Configuring a Resource Priority Namespace List, page 22-3
- Understanding Session Initiation Protocol (SIP), *Cisco Unified Communications Manager System Guide*

CHAPTER 102

Common Device Configuration

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.

Use the following topics to configure common device configurations:

- Common Device Configuration Settings, page 102-1
- Finding a Common Device Configuration, page 102-6
- Configuring a Common Device Configuration, page 102-7
- Synchronizing a Common Device Configuration With Affected Devices, page 102-7
- Deleting a Common Device Configuration, page 102-8
- Related Topics, page 102-8

Common Device Configuration Settings

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.

Table 102-1 describes the common device configuration settings. For related procedures, see the "Deleting a Common Device Configuration" section on page 102-8.

Table 102-1 Common Device Configuration 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.

Table 102-1 Common Device Configuration Settings (continued)

Field	Description
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.
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. Phones that run SIP do not support IPv6, so do not choose this option for these phones. If you configure IPv6 Only as the IP Addressing Mode for phones that run SIP, the Cisco TFTP service overrides the IP Addressing Mode configuration and uses IPv4 Only in the configuration file. • 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.

Table 102-1 Common Device Configuration Settings (continued)

Field	Description
IP Addressing Mode Preference for Signaling	For dual-stack phones, which support both IPv4 and IPv6 addresses, choose the version of IP address that the phone prefers to establish a connection to Cisco Unified Communications Manager during a signaling event. For dual-stack SIP trunks, choose the version of IP address that the SIP trunk uses to connect to the peer device for signaling events. From the drop-down list box, choose one of the following options: • IPv4—The dual-stack device prefers to establish a connection via an IPv4 address during a signaling event. • IPv6—The dual-stack device prefers to establish a connection via an IPv6 address during a signaling event. • Use System Default—The configuration for the enterprise parameter, IP Addressing Mode Preference for Signaling, applies.
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.

Table 102-1 Common Device Configuration Settings (continued)

Field	Description
Use Trusted Relay Point	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 "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 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. Refer to the "Trusted Relay Point" section and its subtopics in the Media Resource Management chapter of the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.

Table 102-1 Common Device Configuration Settings (continued)

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*.
MLPP Domain	From the drop-down list box, choose an MLPP domain that is associated with this common device configuration. If you leave the <None> setting, devices inherit MLPP domains from the value set for the MLPP Domain Identifier enterprise parameter.

Finding a Common Device Configuration

Because you may have several common device configurations in your network, Cisco Unified Communications Manager lets you locate specific common device configurations on the basis of specific criteria. Use the following procedure to locate common device configurations.

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

Procedure

Step 1 Choose **Device** > **Device Settings** > **Common Device Configuration.**

The Find and List Common Device Configurations 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.

To filter or search records

- From the drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Deleting a Common Device Configuration" section on page 102-8.

Configuring a Common Device Configuration

To add a common device configuration for a device, use the following procedure.

Procedure

Step 1 Choose **Device** > **Device Settings** > **Common Device Configuration**.

The Find and List Common Device Configurations window displays.

Step 2 Perform one of the followings tasks:

- To add a new common device configuration, click the **Add New** button and continue with Step 3.
- To update an existing common device configuration, locate the appropriate common device configuration as described in "Finding a Common Device Configuration" section on page 102-6 and continue with Step 3.

Step 3 Enter the appropriate settings as described in Table 102-1.

Step 4 Click **Save**.

Additional Information

See the "Deleting a Common Device Configuration" section on page 102-8.

Synchronizing a Common Device Configuration With Affected Devices

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

Procedure

Step 1 Choose **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**.

Additional Information

See the "Related Topics" section on page 102-8.

Deleting a Common Device Configuration

To delete a common device configuration, use the following procedure.

Before You Begin

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. For more information about dependency records, see the "Accessing Dependency Records" section on page A-2. 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.

Procedure

Step 1 To locate the common device configuration that you want to delete, follow the procedure in "Finding a Common Device Configuration" section on page 102-6.

Step 2 Check the check box next to the common device configurations that you want to delete. To select all the common device configurations in the window, check the check box in the matching records title bar.

Step 3 Click **Delete Selected**.

Step 4 To confirm your selection, click **OK**.

Additional Information

See the "Deleting a Common Device Configuration" section on page 102-8.

Related Topics

- Common Device Configuration Settings, page 102-1
- Finding a Common Device Configuration, page 102-6
- Configuring a Common Device Configuration, page 102-7
- Synchronizing a Common Device Configuration With Affected Devices, page 102-7

- Deleting a Common Device Configuration, page 102-8
- Trusted Relay Point, *Cisco Unified Communications Manager System Guide*

CHAPTER 103

Common Phone Profile Configuration

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.

Use the following topics to configure and locate common phone profiles:

Common Phone Profile Configuration Settings

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.

Table 103-1 describes the available settings in the Common Phone Profile Configuration window. For more information about related procedures, see the "Related Topics" section on page 103-7.

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 103-1 Common Phone Profile Configuration 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.
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.
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.
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.

Table 103-1 Common Phone Profile Configuration Settings (continued)

Field	Description
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. Refer to 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 User	Enter the password for a secure shell user. Contact TAC for further assistance. Refer to 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	
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, refer to the Phone Designer documentation.

Table 103-1 Common Phone Profile Configuration Settings (continued)

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 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.
Services Provisioning	From the drop-down list box, choose whether the phone will use the services provisioned in the phone configuration file (Internal), services received from an external URL (External URL), or both. The default specifies Internal. Select **External URL** if you are using an external provisioning server or **Both** if are using an external server but also want to allow users to subscribe to services in Cisco Unified Communications Manager.

Finding Common Phone Profiles

This topic describes how to use the Find and List Common Phone Profile window.

Procedure

Step 1 Choose **Device > Device Settings > Common Phone Profile.**

The Find and List Common Phone Profiles 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.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 103-7.

Configuring Common Phone Profiles

Perform the following procedure to add, copy, or update a common phone profile.

Procedure

Step 1 Choose **Device > Device Settings > Common Phone Profile**.

The Find and List Common Phone Profiles window displays.

Step 2 Perform one of the followings tasks:

- To copy an existing common phone profile, locate the appropriate common phone profile as described in "Finding Common Phone Profiles" section on page 103-4, click the **Copy** button next to the common phone profile that you want to copy, and continue with Step 3.
- To add a new common phone profile, click the **Add New** button and continue with Step 3.

- To update an existing common phone profile, locate the appropriate common phone profile as described in "Finding Common Phone Profiles" section on page 103-4 and continue with Step 3.

Step 3 Enter the appropriate settings as described in Table 103-1.

Step 4 Click **Save**.

Additional Information

See the "Related Topics" section on page 103-7.

Synchronizing Common Phone Profiles With Affected Devices

To synchronize devices with a common phone profile that has undergone configuration changes, perform the following procedure, which will apply any outstanding configuration settings in the least-intrusive manner possible. (For example, a reset/restart may not be required on some affected devices.)

Procedure

Step 1 Choose **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**.

Additional Information

See the "Related Topics" section on page 103-7.

Deleting Common Phone Profiles

This section describes how to delete a common phone profile.

Before You Begin

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. For more information about dependency records, see the "Accessing Dependency Records" section on page A-2.

Procedure

Step 1 Locate the common phone profile that you want to delete. See the "Finding Common Phone Profiles" section on page 103-4.

Note You cannot delete the Standard Common Phone Profile.

Step 2 From the Common Phone Profile Configuration window, click **Delete**.

A message displays that states that you cannot undo this action.

Step 3 To delete the common phone profile, click **OK** or, to cancel the deletion, click **Cancel**.

Additional Information

See the "Related Topics" section on page 103-7.

Related Topics

- Common Phone Profile Configuration Settings, page 103-1
- Finding Common Phone Profiles, page 103-4
- Configuring Common Phone Profiles, page 103-5
- Synchronizing Common Phone Profiles With Affected Devices, page 103-6
- Deleting Common Phone Profiles, page 103-7
- Cisco Unified IP Phone Configuration, page 91-1
- Cisco TFTP, *Cisco Unified Communications Manager System Guide*
- Understanding Session Initiation Protocol (SIP), *Cisco Unified Communications Manager System Guide*
- Cisco Unified IP Phones, *Cisco Unified Communications Manager System Guide*

CHAPTER 104

Remote Destination Profile Configuration

Mobile Connect 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 Mobile Connect 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 Mobile Connect and Mobile Voice Access and how to configure remote destination profiles, refer to the Cisco Unified Mobility chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

CHAPTER 105

Recording Profile Configuration

To provision line appearances of agents for call recording, administrators create one or more call recording profiles. The administrator then selects a recording profile for a line appearance.

To create a recording profile, a Cisco Unified Communications Manager administrator chooses **Device** > **Device Settings** > **Recording Profile** in Cisco Unified Communications Manager Administration.

Use the following topics to configure recording profiles:

Recording Profile Configuration Settings

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.

To create a recording profile, a Cisco Unified Communications Manager administrator chooses **Device** > **Device Settings** > **Recording Profile** in Cisco Unified Communications Manager Administration.

Table 105-1 describes the recording profile configuration settings. For related procedures, see the "Related Topics" section on page 105-4.

Table 105-1 Recording Profile Configuration 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.

Finding a Recording Profile

Because you may have several recording profiles in your Cisco Unified Communications Manager cluster, Cisco Unified Communications Manager lets you locate specific recording profiles on the basis of specific criteria. Use the following procedure to locate recording profiles.

