System Configuration Guide for Cisco Unified Communications Manager, Release 12.0(1)

First Published: 2017-08-17

Last Modified: 2024-02-02

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

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

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

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

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

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

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

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

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

CHAPTER 1

System Configuration Overview

About System Configuration

This document provides information about the tasks that you need to perform in order to configure the call control system. It contains information such as task flows, procedures, and prerequisites.

For information about system planning, see http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html.

PART I

Configure Initial Parameters for the System

CHAPTER 2

Initial System Parameters

About Initial Configuration

The chapters in this section describe the initial setup tasks that you must complete before you begin to configure the call control system.

Initial Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Smart Software Licensing Task Flow, on page 10	Manage the license requirements for your system.
Step 2	Server Configuration Task Flow, on page 19	Configure basic server information, such as the server name and port settings.
Step 3	Initial System and Enterprise Configuration Task Flow, on page 25	Configure the system-wide parameters that are required when you set up a node for the first time.
Step 4	Service Parameters Configuration Task Flow, on page 35	Configure the service parameters that are required when you set up a node for the first time.
Step 5	Core Settings for Device Pools Configuration Task Flow, on page 48	Configure core system settings, such as a server group, time zone information, and a region (codec selection). These settings are fundamental and become the foundation for basic device pools.

CHAPTER 3

Smart Software Licensing

Smart Software Licensing Overview

Cisco Smart Software Licensing is a new way of thinking about licensing. It adds flexibility to your licensing and simplifies it across the enterprise. It also delivers visibility into your license ownership and consumption.

Cisco Smart Software Licensing helps you to procure, deploy, and manage licenses easily where devices self-register and report license consumption, removing the need for product activation keys (PAK). It pools license entitlements in a single account and allows you to move licenses freely through the network, wherever you need them. It is enabled across Cisco products and managed by a direct cloud-based or mediated deployment model.

The Cisco Smart Software Licensing service registers the product instance, reports license usage, and obtains the necessary authorization from Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

You can use Smart Licensing to:

- See the license usage and count
- See the status of each license type
- See the product licenses available on Cisco Smart Software Manager or Cisco Smart Software Manager satellite
- Renew License Authorization with Cisco Smart Software Manager or Cisco Smart Software Manager satellite
- Renew the License Registration
- Deregister with Cisco Smart Software Manager or Cisco Smart Software Manager satellite

Note The License authorization is valid for 90 days with a renewal at least once in 30 days. The authorization will expire after 90 days if it is not connected to Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

If the Cisco Smart Software Manager satellite option is selected, the satellite must have an internet connection to Cisco Smart Software Manager for the authorization to occur. The Cisco Smart Software Manager satellite can operate in 2 modes: Connected Mode in which the connection time is configurable, and Disconnected mode which requires a manual sync.

There are two main deployment options for Smart Licensing:

- Cisco Smart Software Manager
- Cisco Smart Software Manager satellite

Cisco Smart Software Manager

The Cisco Smart Software Manager is a cloud-based service that handles your system licensing. Use this option if Unified Communications Manager can connect to cisco.com, either directly or via a proxy server. Cisco Smart Software Manager allows you to:

- Manage and track licenses
- Move licenses across virtual account
- Remove registered product instance

Optionally, if Unified Communications Manager cannot connect directly to Cisco Smart Software Manager, you can deploy a proxy server to manage the connection.

For additional information about Cisco Smart Software Manager, go to https://software.cisco.com.

Cisco Smart Software Manager Satellite

Cisco Smart Software Manager satellite is an on-premise deployment that can handle your licensing needs if Unified Communications Manager cannot connect to cisco.com directly, either for security or availability reasons. When this option is deployed, Unified Communications Manager registers and report license consumption to the satellite, which synchronizes its database regularly with the backend Cisco Smart Software Manager that is hosted on cisco.com.

The Cisco Smart Software Manager satellite can be deployed in either Connected or Disconnected mode, depending on whether the satellite can connect directly to cisco.com.

- Connected—Used when there is connectivity to cisco.com directly from the Smart Software Manager satellite. Smart account synchronization occurs automatically.
- Disconnected—Used when there is no connectivity to cisco.com from the Smart Software Manager satellite. Smart Account synchronization must be manually uploaded and downloaded.

For Cisco Smart Software Manager satellite information and documentation, go to https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html.

License Types

The following licensing types are available to cover your needs:

Cisco Unified Workspace Licensing

Cisco Unified Workspace Licensing (UWL) provides the most popular bundles of Cisco Collaboration applications and services in a cost-effective, simple package. It includes soft clients, applications server software, and licensing on a per-user basis.

Cisco User Connect Licensing

User Connect Licensing (UCL) is a per-user based license for individual Cisco Unified Communications applications, which includes the applications server software, user licensing, and a soft client. Depending on the type of device and number of devices that you require, UCL is available in Essential, Basic, Enhanced, and Enhanced Plus versions.

For more information about these license types and the versions in which they are available, see http://www.cisco.com/c/en/us/products/unified-communications/unified-communications-licensing/index.html.