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

Procedure

Step 1 Choose **Device** > **Device Settings** > **Recording Profile.**

The Find and List Recording Profiles 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.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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.

Additional Information

See the "Related Topics" section on page 105-4.

Configuring a Recording Profile

To configure a recording profile, use the following procedure.

Procedure

Step 1 Choose **Device** > **Device Settings** > **Recording Profile**.

The Find and List Recording Profiles window displays.

Step 2 Perform one of the followings tasks:

- To add a new recording profile, click the **Add New** button and continue with Step 3.
- To update an existing recording profile, locate the appropriate recording profile as described in "Finding a Recording Profile" section on page 105-2 and continue with Step 3.

Step 3 Enter the appropriate settings as described in Table 105-1.

Step 4 Click **Save**.

Additional Information

See the "Related Topics" section on page 105-4.

Deleting a Recording Profile

To delete a recording profile, use the following procedure.

Before You Begin

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. For more information about dependency records, see the "Accessing Dependency Records" section on page A-2. 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.

Procedure

Step 1 To locate the recording profile that you want to delete, follow the procedure in "Finding a Recording Profile" section on page 105-2.

Step 2 Check the check box next to the recording profiles that you want to delete. To select all the recording profiles in the window, check the check box in the matching records title bar.

Step 3 Click **Delete Selected**.

Step 4 To confirm your selection, click **OK**.

Additional Information

See the "Related Topics" section on page 105-4.

Related Topics

- Recording Profile Configuration Settings, page 105-1
- Finding a Recording Profile, page 105-2
- Configuring a Recording Profile, page 105-3
- Deleting a Recording Profile, page 105-3

PART 7

Application Configuration

CHAPTER 106

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. Refer to 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, refer to the Cisco Unified Communications Manager Assistant Configuration Wizard in the *Cisco Unified Communications Manager Features and Services Guide*.

CHAPTER 107

Cisco Unified Communications Manager Attendant Console Pilot Point Configuration

Cisco Unified Communications Manager Attendant Console, a client-server application, allows you to use a graphical user interface that contains speed-dial buttons and quick directory access to look up phone numbers, to monitor line status, and to direct calls. A receptionist or administrative assistant can use the attendant console to handle calls for a department or company, or another employee can use it to manage his own telephone calls.

For information and pilot point configuration procedures for Cisco Unified Communications Manager Attendant Console, refer to the "Cisco Unified Communications Manager Attendant Console" section in the *Cisco Unified Communications Manager Features and Services Guide*.

CHAPTER 108

Cisco Unified Communications Manager Attendant Console User Configuration

Cisco Unified Communications Manager Attendant Console, a client-server application, allows you to use a graphical user interface that contains speed-dial buttons and quick directory access to look up phone numbers, to monitor line status, and to direct calls. A receptionist or administrative assistant can use the attendant console to handle calls for a department or company, or another employee can use it to manage his own telephone calls.

For information and configuration procedures for Cisco Unified Communications Manager Attendant Console, refer to the "Cisco Unified Communications Manager Attendant Console" section in the *Cisco Unified Communications Manager Features and Services Guide*.

CHAPTER 109

Cisco Unified Communications Manager Attendant Console User File Upload

Cisco Unified Communications Manager Attendant Console, a client-server application, allows you to use a graphical user interface that contains speed-dial buttons and quick directory access to look up phone numbers, to monitor line status, and to direct calls. A receptionist or administrative assistant can use the attendant console to handle calls for a department or company, or another employee can use it to manage his own telephone calls.

For information on how to upload the user file and configuration procedures for Cisco Unified Communications Manager Attendant Console, refer to the "Cisco Unified Communications Manager Attendant Console" section in the *Cisco Unified Communications Manager Features and Services Guide*.

CHAPTER 110

Plug-in Configuration

This section contains the following topics:

- Update Plugin URL Configuration Settings, page 110-1
- Installing Plug-ins, page 110-2
- Updating the Plugin URL, page 110-3
- Related Topics, page 110-3

Update Plugin URL Configuration Settings

Application plug-ins extend the functionality of Cisco Unified Communications Manager. For example, the Cisco Unified Communications Manager Attendant Console plug-in allows a receptionist to rapidly answer and transfer calls within an organization, and 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).

Table 110-1 describes the Update Plugin URL configuration settings. For additional information, see the "Related Topics" section on page 110-3.

Table 110-1 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.

Installing Plug-ins

Tip After Cisco Unified Communications Manager upgrades, you must reinstall all plug-ins except the Cisco CDR Analysis and Reporting plug-in.

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.

Perform the following procedure to install any 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; go to Step 3.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- From the third drop-down list box, select Application Menu, Installation, User Menu, or Telecaster Menu.
- 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.

Additional Information

See the "Related Topics" section on page 110-3.

Updating the 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 according to the instructions in Installing Plug-ins.

Step 2 Click the Plugin name that you want to update.

The Update Plugin URL window displays.

Step 3 Enter the information described in Table 110-1.

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.

Additional Information

See the "Related Topics" section on page 110-3.

Related Topics

- Update Plugin URL Configuration Settings, page 110-1
- Installing Plug-ins, page 110-2
- Updating the Plugin URL, page 110-3

PART 8

User Management Configuration

CHAPTER 111

Credential Policy Default Configuration

This chapter describes how to assign default credential policies to a credential group. See the "Related Topics" section on page 111-4 for more information about changing credential information for individual users. The following topics contain information on configuring credential policies:

Credential Policy Default Configuration Settings

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.

The system provides the default credential policy to facilitate installs and upgrades. The default credential policy settings in Table 111-1 differ from the credential policy defaults settings that are described in the "Credential Policy Configuration Settings", which you use for adding a new credential policy.

- Upgrades from 5.x releases automatically migrate end user passwords and PINs.
- Upgrades from 4.x releases assign a default password and PIN to end users during installation.

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. For more information, see "Managing Application User Credential Information" section on page 113-9 for application users and "Managing End User Credential Information" section on page 114-12 for end users.

Table 111-1 describes the credential policy default configuration settings. See the "Related Topics" section on page 111-4 for related information and procedures.

Table 111-1 Credential Policy Default Configuration 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, as described in the "Credential Policy Configuration" section on page 112-1.
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 unchecked.
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.

Finding Credential Policy Defaults

This section describes how to find or review existing credential policy default information.

Step 1 Choose **User Management** > **Credential Policy Default**.

The Find and List Credential Policy Defaults window displays the assigned policies.

Step 2 Click the list item to display.

The window displays the credential policy default information for the policy that you choose.

Additional Information

See the "Related Topics" section on page 111-4.

Assigning and Configuring 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. Go to the "Configuring a Credential Policy" section on page 112-4 if you have not yet created the policy you want to use.

Procedure

Step 1 Choose **User Management** > **Credential Policy Default**.

The Find and List 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 111-1, using these guidelines:

- To change the applied credential policy, select the policy from the drop-down list box.
- To change the default credential, enter and confirm the new credential in the appropriate fields.
- To change credential requirements, check or uncheck the appropriate check boxes.

Step 4 Click the **Save** button or the **Save** icon.

Next Steps

To assign a new user credential policy, manage user authentication events, or view credential information for a user, use these procedures:

- Managing Application User Credential Information, page 113-9
- Managing End User Credential Information, page 114-12

To configure a unique password for a user, use these procedures:

- Changing an Application User Password, page 113-9
- Changing an End User Password, page 114-11
- Changing an End User PIN, page 114-11

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. Refer to 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. Refer to the documentation for your Cisco Unified IP Phone for more information.

Additional Information

See the "Related Topics" section on page 111-4.

Related Topics

- Credential Policy Configuration Settings, page 112-1
- Finding Credential Policy Defaults, page 111-2
- Assigning and Configuring Credential Policy Defaults, page 111-3
- Credential Policy Default Configuration Settings, page 111-1
- Finding a Credential Policy, page 112-3
- Configuring a Credential Policy, page 112-4
- Deleting a Credential Policy, page 112-4
- Changing an Application User Password, page 113-9
- Changing an End User Password, page 114-11
- Changing an End User PIN, page 114-11
- Managing End User Credential Information, page 114-12
- Managing Application User Credential Information, page 113-9
- Credential Policy, *Cisco Unified Communications Manager System Guide*
- Understanding the Directory, *Cisco Unified Communications Manager System Guide*
- Application Users and End Users, *Cisco Unified Communications Manager System Guide*
- Cisco Extension Mobility, *Cisco Unified Communications Manager Features and Services Guide*

CHAPTER 112

Credential Policy Configuration

This chapter describes how to configure credential policies. See the "Related Topics" section on page 112-5 for more information about assigning credential policies. The following topics contain information about configuring credential policies:

Credential Policy Configuration Settings

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 logon 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.

Table 112-1 describes the credential policy configuration settings. See the "Related Topics" section on page 112-5 for related information and procedures.

Before You Begin

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.

Table 112-1 Credential Policy Configuration 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 logon attempts. When this threshold is reached, the system locks the account. Enter a number in the range 1-100. To allow unlimited failed logons, 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 logon 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 logon 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.

Table 112-1 Credential Policy Configuration Settings (continued)

Field	Description
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.
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.

Finding a Credential Policy

This section describes how to find or review existing credential policies.

Step 1 Choose **User Management** > **Credential Policy**.

The Find and List Credential Policies window displays.

Step 2 Click the list item to display.

The window displays the credential policy that you choose.

Additional Information

See the "Related Topics" section on page 112-5.

Configuring a Credential Policy

This section describes how to create a new credential policy or modify an existing credential policy. You cannot modify the system Default Credential Policy.

Procedure

Step 1 Choose **User Management > Credential Policy**.

The Find and List window displays.

Step 2 Perform one of the following tasks:

- To add a new policy, click the **Add New** button or **Add New** icon in the Find window OR display a credential policy from the list and click the **Copy** or **Add New** button or icon**.** When you click **Add New**, the Credential Policy Configuration window displays with the default settings for each field. When you click **Copy**, the Credential Policy Configuration window displays with the settings from the displayed policy. Continue with Step 3.
- To update an existing entry, click the policy to change. The Credential Policy Configuration window displays with the current settings. Continue with Step 3.

Step 3 Enter the appropriate settings as described in Table 112-1.

Step 4 Click the **Save** button or the **Save** icon.

Next Steps

To assign the new credential policy as a default policy for a credential type, follow the procedure described in "Assigning and Configuring Credential Policy Defaults" section on page 111-3.

To assign the new credential policy to individual users, follow the procedures described in "Managing Application User Credential Information" section on page 113-9 and "Managing End User Credential Information" section on page 114-12.

Additional Information

See the "Related Topics" section on page 112-5.

Deleting a Credential Policy

This section describes how to delete a security policy from the Cisco Unified Communications Manager database.

Before You Begin

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. For more information about dependency records, see the "Accessing Dependency Records" section on page A-2.

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, as described in Configuring a Credential Policy, page 112-4.

Procedure

Step 1 Find the credential policy to delete by using the procedure in the "Finding a Credential Policy" section on page 112-3. From the list of records, click the policy that you want to delete.

Note You can delete entries from the Find and List window by checking the check boxes next to the appropriate entries and clicking the **Delete Selected** button or the **Delete Selected** icon. You can delete all entries in the list by clicking the **Select All** button or the **Select All** icon and clicking the **Delete Selected** button or the **Delete Selected** icon.

Step 2 Click the **Delete** icon or the **Delete** button in the Credential Policy Configuration window to delete the policy.

Step 3 When asked to confirm the delete operation, click **OK** to delete the policy.

Additional Information

See the "Related Topics" section on page 112-5.

Related Topics

- Credential Policy Configuration Settings, page 112-1
- Finding a Credential Policy, page 112-3
- Finding a Credential Policy, page 112-3
- Configuring a Credential Policy, page 112-4
- Deleting a Credential Policy, page 112-4
- Finding Credential Policy Defaults, page 111-2
- Assigning and Configuring Credential Policy Defaults, page 111-3
- Credential Policy Default Configuration Settings, page 111-1
- Changing an Application User Password, page 113-9
- Changing an End User Password, page 114-11
- Changing an End User PIN, page 114-11
- Managing End User Credential Information, page 114-12
- Managing Application User Credential Information, page 113-9

- Application Users and End Users, *Cisco Unified Communications Manager System Guide*
- Where to Find More Information, *Cisco Unified Communications Manager System Guide*
- Cisco Unity Messaging Integration, *Cisco Unified Communications Manager System Guide*
- LDAP System Configuration, page 14-1
- Directory Number Configuration, page 64-1
- CTI Route Point Configuration, page 88-1
- Cisco Extension Mobility, *Cisco Unified Communications Manager Features and Services Guide*

CHAPTER 113

Application User Configuration

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.

The following topics contain information on managing application user information:

Application User Configuration Settings

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.

Table 113-1 describes the application user configuration settings. For related procedures, see the "Related Topics" section on page 113-13.

Table 113-1 Application User Configuration 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). You can enter the following characters: alphanumeric (a-zA-Z0-9), dash(-), underscore(_), or space( ).

Table 113-1 Application User Configuration Settings (continued)

Field	Description
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.
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, refer to the *Cisco Unified Communications Manager Security Guide*.
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. See "Managing Application User Credential Information" section on page 113-9.
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. Refer to the "Presence" chapter in the *Cisco Unified Communications Manager Features and Services Guide* for information about configuring permissions between groups.

Table 113-1 Application User Configuration Settings (continued)

Field	Description
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, refer to the *Cisco Unified Communications Manager Security Guide*.
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, refer to 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, refer to the *Cisco Unified Communications Manager Security Guide*.

Table 113-1 Application User Configuration Settings (continued)

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 Communications Manager 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 Communications Manager 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 Communications Manager sends a 403 error message to the SIP user agent that is connected to the trunk. For more information on authorization, refer to 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	
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, refer to the *Cisco Unified Communications Manager Security Guide*.

Table 113-1 Application User Configuration Settings (continued)

Field	Description
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 User Group** button. The Find and List User 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 User 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 User 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 User Group Configuration window displays with the current settings. For more information on finding and configuring user groups, see the "User Group Configuration" section on page 116-1.
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. For more information on configuring roles, see the "Role Configuration" section on page 115-1.

Finding an Application User

Cisco Unified Communications Manager lets you find application user information on the basis of specific criteria. Use the following procedure to find application user information.

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

Procedure

Step 1 Choose **User Management** > **Application User**.

The Find and List Application Users 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.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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 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.

Additional Information

See the "Related Topics" section on page 113-13.

Configuring an Application User

Use the following procedure to configure a new application user. 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.Refer to 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.

Procedure

Step 1 Choose **User Management > Application User**.

The Find and List Application Users window displays. Use the two drop-down list boxes to search for an application user.

Step 2 Click **Add New**.

The Application User Configuration window displays.

Step 3 Enter the appropriate settings as described in Table 113-1.

Step 4 When you have completed the user information, save your changes and add the user by clicking **Save**.

Step 5 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. Refer to the "Viewing User Roles, User Groups, and Permissions" section on page 116-7 for details of the user privilege report.

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

If you want to associate devices with this application user, continue with the "Associating Devices to an Application User" procedure.

To manage credentials for this application user, continue with the "Managing Application User Credential Information" procedure.

To add an administrator user to Cisco Unity or Cisco Unity Connection, continue with the procedure in "Adding an Administrator User to Cisco Unity or Cisco Unity Connection" section on page 113-7.

Additional Information

See the "Related Topics" section on page 113-13.

Adding an 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 "Adding an Administrator User to Cisco Unity or Cisco Unity Connection" section on page 113-7. For information on how to use the import feature, refer to 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. Refer to 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, refer to the applicable *User Moves, Adds, and Changes Guide for Cisco Unity Connection.* For Cisco Unity users, refer to the S*ystem Administration Guide for Cisco Unity*.

Procedure

Step 1 Find the application user, as described in the "Finding an Application User" section on page 113-5.

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 Communications Manager 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, refer to the *User Moves, Adds, and Changes Guide for Cisco Unity Connection* for more information. For Cisco Unity, refer to the S*ystem Administration Guide for Cisco Unity*.

Additional Information

See the "Related Topics" section on page 113-13.

Changing an Application User Password

Use the following procedure to change an application user password.

Procedure

Step 1 Use the procedure in the "Finding an Application User" section on page 113-5 to find the application user whose password you want to change.

The Application User Configuration window displays with information about the chosen application user.

Step 2 In the Password field, double-click the existing password, which is encrypted, 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**.

Additional Information

See the "Related Topics" section on page 113-13.

Managing 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. See "Configuring an Application User" section on page 113-6.

Procedure

Step 1 Use the procedure in the "Finding an Application User" section on page 113-5 to find the application user configuration.

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 113-2.

Step 4 If you have changed any settings, click **Save**.

Additional Information

See the "Related Topics" section on page 113-13.

Credential Settings and Fields

Table 113-2 describes credential settings for application users and end users. These settings do not apply to application user or end user digest credentials. For related procedures, see the "Related Topics" section on page 113-13.

Table 113-2 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.

Table 113-2 Application User and End User Credential Settings and Fields (continued)

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 logon attempts since the last successful logon, 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 logon 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 logon attempts. Time of hack lockout gets set whenever failed logon attempts exceed the configured threshold in the applied credential policy.

Associating Devices to an Application User

You can associate devices over which application users will have control. Application users can control some devices, such as phones. Applications that are identified as users can control other devices, such as CTI ports. When application users have control of a phone, they can control certain settings for that phone, such as speed dial and call forwarding.

Before You Begin

To assign devices to an application user, you must access the Application User Configuration window for that user. See the "Finding an Application User" section on page 113-5 for information on finding existing application users. 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:

- 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.
- 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.
- 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.

Additional Information

See the "Related Topics" section on page 113-13.

Deleting an Application User

To delete an application user by using Cisco Unified Communications Manager Administration, perform the following procedure.

Before You Begin

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. For more information about dependency records, see the "Accessing Dependency Records" section on page A-2.

Procedure

Step 1 Choose **User Management** > **Application User**.

The Find and List Users window displays.

Step 2 To locate a specific end user, enter search criteria and click **Find**.

A list of application users that match the search criteria displays.

Step 3 Perform one of the following actions:

- Check the check boxes next to the users that you want to delete and click **Delete Selected**.
- Delete all the users in the window by clicking **Select All** and clicking **Delete Selected**.
- Choose the user ID of the user that you want to delete from the list to display its current settings and click **Delete**.

A confirmation dialog displays.

Step 4 Click **OK**.

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. Refer to the applicable S*ystem Administration Guide for Cisco Unity* for more Cisco Unity information.