Session Management Edition

Session Management Edition can be registered to either Cisco Smart Software Manager or Cisco Smart Software Manager satellite. You can register Session Management Edition using the same processes as for Unified Communications Manager, register to a virtual account that Cisco Unified Communications Manager is registered or a separate virtual account, and fulfill a minimal set of licenses requirement.

Note The SME registered in Specific License Reservation (SLR) requires a minimum set of licenses reserved in CSSM while generating an SLR authorization code.

Product Instance Evaluation Mode

After installation, Unified Communications Manager runs under the 90-day evaluation period. At the end of the evaluation period, Unified Communications Manager stops allowing addition of new users or devices until registered with Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Note Evaluation period is before the product is registered.

System Licensing Prerequisites

Planning your System Licensing

Review and understand the Unified Communications (UC) licensing structure. For details, see http://www.cisco.com/c/en/us/products/unified-communications/unified-communications-licensing/index.html.

Plan how you are going to connect Unified Communications Manager to the Smart Software Manager service:

- Direct connection to Cisco Smart Software Manager on cisco.com—Unified Communications Manager connects directly to the Cisco Smart Software Manager on cisco.com. With this option, you must configure DNS on Unified Communications Manager that resolves `tools.cisco.com`.
- Connection to Smart Software Manager via proxy server—Unified Communications Manager connects to a proxy server or transport gateway, which connects to the Cisco Smart Software Manager service on cisco.com. DNS is not required on Unified Communications Manager, but you do need to configure DNS on the proxy server that can resolve `tools.cisco.com`.
- Connection to on-premise Cisco Smart Software Manager satellite—Unified Communications Manager connects to an on-premise Smart Software Manager satellite. DNS is not required on Unified Communications Manager. DNS that can resolve `tools.cisco.com` is required on the satellite server if you are deploying Connected mode. DNS is not required on the satellite server if you are deploying Disconnected mode.

Smart Licensing Enrollment

Set up Smart and Virtual accounts. For details, see https://software.cisco.com/.

Optional. If you want to deploy Cisco Smart Software Manager satellite, install and set up the satellite. Refer to documentation, including the *Smart Software Manager satellite Installation Guide*. You can find documentation at https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html.

Smart Software Licensing Task Flow

Complete these tasks to set up system licensing for Unified Communications Manager.

Procedure

	Command or Action	Purpose
Step 1	Obtain the Product Instance Registration Token, on page 11.	Use this procedure to generate a product instance registration token for your virtual account.
Step 2	Configure Connection to Smart Software Licensing, on page 11	Select transport settings through which Unified Communications Manager connects to the Smart Software Licensing service. The **Direct** option is selected by default where the product communicates directly with Cisco licensing servers.
Step 3	Register with Cisco Smart Software Manager, on page 12.	Perform this step to register Unified Communications Manager with Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Obtain the Product Instance Registration Token

Before you begin

Obtain the product instance registration token from Cisco Smart Software Manager or Cisco Smart Software Manager satellite to register the product instance. Tokens can be generated with or without the Export-Controlled functionality feature being enabled.

Procedure

Step 1 Log in to your smart account in either Cisco Smart Software Manager or your Cisco Smart Software Manager satellite.

Step 2 Navigate to the virtual account with which you want to associate the Unified Communications Manager cluster.

Step 3 Generate a “Product Instance Registration Token”.

Note Select the **Allow export-controlled functionality on the products registered with this token** check box to turn on the Export-Controlled functionality for tokens of a product instance you wish in this smart account. By checking this check box and accepting the terms, you enable higher levels of the product encryption for products registered with this Registration Token. By default, this check box is selected. You can uncheck this check box if you wish not to allow the Export-Controlled functionality to be made available for use with this token.

Caution Use this option only if you are compliant with the Export-Controlled functionality.

Note The **Allow export-controlled functionality on the products registered with this token** check box is not displayed for the Smart Accounts that are not permitted to use the Export-Controlled functionality.

Step 4 Copy the token or save it to another location.

For more information, see https://software.cisco.com/.

Configure Connection to Smart Software Licensing

Complete this task to connect Unified Communications Manager to the Smart Software Licensing service.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Licensing** > **License Management**.
The **License Management** window appears.

Step 2 From the **Smart Software Licensing** section, click the **View/Edit the Licensing Smart Call Home settings** link.
The **Transport Settings** dialog box appears.

Step 3 Select the method of connecting Unified Communications Manager to the Smart Licensing service:

- **Direct**—Unified Communications Manager connects directly to the Smart Software Manager on cisco.com. This is the default option. With this option, you must deploy DNS on Unified Communications Manager that can resolve `tools.cisco.com`.
- **Transport Gateway**—Unified Communications Manager connects to an on-premise Cisco Smart Software Manager satellite or Transport Gateway for system licensing. In the URL text box, enter the address and port of the Smart Software Manager satellite or Transport Gateway. For example, `fqdn_of_smart_software_manager:port_number`. For HTTPS, use port 443.
- **HTTP/HTTPS Proxy**— Unified Communications Manager connects to a proxy server, which connects to the Cisco Smart Software Manager service along with Transport Gateway also along with satellite on cisco.com. Enter the IP address or hostname of the proxy server along with the port:
  - IP Address/Host Name
  - Port—For HTTPS, use port 443.