Additional Information

See the "Related Topics" section on page 113-13.

Related Topics

- Application User Configuration Settings, page 113-1
- Finding an Application User, page 113-5
- Configuring an Application User, page 113-6
- Adding an Administrator User to Cisco Unity or Cisco Unity Connection, page 113-7
- Changing an Application User Password, page 113-9
- Managing Application User Credential Information, page 113-9
- Credential Settings and Fields, page 113-10
- Associating Devices to an Application User, page 113-11
- Deleting an Application User, page 113-12
- Finding an End User, page 114-8
- Configuring an End User, page 114-9
- Creating a Cisco Unity Connection Voice Mailbox, page 114-10
- Changing an End User Password, page 114-11
- Changing an End User Password, page 114-11
- Changing an End User PIN, page 114-11
- Managing End User Credential Information, page 114-12
- Credential Settings and Fields, page 114-13
- Configuring User-Related Information for End Users, page 114-14
- Associating Devices to an End User, page 114-15
- Associating Cisco Extension Mobility Profiles, page 114-17
- Deleting an End User, page 114-17
- LDAP System Configuration, page 14-1
- Role Configuration, page 115-1
- User Group Configuration, page 116-1

- Viewing User Roles, User Groups, and Permissions, page 116-7
- Directory Number Configuration, page 64-1
- CTI Route Point Configuration, page 88-1
- Cisco Unified IP Phone Configuration, page 91-1
- Credential Policy Configuration, page 112-1
- Credential Policy Default Configuration, page 111-1
- Credential Policy, *Cisco Unified Communications Manager System Guide*
- Where to Find More Information, *Cisco Unified Communications Manager System Guide*
- Application Users and End Users, *Cisco Unified Communications Manager System Guide*
- Cisco Extension Mobility, *Cisco Unified Communications Manager Features and Services Guide*
- Device Association, *Cisco Unified Communications Manager System Guide*
- Associating a User Device Profile to a User, *Cisco Unified Communications Manager Features and Services Guide*
- Cisco Unified Communications Manager Assistant With Proxy Line Support, *Cisco Unified Communications Manager Features and Services Guide*
- Cisco Unified Communications Manager Assistant With Shared Line Support, *Cisco Unified Communications Manager Features and Services Guide*
- Cisco Unity Messaging Integration, *Cisco Unified Communications Manager System Guide*
- Presence, *Cisco Unified Communications Manager Features and Services Guide*

Related Documentation

- *Cisco Unified Communications Manager Security Guide*
- *User Moves, Adds, and Changes Guide for Cisco Unity Connection*
- *System Administration Guide for Cisco Unity*

CHAPTER 114

End User Configuration

The End User Configuration window in Cisco Unified Communications Manager Administration allows the administrator to add, search, display, and maintain information about Cisco Unified Communications Manager end users.

- If you configure your system to use the LDAP corporate directory as the end user directory for Cisco Unified Communications Manager, you cannot add or delete users in Cisco Unified Communications Manager Administration.You add and remove end users in the corporate LDAP directory.
- If you configure your system to authenticate users against the LDAP directory, you cannot configure or change end user passwords in Cisco Unified Communications Manager Administration. You configure and change end user passwords in the corporate LDAP directory.

The following topics contain information on managing end user directory information:

End User Configuration Settings

The End User Configuration window in Cisco Unified Communications Manager Administration allows the administrator to add, search, display, and maintain information about Cisco Unified Communications Manager end users. End users can control phones after you associate a phone in the End User Configuration window.

Table 114-1 describes the end user configuration settings. For related procedures, see the "Related Topics" section on page 114-18.

Before You Begin

- If you enable LDAP synchronization in Cisco Unified Communications Manager Administration, you cannot add an end user, delete an end user, or change some existing user information, including user IDs, in the End User Configuration windows. Instead, you must add, update some user information, and delete end users in the corporate LDAP directory. To verify that the Enable Synchronizing from LDAP Server check box is not checked, choose **System > LDAP > LDAP System**.
- If you configure your system to authenticate users against the LDAP directory, you cannot configure or change end user passwords in Cisco Unified Communications Manager Administration. You configure and change end user passwords in the corporate LDAP directory.
- 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 Cisco Unified Communications Manager Administration end user as a Cisco Unity Connection user by using the Create a Cisco Unity User option in the End User Configuration window, as described in the "Creating a Cisco Unity Connection Voice Mailbox" section on page 114-10.

Table 114-1 End User Configuration Settings

Field	Description
User Information	
LDAP Sync Status	This field displays the LDAP synchronization status, which you set with the **System** > **LDAP** > **LDAP System** menu option.
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 User ID only if synchronization with an LDAP server is not enabled. If synchronization is enabled, you can view the user ID, but you cannot modify it. If synchronization is disabled, Cisco Unified Communications Manager permits you to modify the user ID after it is created.
Password / Edit Credential	This field does not display 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. See the "Managing End User Credential Information" section on page 114-12.
Confirm Password	This field does not display if LDAP Authentication is enabled. Enter the end user password again.

Table 114-1 End User Configuration Settings (continued)

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 displays after you add this user to the database. Click the **Edit Credential** button to manage credential information for this user. See the "Managing End User Credential Information" section on page 114-12.
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.
Telephone Number	Enter the end user telephone 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. The manager user ID that you enter must already exist in the directory as an end user.
Department	Enter the end user department information (for example, the department number or name).
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. Cisco Unified Communications Manager uses this locale for extension mobility and the Cisco Unified CM User Options. For Cisco Extension Mobility log on, the locale that is specified here takes precedence over the device and device profile settings. For Cisco Extension Mobility log off, Cisco 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 and Cisco Unified Communications Manager Attendant Console users.
Digest Credentials	Enter a string of alphanumeric characters. Cisco 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 on digest authentication, refer to 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.

Table 114-1 *End User Configuration Settings (continued)*

Field	Description
Device Associations	
Controlled Devices	After the device is associated, this field displays the description information (for example, the MAC address) that the end user controls. This field displays after you create a user in the database. To associate a device with this end user, click the **Device Association** button. See the "Associating Devices to an End User" section on page 114-15 for a detailed procedure.
Extension Mobility	
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 displays 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 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.
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 destinations that the end user can monitor. 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. Refer to the "Presence" chapter in the *Cisco Unified Communications Manager Features and Services Guide* for information about configuring permissions between groups and how presence works with extension mobility.

Table 114-1 End User Configuration Settings (continued)

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 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 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. For information on how to configure a calling search space, see the "Calling Search Space Configuration" section on page 53-1
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.
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 displays only if the IPCC Express Installed enterprise parameter is set to *True*.

Table 114-1 End User Configuration Settings (continued)

Field	Description
Mobility Information	
Enable Mobility	Check this check box to activate Mobile Connect, 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, which triggers licensing to consume device license units for Mobile Connect, works in conjunction with the Primary User Device drop-down list box. If you check the Enable Mobility check box and fail to choose an adjunct device from the Primary User Device drop-down list box, four device license units (DLUs) get consumed, as indicated in the Mobility Enabled End Users row in the License Unit Calculation window. If you enable Cisco Unified Mobility and later choose an adjunct device from the Primary User Device drop-down list box, the system credits you with two DLUs, as indicated in the Mobility Enabled End Users row in the License Unit Calculation window.
Primary User Device	The Primary User Device drop-down list box, which works in conjunction with the Enable Mobility check box, controls the number of device license units that are consumed for adjunct devices for Mobile Connect. After you check the Enable Mobility check box, choose an adjunct device that you want to assign to the user specifically for Cisco Unified Mobility. For example, choose a device, such as a desktop phone, that the user uses in addition to the cell phone for Cisco Unified Mobility. Before you choose an adjunct device, consider the following information: • Only devices that consume two or more device license units (DLUs) display in the drop-down list box. • For Cisco Unified Mobility, you cannot assign the same device to multiple users, so only the devices that you can assign display in the drop-down list box. • If you check the Enable Mobility check box and choose a device from the drop-down list box, two DLUs get consumed, as indicated in the Mobility Enabled End Users (Adjunct) row in the Licensing Unit Calculation window. • If you delete the device from Cisco Unified Communications Manager Administration or remove the assignment after you enable Mobile Connect, two DLUs get consumed after you delete the device or remove the assignment, as indicated in the Mobility Enabled End Users row in the License Unit Calculation window.
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 Mobile Connect calls and activate or deactivate Mobile Connect capabilities.

Table 114-1 End User Configuration Settings (continued)

Field	Description
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 have been 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.
CAPF Information	
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 End User CAPF Profile Configuration window displays with the current settings. For information on how to configure the End User CAPF Profile, refer to the *Cisco Unified Communications Manager Security Guide*.
Permissions Information	
Groups	This list box displays after an end user record has been saved. The list box displays the groups to which the end user belongs. To add the user to one or more user groups, click the **Add to User Group** button. The Find and List User Groups window opens as a separate window. Locate the groups to which you want to add the user, check the check boxes beside those groups, and click **Add Selected** at the bottom of the window. The Find and List User Groups window closes, and the End User Configuration window displays and now shows 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 User 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 User Group Configuration window displays with the current settings. For more information on finding and configuring user groups, see the "User Group Configuration" section on page 116-1.
Roles	This list box displays after an end user has been added, the Groups list box has been populated, and the user record has been saved. The list box displays the roles that are assigned to the end 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. For more information on configuring roles, see the "Role Configuration" section on page 115-1.

Finding an End User

Cisco Unified Communications Manager lets you find end user information on the basis of specific criteria. Use the following procedure to find end user information.

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

Procedure

Step 1 Choose **User Management > End User**.

The Find and List Users 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.

To filter or search records

- From the first drop-down list box, choose a search parameter.
- From the second drop-down list box, choose a search pattern.
- 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 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.

Additional Information

See the "Related Topics" section on page 114-18.

Configuring an End User

The following procedure provides instructions on adding and configuring an end user.

Note You can add end users through Cisco Unified Communications Manager Administration only when synchronization with an LDAP server is not enabled. When synchronization is disabled, you can add new users to the Cisco Unified Communications Manager database, and you can change the settings for existing users, including the user ID. Use the **System** > **LDAP** > **LDAP System** menu option to verify that LDAP synchronization is not enabled. In the LDAP System window that displays, ensure that the Enable Synchronizing from LDAP Server check box is not checked.

If you enable LDAP synchronization, you cannot add an end user, delete an end user, or change some existing user information, including user IDs, in the End User Configuration windows.

You can configure a Cisco Unified Communications Manager Administration end user as a Cisco Unity Connection user by using the Create a Cisco Unity User option in the End User Configuration window, as described in the "Creating a Cisco Unity Connection Voice Mailbox" section on page 114-10. You can then configure any additional settings in Cisco Unity Connection Administration.

Procedure

Step 1 Choose **User Management** > **End User**.

The Find and List End Users window displays. Use the two drop-down list boxes to search for an end user.

Step 2 Click **Add New**.

The End User Configuration window displays.

Step 3 Enter the appropriate settings as described in Table 114-1.

Step 4 When you have completed the end user information, save your changes and add the end user by clicking **Save**.

Next Steps

If you want to associate devices to this end user, continue with the "Associating Devices to an End User" procedure.

To manage credentials for this end user, continue with the "Managing End User Credential Information" procedure.

To create a Cisco Unity Connection Voice Mailbox for this user in Cisco Unified Communications Manager Administration, continue with the procedure in "Creating a Cisco Unity Connection Voice Mailbox" section on page 114-10.

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 Cisco Unified Communications Manager and Cisco Unity Connection must be complete. For more information, refer to 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*.

Additional Information

See the "Related Topics" section on page 114-18.

Creating a 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 Administration.

Before You Begin

- You must configure Cisco Unified Communications Manager for voice messaging.
- You must configure the Cisco Unity Connection server to use the integrated mailbox feature. Refer to the *"Creating Multiple User Accounts from Cisco Unified Communications Manager 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 have defined an appropriate template and class of service (COS) for any voice-messaging users that you plan to add in Cisco Unified Communications Manager Administration. For Cisco Unity Connection users, refer to 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 displays in the Related Links menu.
- If you want to do so, you can use the import feature that is available in Cisco Unity Connection instead of performing the procedure that is described in the "Creating a Cisco Unity Connection Voice Mailbox" section on page 114-10. For information on how to use the import feature, refer to the *"Creating Multiple User Accounts from Cisco Unified Communications Manager 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 Find the end user, as described in "Finding an End User" section on page 114-8.

Step 2 Verify that a primary extension number is associated with this user.

Note You must ensure that you have defined a primary extension; otherwise, the "Create Cisco Unity User" link will not display in the Related Links drop-down list box.

Step 3 From the Related Links drop-down list box, in the upper, right corner of the window, choose the "Create Cisco Unity User" 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 user 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 mailbox gets 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 When the Cisco Unity Connection user is integrated with the Cisco Unified Communications Manager end 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 Connection Administration. You can only update these fields in Cisco Unified Communications Manager Administration.

Additional Information

See the “Related Topics” section on page 114-18.

Changing an 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 procedure in the “Finding an End User” section on page 114-8 to find the end user configuration.

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**.

Additional Information

See the “Related Topics” section on page 114-18.

Changing an End User PIN

Use the following procedure to change the personal identification number (PIN) for an end user.

Procedure

Step 1 Use the procedure in the "Finding an End User" section on page 114-8 to find the end user configuration.

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**.

Additional Information

See the "Related Topics" section on page 114-18.

Managing 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. 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.

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. See "Configuring an End User" section on page 114-9.

Procedure

Step 1 To find the end user configuration, use the procedure in the "Finding an End User" section on page 114-8.

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 114-2.

Step 4 If you have changed any settings, click **Save**.

Additional Information

See the "Related Topics" section on page 114-18.

Credential Settings and Fields

Table 114-2 describes the credential settings for end users and application users. These settings do not apply to application user or end user digest credentials. For related procedures, see the "Related Topics" section on page 114-18.

Table 114-2 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. You cannot uncheck this check box if the policy setting specifies Never Expires.
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.

Table 114-2 Application User and End User Credential Settings and Fields (continued)

Field	Description
Failed Logon Attempts	This field displays the number of failed logon attempts since the last successful logon, since the administrator reset the hack count for this user credential, or since the reset failed login attempts time has expired.
Time of Last Field Logon Attempt	This field displays the date and time for the most recent failed logon 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 logon attempts. The associated credential policy defines lockouts due to failed logon attempts.

Configuring User-Related Information for End Users

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. See the "Finding an End User" section on page 114-8 for more information.

Procedure

Step 1 Use the procedure in the "Finding an End User" section on page 114-8 to find the end user whose application profile(s) you want to configure. Click the userid.

The End User Configuration window displays with information about the chosen end user.

Step 2 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 click **Go**.

The Manager Configuration window displays for this end user. Refer to the "Cisco Unified Communications Manager Assistant With Proxy Line Support" and "Cisco Unified Communications Manager Assistant With Shared Line Support" chapters in the *Cisco Unified Communications Manager Features and Services Guide* for details of configuring Cisco Unified Communications Manager Assistant.

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 click **Go**.

Step 3 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 click **Go**.

The Assistant Configuration window displays for this end user. Refer to the "Cisco Unified Communications Manager Assistant With Proxy Line Support" and "Cisco Unified Communications Manager Assistant With Shared Line Support" chapters in the *Cisco Unified Communications Manager Features and Services Guide* for details of configuring Cisco Unified Communications Manager Assistant.

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 4 To show the user privilege report for this end user, from the Related Links drop-down list box, choose User Privilege Report and click **Go**.

The User Privilege window displays for this end user. Refer to the "Viewing User Roles, User Groups, and Permissions" section on page 116-7 for details of the user privilege report.

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 click **Go**.

Additional Information

See the "Related Topics" section on page 114-18.

Associating Devices to an End User

You can associate devices over which end users will 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 (*) displays 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. See the "Finding an End User" section on page 114-8 for information on finding existing end users. When the End User Configuration window displays, 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 displays.

Finding a Device

Because you may have several devices in your network, Cisco Unified Communications Manager 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, Cisco Unified Communications Manager Administration retains your search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your search preferences until you modify your search or close the browser.

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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 display. You can change the number of items that display 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 name(s).

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:

- **Select All**—Click this button to select all devices that display in this window.
- **Clear All**—Click this button to uncheck the check boxes next to all devices that display in this window.
- **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.
- **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.

- **Save Selected/Changes**—Click this button to associate the devices that you have selected with this end user.
- **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 popup window 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 in the upper, right corner of the window, choose **Back to User**, and click **Go**.

The End User Configuration window displays, and the associated devices that you chose display in the Controlled Devices pane.

Additional Information

See the "Related Topics" section on page 114-18.

Associating Cisco Extension Mobility Profiles

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 log 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. See the "Finding an End User" section on page 114-8 for information on accessing information on existing end users. To configure and associate Cisco Extension Mobility for end users, refer to the "Cisco Extension Mobility" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Deleting an End User

To delete an end user in Cisco Unified Communications Manager Administration, perform the following procedure.

Before You Begin

Before you delete the end user, determine whether the devices or profiles that are associated with the end user need to be removed or deleted.

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, see the "Accessing Dependency Records" section on page A-2.

Procedure

Step 1 Choose **User Management** > **End User**.

The Find and List Users window displays.

Step 2 To locate a specific end user, enter search criteria and click **Find**.

A list of end users that match the search criteria displays.

Step 3 Perform one of the following actions:

- Check the check boxes next to the users that you want to delete and click **Delete Selected**.
- Delete all the users in the window by clicking **Select All** and clicking **Delete Selected**.
- Choose the user ID of the user that you want to delete from the list to display its current settings and click **Delete**.

A confirmation dialog displays.

Step 4 Click **OK**.

Next Steps

If this user is configured in Cisco Unity Connection, the user association to Cisco Unified Communications Manager gets broken when you delete the user in Cisco Unified Communications Manager 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* for more information. Deleting the user will delete all messages in the user voice mailbox.

Additional Information

See the "Related Topics" section on page 114-18.