Step 4 Check the **Do not share my hostname or IP address with Cisco** check box to restrict Unified Communications Manager from sharing its IP address and hostname during the Smart Licensing registration.

Step 5 Click **Save**.

Register with Cisco Smart Software Manager

Use this procedure to register your product with Cisco Smart Software Manager or Cisco Smart Software Manager satellite. Until you register, your product is still in Evaluation Mode.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Licensing** > **License Management**.
The **License Management** window appears.

Step 2 From the **Smart Software Licensing** section, click the **Register** button.
The **Registration** window appears.

Step 3 In the **Product Instance Registration Token** section, paste the copied or saved “Registration Token Key” that you generated using the Smart Software Manager or Smart Software Manager satellite.

Step 4 Click **Register** to complete the registration process.

Step 5 Click **Close**. For more information, see the online help.

Step 6 In the **License Usage Report** section, click **Update Usage Details** to manually update the system license usage information.

Note Usage information is updated once every 24 hours automatically. For more information, see the online help.

Additional Tasks with Smart Software Licensing

The following optional tasks are available for Unified Communications Manager and Smart Software Licensing:

Procedure

	Command or Action	Purpose
Step 1	Renew Authorization, on page 14	Complete this task to manually renew the License Authorization Status for all the license listed under the License Type. **Note** The license authorization is renewed automatically every 30 days. The authorization status will expire after 90 days if it is not connected to Cisco Smart Software Manager or Cisco Smart Software Manager satellite. If the Cisco Smart Software Manager satellite option is selected, the satellite must have an internet connection to Cisco Smart Software Manager for the authorization to occur. The Cisco Smart Software Manager satellite can operate in 2 modes: Connected Mode in which the connection time is configurable, and Disconnected mode which requires a manual sync.
Step 2	Renew Registration, on page 15	Complete this task to renew the registration information manually. **Note** The initial registration is valid for one year. Renewal of registration is automatically done every six months provided the product is connected to Cisco Smart Software Manager or Cisco Smart Software Manager satellite.
Step 3	Deregister, on page 15	Complete this task to disconnect the Unified Communications Manager cluster from Cisco Smart Software Manager or Cisco Smart Software Manager satellite. The product reverts to evaluation mode as long as the evaluation period is not expired. All license entitlements used for the product are immediately released

	Command or Action	Purpose
		back to the virtual account and are available for other product instances to use it.
Step 4	Reregister License with Cisco Smart Software Manager, on page 17	Complete this task to reregister Unified Communications Manager with Cisco Smart Software Manager or Cisco Smart Software Manager satellite. **Note** Product may migrate to a different virtual account by reregistering with token from a new virtual account.

Renew Authorization

Use this procedure to manually renew the License Authorization Status for all the licenses listed under the License Type.

Note The license authorization is renewed automatically every 30 days. The authorization status will expire after 90 days if it is not connected to Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

If the Cisco Smart Software Manager satellite option is selected, the satellite must have an internet connection to Cisco Smart Software Manager for the authorization to occur. The Cisco Smart Software Manager satellite can operate in 2 modes: Connected Mode in which the connection time is configurable, and Disconnected mode which requires a manual sync.

Before you begin

The product should be registered with Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Licensing** > **License Management**.
The **License Management** window appears.

Step 2 From the **Smart Software Licensing** section, click the **Actions** drop-down list.

Step 3 Choose **Renew Authorization Now**.
The **Renew Authorization** window appears.

Step 4 Click **Ok**.

Unified Communications Manager sends a request to Cisco Smart Software Manager or Cisco Smart Software Manager satellite to check the “License Authorization Status” and Cisco Smart Software Manager or Cisco Smart Software Manager satellite reports back the status to Unified Communications Manager. For more information, see the online help.

Step 5 In the **License Usage Report** section, click **Update Usage Details** to manually update the system license usage information.

Note Usage information is updated once every 24 hours automatically. For more information on the fields and their configuration options, see the system Online Help.

Renew Registration

During product registration to Cisco Smart Software Manager or Cisco Smart Software Manager satellite, there is a security association used to identify the product and is anchored by the registration certificate, which has a lifetime of one year (that is, registration period). This is different from the registration token ID expiration, which has the time limit for the token to be active. This registration period is automatically renewed every 6 months. However, if there is an issue, you can manually renew this registration period.

Before you begin

The product should be registered with Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Licensing** > **License Management**.
The **License Management** window appears.

Step 2 From the **Smart Software Licensing** section, click the **Actions** drop-down list.

Step 3 Choose **Renew Registration Now**.
The **Renew Registration** window appears.

Step 4 Click **Ok**.

Unified Communications Manager sends a request to Cisco Smart Software Manager or Cisco Smart Software Manager satellite to check the “Registration Status” and Cisco Smart Software Manager or Cisco Smart Software Manager satellite reports back the status to Unified Communications Manager.

Step 5 In the **License Usage Report** section, click **Update Usage Details** to manually update the system license usage information.

Note Usage information is updated once every 24 hours automatically. For more information on the fields and their configuration options, see the system Online Help.

Deregister

Use this procedure to unregister from Cisco Smart Software Manager or Cisco Smart Software Manager satellite and release all the licenses from the current virtual account. This procedure also disconnects Unified Communications Manager cluster from Cisco Smart Software Manager or Cisco Smart Software Manager satellite. All license entitlements used for the product are released back to the virtual account and is available for other product instances to use.

Note If Unified Communications Manager is unable to connect with the Cisco Smart Software Manager or Cisco Smart Software Manager satellite, and the product is still deregistered, then a warning message is displayed. This message notifies you to remove the product manually from Cisco Smart Software Manager or Cisco Smart Software Manager satellite to free up licenses.

Before you begin

The product should be registered with Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Licensing** > **License Management**.
The **License Management** window appears.

Step 2 From the **Smart Software Licensing** section, click the **Actions** drop-down list.

Step 3 Choose **Deregister**.
The **Deregister** window appears.

Step 4 Click **Ok**.

Step 5 In the **License Usage Report** section, click **Update Usage Details** to manually update the system license usage information.

Note Usage information is updated once every 24 hours automatically. For more information on the fields and their configuration options, see the system Online Help.

Note

- If the data plane encryption (Unified Communications Manager cluster in mixed-mode) has been enabled after registered with Cisco Smart Software Manager or Cisco Smart Software Manager satellite and the product is later deregistered, then mixed-mode will continue to be enabled.

  An alert named SmartLicenseExportControlNotAllowed is sent to the administrator to set cluster to non-secure mode when the product is deregistered from Cisco Smart Software Manager or Cisco Smart Software Manager satellite. The mixed-mode will continue to be enabled even after the reboot.

- This behavior after deregistration, may change in future versions of the product. For more details on setting up CTL Client, see the “Set Up Cisco CTL Client” chapter of the *Security Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-maintenance-guides-list.html.

  For more details on Mixed Mode with Tokenless CTL, see the “CUCM Mixed Mode with Tokenless CTL” section at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-tech-notes-list.html.

Reregister License with Cisco Smart Software Manager

Use this procedure to Reregister Cisco Unified Communications Manager with Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Before you begin

Obtain the Product Instance Registration Token, on page 11.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Licensing** > **License Management**.
The **License Management** window appears.

Step 2 From the **Smart Software Licensing** section, click the **Register** button.
The **Registration** window appears.

Step 3 From the **Smart Software Licensing** section, click the **Actions** drop—down list.

Step 4 Choose **Reregister**.
The **Reregister** window appears.

Step 5 Click **Ok**.

Step 6 In the **Product Instance Registration Token** section, paste the copied or saved “Registration Token Key” that you generated using the Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Step 7 Click **Register** to complete the registration process.

Step 8 Click **Close**. For more information, see the online help.

Step 9 In the **License Usage Report** section, click **Update Usage Details** to manually update the system license usage information.

Note Usage information is updated once every 24 hours automatically. For more information on the fields and their configuration options, see the system Online Help.

Version Independent Licensing

Important This section is applicable from Release 14 onwards.

Unified Communications Manager supports Version Independent User Licenses. The Licenses are annuity-style and issued for the subscription term. You can order these V14 licenses through Flex EA (Enterprise Agreement) or Flex NU (Named User—Professional, Enhanced, Access). For more information, see the Ordering Guide.

Unified Communications Manager continues to use the version 12.X License.

The licenses are managed on CSSM (Cisco Smart Software Manager). For more information, see Smart Software Licensing, on page 7.

CHAPTER 4

Configure Server Information

System Information Overview

This chapter describes how to configure the properties of the Unified Communications Manager node.

Note All Unified Communications products such as Unified Communications Manager, Cisco Unity Connections, and Cisco IM and Presence, and so on, have only one interface. Thus, you can assign only one IP address for each of these products.

Server Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure Server Information, on page 20	Specify a name for the Unified Communications Manager node, and add a description.
Step 2	Configure Ports , on page 20	Configure the following ports: • Ethernet Phone Port • MGCP Listen Port • MGCP Keep-alive Port • SIP Phone Port • SIP Phone Secure Port

Configure Server Information

Specify a name for the Unified Communications Manager node, and add a description. You can also use this procedure to view the following read-only information:

- The computer telephony integration identification (CTI ID).
- The server where this Unified Communications Manager is installed.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, select **System** > **Cisco Unified CM**.
The **Find and List Cisco Unified CMs** window appears.

Step 2 Enter the appropriate search criteria and click **Find**.
All matching Cisco Unified Communications Managers are displayed.