Related Topics

- End User Configuration Settings, page 114-1
- Finding an End User, page 114-8
- Configuring an End User, page 114-9
- Creating a Cisco Unity Connection Voice Mailbox, page 114-10
- Changing an End User Password, page 114-11
- Changing an End User PIN, page 114-11
- Managing End User Credential Information, page 114-12
- Credential Settings and Fields, page 114-13
- Configuring User-Related Information for End Users, page 114-14
- Associating Devices to an End User, page 114-15
- Associating Cisco Extension Mobility Profiles, page 114-17
- Deleting an End User, page 114-17
- Finding an Application User, page 113-5

- Configuring an Application User, page 113-6
- Adding an Administrator User to Cisco Unity or Cisco Unity Connection, page 113-7
- Changing an Application User Password, page 113-9
- Changing an Application User Password, page 113-9
- Managing Application User Credential Information, page 113-9
- Credential Settings and Fields, page 113-10
- Associating Devices to an Application User, page 113-11
- Deleting an Application User, page 113-12
- LDAP System Configuration, page 14-1
- Role Configuration, page 115-1
- User Group Configuration, page 116-1
- Viewing User Roles, User Groups, and Permissions, page 116-7
- Directory Number Configuration, page 64-1
- CTI Route Point Configuration, page 88-1
- Cisco Unified IP Phone Configuration, page 91-1
- Credential Policy Configuration, page 112-1
- Credential Policy Default Configuration, page 111-1
- Credential Policy, *Cisco Unified Communications Manager System Guide*
- Where to Find More Information, *Cisco Unified Communications Manager System Guide*
- Application Users and End Users, *Cisco Unified Communications Manager System Guide*
- Cisco Extension Mobility, *Cisco Unified Communications Manager Features and Services Guide*
- Device Association, *Cisco Unified Communications Manager System Guide*
- Associating a User Device Profile to a User, *Cisco Unified Communications Manager Features and Services Guide*
- Cisco Unified Communications Manager Assistant With Proxy Line Support, *Cisco Unified Communications Manager Features and Services Guide*
- Cisco Unified Communications Manager Assistant With Shared Line Support, *Cisco Unified Communications Manager Features and Services Guide*
- Cisco Unity Messaging Integration, *Cisco Unified Communications Manager System Guide*
- Presence, *Cisco Unified Communications Manager Features and Services Guide*

Related Documentation

- *Cisco Unified Communications Manager Security Guide*
- *User Moves, Adds, and Changes Guide for Cisco Unity Connection*

CHAPTER 115

Role Configuration

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 the Cisco Unified Communications Manager Administration application, 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 nor icons.

Roles comprise groups of resources for an application. At installation, default standard roles get created for various administrative functions. You may, however, create custom roles that comprise custom groupings of resources for an application.

Note Certain standard roles have no associated application nor resource. These roles provide login authentication for various applications.

Use the following topics to configure roles:

- Role Configuration Settings, page 115-2
- Finding a Role, page 115-3
- Configuring a Role, page 115-4
- Deleting a Role, page 115-5
- Related Topics, page 115-5

Additional Information

See the "Related Topics" section on page 115-5.

Role Configuration Settings

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 nor 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 get created for various administrative functions. For example, to configure Audit Log Administration, choose the **Standard Audit Log Administration** role. When the Role Configuration window display, click 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.

Table 115-1 describes the role configuration settings. For related procedures, see the "Related Topics" section on page 115-5.

Table 115-1 Role Configuration 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 have up to 128 characters.
Description	Enter a description for the role. Descriptions can have up to 128 characters.
Resource Access Information	
(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.

Table 115-1 Role Configuration Settings (continued)

Field	Description
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.

Finding a Role

Because you might have several roles in your network, Cisco Unified Communications Manager lets you locate specific roles on the basis of specific criteria. Use the following procedure to locate roles.

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

Procedure

Step 1 Choose **User Management** > **Role**.

The Find and List Roles 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.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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**.

Note You cannot delete standard roles.

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.

Additional Information

See the "Related Topics" section on page 115-5.

Configuring a Role

This section describes how to add a role to Cisco Unified Communications Manager Administration.

The following example provides more detail about configuring a role.

Example

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**.

Procedure

Step 1 Choose **User Management** > **Role**.

The Find and List Roles window displays.

Step 2 Perform one of the following tasks:

- To copy an existing role, locate the appropriate role as described in the "Finding a Role" section on page 115-3 and click the **Copy** button next to the role that you want to copy. In the popup window that displays, enter a name for the new role and click **OK**. Continue with Step 4.

  Note Copying a role also copies the privileges that are associated with that role.

- To add a new role, click the Add New button, and continue with Step 3.

- To update an existing role, locate the appropriate role as described in the "Finding a Role" section on page 115-3 and continue with Step 4.

Step 3 If you are adding a new role, choose an application from the Application drop-down list box and click **Next**.

Step 4 In the Role Configuration window that displays, enter the appropriate settings as described in Table 115-1.

Step 5 To add the role, click **Save**.

The new role gets added to the Cisco Unified Communications Manager database.

Additional Information

See the "Related Topics" section on page 115-5.

Deleting a Role

This section describes how to delete a role in Cisco Unified Communications Manager Administration.

Procedure

Step 1 Choose **User Management** > **Role**.

The Role Configuration window displays.

Step 2 In the list of Roles at left, click the name of the role that you want to delete.

Note You cannot delete a standard role.

The role that you chose displays.

Step 3 Click **Delete**.

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

Step 4 Click **OK**.

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

Additional Information

See the "Related Topics" section on page 115-5.

Related Topics

- Role Configuration Settings, page 115-2
- Finding a Role, page 115-3
- Configuring a Role, page 115-4
- Deleting a Role, page 115-5

- User Group Configuration, page 116-1
- Roles and User Groups, *Cisco Unified Communications Manager System Guide*

CHAPTER 116

User Group Configuration

The role and user group menu options in the Cisco Unified Communications Manager Administration User Management menu allow users with full access to configure different levels of access for Cisco Unified Communications Manager administrators. Users with full access configure roles, user groups, and access privileges for roles. In general, full-access users configure the access of other users to Cisco Unified Communications Manager Administration.

User groups comprise lists of application users and end users. A user may belong to multiple user groups. After you add a user group, you then add users to a user group. Afterward, you may proceed to assign roles to a user group. If a user belongs to multiple user groups, the MLA permission enterprise parameter determines the effective privilege of the user.

Use the following topics to configure user groups, assign users to user groups, and view the roles, user groups, and permissions of a user:

- Finding a User Group, page 116-1
- Configuring a User Group, page 116-2
- Deleting a User Group, page 116-3
- Adding Users to a User Group, page 116-4
- Deleting Users from a User Group, page 116-6
- Assigning Roles to a User Group, page 116-6
- Viewing User Roles, User Groups, and Permissions, page 116-7
- Related Topics, page 116-8

Finding a User Group

Because you might have several user groups in your network, Cisco Unified Communications Manager lets you locate specific user groups on the basis of specific criteria. Use the following procedure to locate user groups.

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

Procedure

Step 1 Choose **User Management** > **User Group**.

The Find and List User Groups 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.

To filter or search records

- From the drop-down list box, select a search pattern.
- 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**.

Note You cannot delete the standard user groups.

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.

Additional Topics

See the "Related Topics" section on page 116-8.

Configuring a User Group

This section describes how to add, copy, and update a user group to and in the Cisco Unified Communications Manager Administration.

The following example provides more detail about configuring a user group.

Example

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 displays, choose the user that you want to add to the group and click **Add Selected**.

Procedure

Step 1 Choose **User Management** > **User Group**.

The Find and List User Groups window displays.

Step 2 Perform one of the followings tasks:

- To copy an existing user group, locate the appropriate user group as described in "Finding a User Group" section on page 116-1 and click the **Copy** button next to the user group that you want to copy. In the popup window that displays, enter a name for the new user group and click **OK**. Continue with Step 3.
- To add a new user group, click the **Add New** button. Enter a name for the new user group and click **OK**. Continue with Step 3.

Note The user group name can contain up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that the user group name is unique.

- To update an existing user group, locate the appropriate user group as described in "Finding a User Group" section on page 116-1. Click the name of the user group that you want to update. The user group that you chose displays. Update the appropriate settings. Continue with Step 3.

Note You cannot delete a standard user group, but you can update the user membership for a standard user group.

Step 3 Click **Save**.

Step 4 Proceed to add users to this user group. See Adding Users to a User Group, page 116-4.

Step 5 Proceed to assign roles to the user group. See Assigning Roles to a User Group, page 116-6.

Additional Topics

See the "Related Topics" section on page 116-8.

Deleting a User Group

This section describes how to delete a user group from Cisco Unified Communications Manager Administration. Use the following procedure to delete a user group entirely. If you want to delete only certain users from a user group, refer to the "Deleting Users from a User Group" section on page 116-6.

Before You Begin

When you delete a user group, Cisco Unified Communications Manager removes all user group data from the database. To find out which roles are using the user group, in the User Group 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. For more information about dependency records, see the "Accessing Dependency Records" section on page A-2.

Procedure

Step 1 Choose **User Management** > **User Group**.

The Find and List User Groups window displays.

Step 2 Find the user group that you want to delete by using the procedure in the "Finding a User Group" section on page 116-1.

Step 3 Click the name of the user group that you want to delete.

The user group that you chose displays. The list shows the users in this user group in alphabetical order.

Step 4 If you want to delete the group entirely, click **Delete**.

A dialog box displays to warn you that you cannot undo deletion of user groups.

Step 5 To delete the user group, click **OK** or to cancel the action, click **Cance**l. If you click **OK**, Cisco Unified Communications Manager removes the user group from the database.

Additional Topics

See the "Related Topics" section on page 116-8.

Adding Users to a User Group

This section describes how to add end users and application users to a user group in Cisco Unified Communications Manager Administration.

Procedure

Step 1 Choose **User Management** > **User Group**.

The Find and List User Groups window displays.

Step 2 Find the user group to which you want to add users. Use the procedure in the "Finding a User Group" section on page 116-1.