Step 3 Select the **Cisco Unified CM** that you want to view.
The **Cisco Unified CM Configuration** window appears.

Step 4 In the **Name** field, enter the name that you want to assign to this Cisco Unified Communications Manager.

Step 5 In the **Description** field, enter a description for the node.

The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).

Step 6 Click **Save**.

Configure Ports

Use this procedure to change the port settings used for connections such as SCCP device registration, SIP device registration, and MGCP gateway connections.

Note Normally, you need not change the default port settings. Use this procedure only if you really want to change the defaults.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, select **System** > **Cisco Unified CM**.
The **Find and List Cisco Unified CMs** window appears.

Step 2 Enter the appropriate search criteria and click **Find**.
All matching Cisco Unified Communications Managers are displayed.

Step 3 Select the **Cisco Unified CM** that you want to view.
The **Cisco Unified CM Configuration** window appears.

Step 4 Navigate to the **Cisco Unified Communications Manager TCP Port Settings for this Server** section.

Step 5 Click **Save**.

Step 6 Click **Apply Config**.

Step 7 Click **OK**.

Port Settings

Field	Description
Ethernet Phone Port	The system 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.
MGCP Listen Port	The system 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	The system 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 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 the system uses to listen for SIP line registrations over TLS.
SIP Phone OAuth Port	This field specifies the port number that Cisco Unified Communications Manager uses to listen for SIP line registrations from Jabber On-Premise devices over TLS (Transport Layer Security). The default value is 5090. Range is 1024 to 49151.
SIP Mobile and Remote Access OAuth Port	This field specifies the port number that Cisco Unified Communications Manager uses to listen for SIP line registrations from Jabber over Expressway through MTLS (Mutual Transport Layer Security). The default value is 5091. Range is 1024 to 49151.

Hostname Configuration

Table5-2 lists the locations where you can configure a host name for the Unified Communications Manager server, the allowed number of characters for the host name, and the recommended first and last characters for the host name. Be aware that if you do not configure the host name correctly, some components in Unified Communications Manager, such as the operating system, database, installation, and so on, may not work as expected.

Caution Before you change the host name or IP address for any locations that are listed in Table5-2, see Changing the IP Address and Host Name for Unified Communications Manager 8.5(1). Failing to update the host name or IP address correctly after it is configured may cause problems for Unified Communications Manager.

Table 1: Host Name Configuration in Cisco Unified Communications Manager

Host Name Location	Allowed Configuration	Allowed Number of Characters	Recommended First Character for Host Name	Recommended Character for H
Host Name/ IP Address field **System** > **Server** in Cisco Unified Communications Manager Administration	You can add or change the host name for a server.	2-63	alphabetic	alphanumeric
Hostname field Cisco Unified Communications Manager installation	You can add the host name for a server.	1-63	alphabetic	alphanumeric
Hostname field **Settings** > **IP** > **Ethernet** in Cisco Unified Communications Operating System	You can change, not add, the host name for a server.	1-63	alphabetic	alphanumeric
set network hostname hostname Command Line Interface	You can change, not add, the host name for a server.	1-63	alphabetic	alphanumeric

Tip The host name must follow the rules for ARPANET host names. Between the first and last character of the host name, you can enter alphanumeric characters and hyphens.

Before you configure the host name in any location in Table5-2, review the following information:

- The Host Name/IP Address field in the Server Configuration window, which supports device-to-server, application-to-server, and server-to-server communication, allows you to enter an IPv4 address in dotted decimal format or a host name.

  In this field, only configure a host name if Unified Communications Manager can access the DNS server to resolve host names to IP addresses; make sure that you configure the Unified Communications Manager name and address information on the DNS server.

Tip In addition to configuring Unified Communications Manager information on the DNS server, you enter DNS information during the Unified Communications Manager installation.

CHAPTER 5

Configure System and Enterprise Parameters

Initial System and Enterprise Parameters Overview

Consider the following system-wide parameters when you set up a Unified Communications Manager node for the first time. You can modify system-wide parameters for your deployment if needed; however, the recommended default settings should work in most cases.

- Set the fall-back connection monitor duration for IP phones.
- Allow searches of the corporate directory for all users.
- Set the Fully Qualified Directory Number (FQDN) for the cluster and the top-level domain for the organization.
- Set the Cisco Jabber start condition for video.
- (Optional) Enable Multi-Level Precedence and Preemption (MLPP) if your cluster uses MLPP.
- (Optional) Enable IPv6 if your network uses IPv6.
- (Optional) Enter a remote syslog server name.
- (Optional) Set up call trace log to troubleshoot your deployment.
- (Optional) Enable dependency records.

Initial System and Enterprise Configuration Task Flow

Before you begin

Set up your Unified Communications Manager node and port settings.

Procedure

	Command or Action	Purpose
Step 1	Configure Initial System and Enterprise Parameters, on page 26	Configure the system-wide parameters that are required for an initial setup of your Unified Communications Manager node. For a list of the recommended system settings, see Common Enterprise Parameters, on page 28.
Step 2	Configure SSO Login Behavior for Cisco Jabber on iOS, on page 32	Configure the enterprise parameter that is required to allow Cisco Jabber to perform certificate-based authentication with the IdP in a controlled mobile device management (MDM) deployment.
Step 3	Configure SSO for RTMT, on page 33	Configure the enterprise parameter through Unified Communications Manager to enable SAML SSO for Real-Time Monitoring Tool (RTMT).

What to do next

Configure some core settings for device pools to lay a foundation of common settings to apply across all devices that are configured in the Unified Communications Manager cluster, see Core Settings for Device Pools Configuration Task Flow, on page 48 .

Configure Initial System and Enterprise Parameters

You can use Cisco Unified Communications Manager Administration to configure system and enterprise parameters for your particular deployment. Although we've listed parameters that are important for an initial system setup, the recommended default settings work for most deployments.

Parameters that are useful for troubleshooting, such as enabling call trace logs, should be disabled after you are finished troubleshooting so that network performance is not impacted.

Most parameters require that you reset all devices for the changes to take effect. Consider completing all configuration steps before you perform a reset of all devices. We recommend that you reset all devices during off-peak hours.

Note From Release 10.0(1), the same enterprise parameters are used on Unified Communications Manager and IM and Presence Service. If you change the value of an enterprise parameter on IM and Presence Service, the changed value is automatically updated to Unified Communications Manager.

Procedure

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

Step 2 In the **Enterprise Parameters Configuration** section, enter the number of seconds in the **Connection Monitor Duration** field before a IP phone in the cluster falls back to the primary node when the TCP connection becomes available, then click **Save**. The default value is 120 seconds.

Tip To apply the changes to all affected devices in the cluster without resetting all devices, click **Apply Config**, and then click **OK**.

Step 3 In the **User Data Service Parameters** section, select **True** in the **Enable All User Search** field to allow users to search the corporate directory for all users when no last name, first name, or directory number is specified.

Step 4 In the **Clusterwide Domain Configuration** section, set up the clusterwide domain.

a) Enter the top-level domain for the organization in the **Organization Top Level Domain** field. The maximum length is 255 characters.
b) Enter the Fully Qualified Domain Name (FQDN) for the cluster in the **Cluster Fully Qualified Domain Name** field. The maximum length is 255 characters.

   Multiple FQDNs must be separated by a space. Wildcards can be specified within an FQDN using an asterisk (*). Example: cluster-1.cisco.com *.cisco.com.

Step 5 In the Cisco Jabber section, select **False** in the **Never Start Call with Video** field.

Step 6 (Optional) In the **MLPP and Confidential Access Level Parameters** section, enter the Multi-Level Precedence and Preemption (MLPP) domain and enable devices to use MLPP.

a) Enter the domain for the MLPP service in the **MLPP Domain Identifier** field. This parameter accepts hexadecimal values starting with 0x.
b) Select **MLPP indication turned on** in the **MLPP Indication Status** field.

Step 7 (Optional) In the **IPv6** section, set the **Enable IPv6** field to **True**.

Step 8 (Optional) In the **Cisco Syslog Agent** section, enter the name or IP address of the remote Syslog server in the **Remote Syslog Server Name 1** field. If a server name is not specified, Cisco Unified Serviceability does not send the Syslog messages.

Step 9 (Optional) In the **Call Trace Log Configuration for Session Trace** section, set up the call trace log to allow the collection of SIP call information for session traces.

The Session Trace feature in the Real-Time Monitoring Tool (RTMT) uses this information to generate call flow diagrams that are useful for troubleshooting.

a) Set the **Enable Call Trace Log** field to **True**.
b) Enter the maximum number of SIP call trace log files that Unified Communications Manager can generate in the **Max Number of Call Trace Log Files** field.

   The default value is 2000. Valid range is from 5 to 4000.

c) Enter the maximum file size, in megabytes, of the SIP call trace log files in the **Call Trace Log** field.

   The default value is 2. Valid range is from 1 to 10.

Note Some performance degradation can occur during periods of high SIP call traffic. To reduce the impact on system performance, set the Cisco CallManager service parameter called **Log Call-Related REFER/NOTIFY/SUBSCRIBE SIP Messages for Session Trace** to False. This will omit the REFER, NOTIFY, and SUBSCRIBE messages from the SIP call tracing.

Step 10 In the in the **CCMAdmin Parameters** section, select **True** in the **Enable Dependency Records** field.

Step 11 Click **Save**.

Step 12 Click **Reset**, and then click **OK** to reset all devices.

We recommend that you reset all devices during off-peak hours.

Tip To reset all devices, you can reset every device pool in the system.

Common Enterprise Parameters

The following table lists common enterprise parameters that are used to set enterprise settings such as Organization Top-Level Domain or Cluster Fully Qualified Domain Name. For a detailed list, use the **System** > **Enterprise Parameters** menu in Cisco Unified CM Administration.