Step 3 Click the name of the user group that you want to update.

The user group that you chose displays. The Users in Group list shows the users that currently belong to the user 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 displays.

Step 5 Use the Find User drop-down list boxes to find the end users that you want to add and 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 displays.

Note The list of search results does not display end users that already belong to the user group.

Step 6 In the list of search results, click the check box next to the users that you want to add to this user group. If the list comprises multiple pages, use the links at the bottom to see more results.

Step 7 Click **Add Selected**.

The User Group Configuration window redisplays with the users that you added listed in the Users in Group 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 displays.

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, click the check box next to the application users that you want to add to this user 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 User Group Configuration window redisplays with the application users that you added listed in the Users in Group 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 user group, click **Save**.

Additional Topics

See the "Related Topics" section on page 116-8.

Deleting Users from a User Group

This section describes how to delete users from a user group in Cisco Unified Communications Manager Administration.

Procedure

Step 1 Choose **User Management** > **User Group**.

The Find and List User Groups window displays.

Step 2 Find the user group from which you want to delete users. Use the procedure in the "Finding a User Group" section on page 116-1.

Step 3 Click the name of the user group that you want to update.

The user group that you chose displays. The Users in Group list shows the users that currently belong to the user group.

Step 4 Click the check boxes next to the names of the users that you want to delete from this user group.

Step 5 Click **Delete Selected**.

A confirmation message asks you to confirm the deletion.

Step 6 To delete the selected user group members, click **OK** or click **Cancel** to exit this window.

The User Group redisplays with the deleted users removed from the Users in Group pane.

Additional Topics

See the "Related Topics" section on page 116-8.

Assigning Roles to a User Group

Users with full access can assign roles to user groups. A user group that has assigned roles has access to the resources that the role comprises.

This section describes assigning roles to a user group in Cisco Unified Communications Manager Administration.

Note When an administrator assigns roles to a user group, the administrator should assign the Standard Unified CM Admin Users role to the user group. This role enables the users to log into Cisco Unified Communications Manager Administration.

Procedure

Step 1 Choose **User Management** > **User Group**.

The Find and List User Groups windows displays.

Step 2 Find the user group to which you want to assign roles. Use the procedure in the "Finding a User Group" section on page 116-1.

Step 3 Click the name of the user group for which you want to assign roles.

The user group that you chose displays. The Users in Group list shows the users that currently belong to the user group.

Step 4 From the Related Links drop-down list box, choose **Assign Role to User Group** and click **Go**.

The User Group Configuration window changes to display the Role Assignment pane. For the user group that you chose, the list of assigned roles displays. Choose one of the following options:

- To assign roles to the user group, go to Step 5.
- To delete roles from the user group, go to Step 9.

Step 5 To assign additional roles to the user group, click **Assign Role to Group**.

The Find and List Roles popup window displays.

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 user group by clicking the check boxes next to the role names. To close the Find and List Roles popup window without assigning roles to this user group, click **Close**.

Step 8 Click **Add Selected**.

The Find and List Roles popup window closes. The chosen roles get added to the Role Assignment pane for this user group. If you do not want to delete any assigned roles for this user group, skip to Step 10.

Step 9 To delete an assigned role from the user group, select a role in the Role Assignment pane and click **Delete Role Assignment**. Repeat this step for each role that you want to delete from this user group.

Step 10 Click **Save**.

The system makes the added and deleted role assignments to the user group in the database.

Additional Topics

See the "Related Topics" section on page 116-8.

Viewing User Roles, User Groups, and Permissions

This section describes how to view the roles, user groups, and permissions that are assigned to a user that belongs to a specified user group. Use the following procedure to view the roles, user groups, and permissions that are assigned to a user in a user 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 Group**.

The Find and List User Groups window displays.

Step 2 Find the user group that has the users for which you want to display assigned roles. Use the procedure in the "Finding a User Group" section on page 116-1.

Step 3 Click the name of the user group for which you want to view the roles that are assigned to the users.

The User Group Configuration window displays for the user group that you chose. The Users in Group pane shows the users that belong to the user group.

Step 4 For a particular user, click the user name.

The Application User Configuration window (for application users) or End User Configuration window (for end users) displays.

Step 5 From the Related Links drop-down list box, choose **User Privilege Report** and click **Go**.

For the user that you chose, the following information displays:

- User groups to which the user belongs
- Roles that are assigned to the user
- Resources to which the user has access. For each resource, the following information displays:
  - 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**.

Additional Topics

See the "Related Topics" section on page 116-8.

Related Topics

- Finding a User Group, page 116-1
- Configuring a User Group, page 116-2
- Deleting a User Group, page 116-3
- Adding Users to a User Group, page 116-4
- Deleting Users from a User Group, page 116-6
- Assigning Roles to a User Group, page 116-6
- Viewing User Roles, User Groups, and Permissions, page 116-7
- Roles and User Groups, *Cisco Unified Communications Manager System Guide*
- End User Configuration, *Cisco Unified Communications Manager System Guide*
- Application User Configuration, *Cisco Unified Communications Manager System Guide*

CHAPTER 117

User/Phone Add Configuration

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.

Note The End User, Phone, DN, and LA Configuration window does not allow you to enter existing end users, phones, or directory numbers.

The End User, Phone, DN, and LA Configuration window 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, use 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.

The following topics contain information on adding and configuring end users at the End User, Phone, DN, and LA Configuration window:

- User and Device Configuration Settings, page 117-2
- Adding an End User and Phone, page 117-4

Additional Information

See the "Related Topics" section on page 117-4.

User and Device Configuration Settings

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 verify that the Enable Synchronizing from LDAP Server check box is not checked, choose **System > LDAP > LDAP System**. If synchronization is enabled (checked), access to the End User, Phone, DN, and LA Configuration window is blocked.

Table 117-1 describes the end user configuration settings. For related procedures, see the "Related Topics" section on page 117-4.

Table 117-1 User and Device Configuration 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.

Table 117-1 User and Device Configuration Settings (continued)

Field	Description
Device Associations	
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.

Adding an 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**.

The End User, Phone, DN, and LA Configuration window displays.

Note If LDAP synchronization is enabled, access to this window is blocked. For more information about LDAP synchronization, see the "LDAP System Configuration" section on page 14-1.

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 to return to the End User, Phone, DN, and LA Configuration window.

Step 2 Enter the appropriate settings as described in Table 117-1.

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.

Additional Information

See the "Related Topics" section on page 117-4.

Related Topics

- User and Device Configuration Settings, page 117-2
- Adding an End User and Phone, page 117-4
- Application Users and End Users, *Cisco Unified Communications Manager System Guide*
- Cisco Unified IP Phones, *Cisco Unified Communications Manager System Guide*

- Understanding Directory Numbers, *Cisco Unified Communications Manager System Guide*
- Finding an End User, page 114-8
- Configuring an End User, page 114-9
- Changing an End User Password, page 114-11
- Changing an End User Password, page 114-11
- Changing an End User PIN, page 114-11
- Associating Devices to an End User, page 114-15
- Associating Cisco Extension Mobility Profiles, page 114-17
- LDAP System Configuration, page 14-1
- Directory Number Configuration, page 64-1
- CTI Route Point Configuration, page 88-1
- Cisco Unified IP Phone Configuration, page 91-1
- Cisco Extension Mobility, *Cisco Unified Communications Manager Features and Services Guide*
- Associating a User Device Profile to a User, *Cisco Unified Communications Manager Features and Services Guide*

CHAPTER 118

Application User CAPF Profile Configuration

The Application User CAPF Profile Configuration window in Cisco Unified Communications Manager Administration allows you to issue locally significant certificates to secure application users. After you issue the certificate and perform other security-related tasks, a TLS connection opens between the CTIManager service and the application that is activated on the server.

One Application User CAPF Profile corresponds to a single instance of an application on a server. For example, if you activate an application on two servers in the cluster, you must configure two Application User CAPF Profiles, one for each server. If you activate two different applications on the same server, you must configure two Application User CAPF Profiles, one for each application on the server.

For information on how to configure the Application User CAPF Profile, refer to the *Cisco Unified Communications Manager Security Guide*.

CHAPTER 119

End User CAPF Profile Configuration

The End User CAPF Profile Configuration window in Cisco Unified Communications Manager Administration allows you to issue locally significant certificates to CTI clients. After you issue the certificate and perform other security-related tasks, the CTI client communicates with the CTIManager service via a TLS connection.

For information on how to configure the End User CAPF Profile, refer to the *Cisco Unified Communications Manager Security Guide*.

CHAPTER 120

SIP Realm Configuration

When you configure digest authentication for SIP trunks, Cisco Unified Communications Manager challenges the identity of the SIP user agent that connects to the trunk every time the trunk sends a SIP request to Cisco Unified Communications Manager; the SIP user agent, in turn, can challenge the identity of Cisco Unified Communications Manager. For Cisco Unified Communications Manager to respond to a challenge from the SIP user agent, you must configure the SIP realm for Cisco Unified Communications Manager.

For information on how to configure SIP realm for Cisco Unified Communications Manager, refer to the *Cisco Unified Communications Manager Security Guide*.

PART 9

Cisco Unified Communications Manager Bulk Administration

CHAPTER 121

Bulk Administration Tool (BAT)

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.

For more information about the BAT and TAPS, refer to the *Cisco Unified Communications Manager Bulk Administration Guide*.

PART 10

Appendixes

APPENDIX A

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.