Table 2: Common Enterprise Parameters for an Initial Unified Communications Manager Setup

Parameter Name	Description
Enterprise Parameters	
Connection Monitor Duration	If an IP phone in the cluster registers on a secondary node, use this parameter to set the amount of time that the IP phone waits before it falls back and re-registers with the primary node after the primary node becomes available. This parameter affects all secure devices for a specific Secure Survivable Remote Site Telephony (SRST) router. For more information, see *Security Guide for Cisco Unified Communications Manager*. Default: 120 seconds Restart all services for the changes to take effect.
CCMAdmin Parameters	
Enable Dependency Records	This parameter is used to display dependency records that are required for troubleshooting. Displaying the dependency records may be beneficial during an initial system setup. Displaying the dependency records could lead to high CPU usage spikes and could impact call processing. To avoid possible performance issues, disable this parameter after the system setup is complete. We recommend displaying dependency records only during off-peak hours or during a maintenance window. When enabled, you can select **Dependency Records** from the **Related Links** drop-down list, which is accessible from most configuration windows using Unified Communications Manager. Default: False
User Data Service Parameters	

Parameter Name	Description
Enable All User Search	This parameter allows you to search the corporate directory for all users when no last name, first name, or directory number is specified. This parameter also applies to directory searches on the **Cisco CallManager Self Care** (CCMUser) window. Default: True
Clusterwide Domain Configuration	
Organization Top Level Domain	This parameter defines the top-level domain for the organization. For example, cisco.com. Maximum length: 255 characters Allowed values: A valid domain using upper and lowercase letters, numbers (0-9), hyphens, and dots (as a domain label separator). Domain labels must not start with a hyphen. The last label must not start with a number. For example, this domain is invalid -cisco.1om.
Cluster Fully Qualified Domain Name	This parameter defines one or more Fully Qualified Domain Names (FQDN) for the cluster. Multiple FQDNs must be separated by a space. Specify wildcards within an FQDN using an asterisk (*). Example: `cluster-1.cisco.com *.cisco.com`. Requests containing URLs, such as SIP calls, that have a host portion that matches any of the FQDNs in this parameter are routed to that cluster and the attached devices. Maximum length: 255 characters Allowed values: An FQDN or a partial FQDN using the * wildcard. Upper and lowercase letters, numbers (0-9), hyphens, and dots (as a domain label separator). Domain labels must not start with a hyphen. The last label must not start with a number. For example, this domain is invalid -cisco.1om.
IPv6	

Parameter Name	Description
Enable IPv6	This parameter determines whether Unified Communications Manager can negotiate Internet Protocol Version 6 (IPv6) and whether phones are allowed to advertise IPv6 capability. IPv6 must be enabled on all other network components including on the platform of all nodes before you enable this parameter. Otherwise, the system continues to run in IPv4-only mode. This is a required field. Default: False (IPv6 is disabled) You must restart the following services for the IPv6 parameter change to take effect, and the affected services in the IM and Presence Service cluster. • Cisco CallManager • Cisco IP Voice Media Streaming App • Cisco CTIManager • Cisco Certificate Authority Proxy Function
Cisco Syslog Agent	
Remote Syslog Server Name 1	Enter the name or IP address of the remote Syslog server. Cisco Unified Serviceability do not send the Syslog messages if a server name is not specified. This parameter is required only if you are using the Syslog server for logs. Maximum length: 255 characters Allowed values: A valid remote Sylog server name using upper and lowercase letters, numbers (0-9), hyphens, and dots. Do not specify another Unified Communications Manager node as the destination.
Cisco Jabber	
Never Start Call with Video	This parameter determines if video is sent when a video call starts. Select **True** to start video calls without immediately sending video. Anytime during the video call, you can choose to start sending your video. This parameter overrides any IM and Presence Service preferences. When set to False, video calls start according to the preferences set in IM and Presence Service. Default: False.
SSO and OAuth Configuration	

Parameter Name	Description
SSO Login Behavior for iOS	This parameter is required to allow Cisco Jabber to perform the certificate-based authentication with the IdP in a controlled mobile device management (MDM) deployment. The **SSO Login Behavior for iOS** parameter includes the following options: • **Use Embedded Browser**—If you enable this option, Cisco Jabber uses the embedded browser for the SSO authentication. Use this option to allow iOS devices prior to version 9 to use SSO without cross-launching into the native Apple Safari browser. • **Use Native Browser**—If you enable this option, Cisco Jabber uses the Apple Safari framework on an iOS device to perform the certificate-based authentication with an Identity Provider (IdP) in the MDM deployment. **Note** We do not recommend configuring this option, except in a controlled MDM deployment, because using a native browser is not as secure as the using the embedded browser. This is a required field. Default: Use the embedded browser (WebView).
OAuth with Refresh Login Flow	This parameter controls the login flow used by clients such as Cisco Jabber when connecting to Unified Communications Managers. • Enabled—If you enable this option, clients can use an oAuth-based Fast Login flow to provide a quicker and streamlined login experience, without requiring the user input to re-log in. For example, due to a network change. The option requires support from the other components of the Unified Communications solution, such as Expressway and Unity Connection (compatible versions with the refresh login flow enabled). • Disabled—If you enable this option, the existing behavior is preserved and is compatible with older versions of other system components. **Note** For Mobile and Remote Access deployment with Cisco Jabber, we recommend enabling this parameter only with a compatible version of Expressway that supports oAuth with Refresh login flow. Incompatible version may impact the Cisco Jabber functionality. Please refer the specific product documents for supported version and configuration requirements. This is a required field. Default: Disabled.