This appendix contains the following sections:

Enabling 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**.

Disabling 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**.

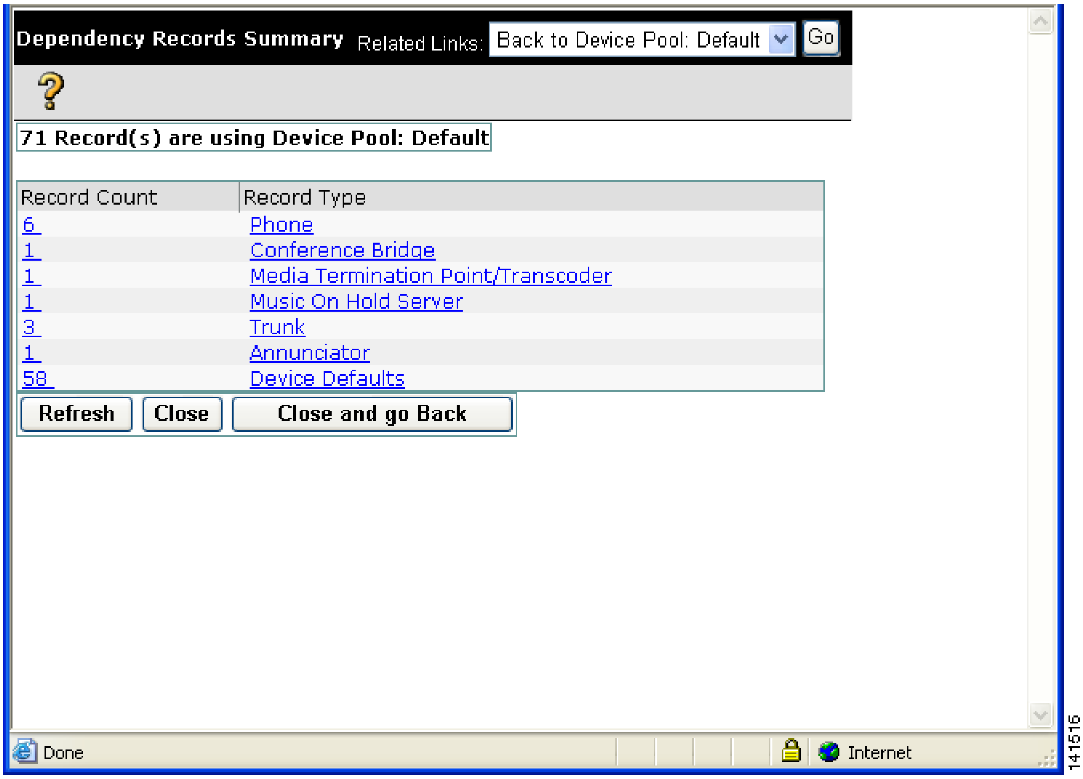
Accessing Dependency Records

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. To enable dependency records, see the "Enabling Dependency Records" section on page A-1.

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 Figure A-1.

Figure A-1 Dependency Records—Summary Example



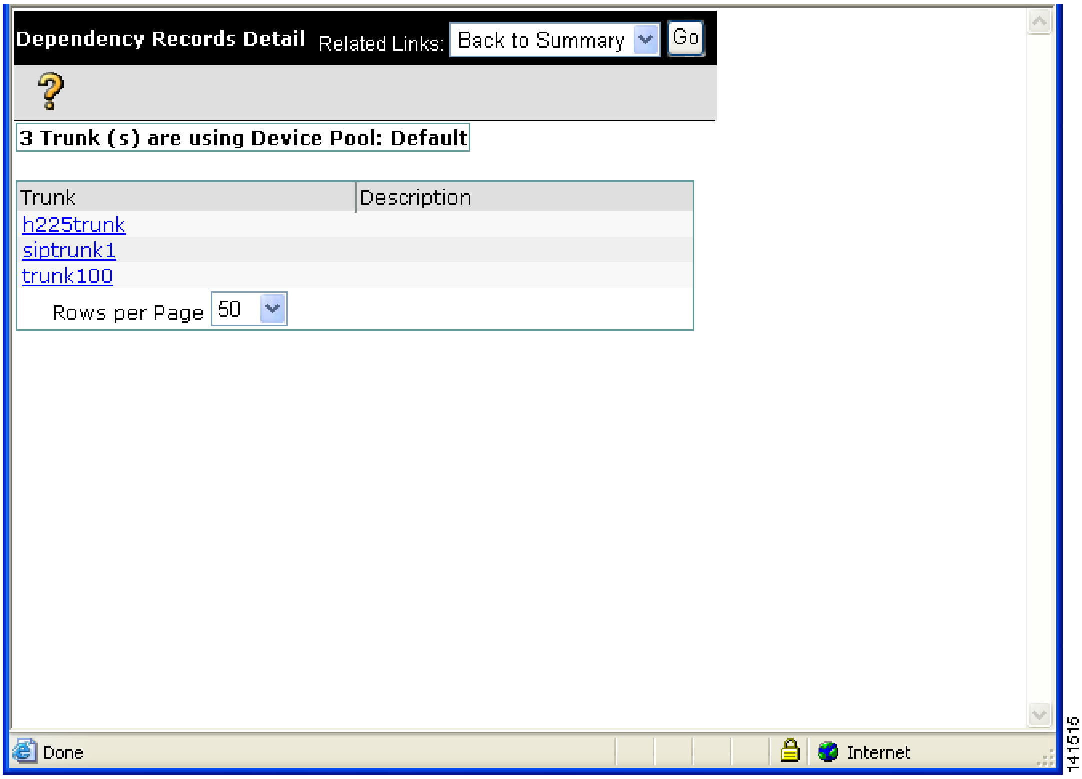
Dependency Records Summary Related Links: Back to Device Pool: Default Go

71 Record(s) are using Device Pool: Default

Record Count	Record Type
6	Phone
1	Conference Bridge
1	Media Termination Point/Transcoder
1	Music On Hold Server
3	Trunk
1	Annunciator
58	Device Defaults

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 Figure A-2. 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 A-2 Dependency Records—Detail Example



3 Trunk (s) are using Device Pool: Default

Trunk	Description
h225trunk	
siptrunk1	
trunk100	

Rows per Page 50

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 Figure A-2, the Trunk Configuration window displays with information about the h225trunk.

Dependency Records 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 B

Configuring Non-Cisco Phones That Are Running SIP

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.

This appendix contains the following sections:

- Where to Find More Information, page B-6
- Configuration Differences for Phones That Are Running SIP, page B-3
- Migrating from Cisco Unified Communications Manager Release 5.0 to Release 7.1(2), page B-5
- Where to Find More Information, page B-6

Configuration Checklist for Third-Party Phones That Are Running SIP

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. Table B-1 provides steps to manually configure a third-party phone that is running SIP by using Cisco Unified Communications Manager Administration.

Table B-1 Configuration Checklist for Third-Party Phone That Is Running SIP

Configuration Steps		Procedures and Related Topics
Step 1	Gather the following 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	

Table B-1 Configuration Checklist for Third-Party Phone That Is Running SIP (continued)

Configuration Steps		Procedures and Related Topics
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.	Calculating License Units, page 31-1 Obtaining a License File, page 32-2
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).	Configuring an End User, page 114-9
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.	Configuring SIP Profiles, page 101-10 Configuring Cisco Unified IP Phones, page 91-27
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.	Enabling Digest Authentication for Third-Party Phones That Are Running SIP, page B-4 Phone Security Profile Configuration, *Cisco Unified Communications Manager Security Guide*
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.	Configuring Cisco Unified IP Phones, page 91-27
Step 7	Add and configure lines (DNs) on the phone.	Directory Number Configuration, page 64-1
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.	Associating Devices to an End User, page 114-15
Step 9	In the Digest User field of the Phone Configuration window, choose the end user that you created in Step 3.	Configuring Speed-Dial Buttons or Abbreviated Dialing, page 91-34
Step 10	Provide power, install, verify network connectivity, and configure network settings for the third-party phone that is running SIP.	Refer to 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.	Refer to the user guide that came with your third-party phone that is running SIP.

Configuration Differences for Phones That Are Running SIP

Table B-2 provides a comparison overview of the configuration differences between Cisco Unified IP Phones and third-party phones that are running SIP.

Table B-2 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 (see the "Where to Find More Information" section on page B-6). 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.

How Cisco Unified Communications Manager Identifies a Third-Party Phone

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 (see Configuring an End User, page 114-9). 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, page 91-27).

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 That Are 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.

Enabling Digest Authentication for Third-Party Phones That Are Running SIP

To enable digest authentication for third-party phones that are running SIP, the administrator must create a Phone Security Profile. (See Phone Security Profile Configuration in the *Cisco Unified Communications Manager Administration Guide*.) 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.

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 for Third-Party Phones That Are Running SIP

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.

Migrating from Cisco Unified Communications Manager Release 5.0 to Release 7.1(2)

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. See Table B-3 and Table B-4 for more information.

Table B-3 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
Default Maximum Number of Calls per DN	4	2
Default Busy Trigger per DN	2	2

Table B-4 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

- Configuration Checklist for Third-Party Phones That Are Running SIP, page B-1
- Directory Number Configuration, page 64-1
- Cisco Unified IP Phone Configuration, page 91-1
- SIP Profile Configuration, page 101-1
- End User Configuration, page 114-1
- Cisco Unified IP Phones, *Cisco Unified Communications Manager System Guide*

INDEX