Parameter Name	Description
Use SSO for RTMT	This parameter is configured to enable SAML SSO for Real-Time Monitoring Tool (RTMT). The **Use SSO for RTMT** parameter includes the following options: • **True**—If you choose this option, RTMT displays the SAML SSO-based IdP sign-in window. **Note** When you perform a fresh install, the default value of the **Use SSO for RTMT** parameter appears as **True**. • **False**—If you choose this option, RTMT displays the basic authentication sign-in window. **Note** When you perform an upgrade from a Cisco Unified Communications Manager version where **Use SSO for RTMT** parameter does not exist, the default value of this parameter in the newer version appears as **False**. This is a required field. Default: True.

Configure SSO Login Behavior for Cisco Jabber on iOS

Procedure

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

Step 2 To configure the opt-in control, in the SSO Configuration section, choose the **Use Native Browser** option for the **SSO Login Behavior for iOS** parameter:

Note The **SSO Login Behavior for iOS** parameter includes the following options:

- **Use Embedded Browser**—If you enable this option, Cisco Jabber uses the embedded browser for SSO authentication. Use this option to allow iOS devices prior to version 9 to use SSO without cross-launching into the native Apple Safari browser. This option is enabled by default.
- **Use Native Browser**—If you enable this option, Cisco Jabber uses the Apple Safari framework on an iOS device to perform certificate-based authentication with an Identity Provider (IdP) in the MDM deployment.

  Note We don't recommend to configure this option, except in a controlled MDM deployment, because using a native browser is not as secure as the using the embedded browser.

Step 3 Click **Save**.

Configure SSO for RTMT

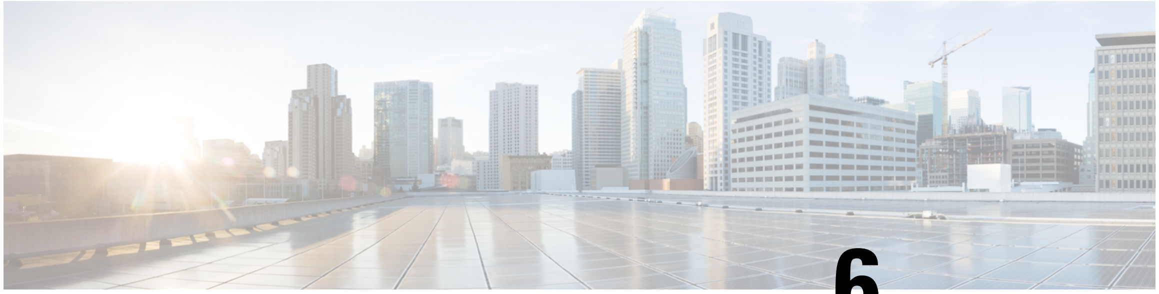
Procedure

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

Step 2 To configure SSO for RTMT, in the SSO Configuration section, choose **True** for the **Use SSO for RTMT** parameter:

> **Note** The **Use SSO for RTMT** parameter includes the following options:
>
> - **True**—If you choose this option, RTMT displays the SAML SSO-based IdP sign-in window.
>
>   **Note** When you perform a fresh install, the default value of the **Use SSO for RTMT** parameter appears as **True**.
>
> - **False**—If you choose this option, RTMT displays the basic authentication sign-in window.
>
>   **Note** When you perform an upgrade from a Cisco Unified Communications Manager version where **Use SSO for RTMT** parameter does not exist, the default value of this parameter in the newer version appears as **False**.

Step 3 Click **Save**.



CHAPTER 6

Configure Service Parameters

Service Parameters Overview

Service parameters let you configure different services on selected Unified Communications Manager servers. Unlike enterprise parameters, which apply to all services, each service gets configured with a separate set of service parameters.

Service parameters let you configure settings for the following two types of services, both of which can be activated within Cisco Unified Serviceability:

- **Feature Services** - These services are used to run certain system features. You must turn feature services on in order to use them.
- **Network Services** - Network services are on by default, but you can stop and start (or restart) a network service for troubleshooting purposes. These services includes services that allow system components like the database and platform to function properly.

You can view service parameter field descriptions for service parameters by by clicking the ? icon within the **Service Parameter Configuration** window, or by clicking on one of the parameter names.

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

Service Parameters Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Activate Essential Services, on page 36	You can activate and deactivate services on the node using Cisco Unified Serviceability. For a

	Command or Action	Purpose
		list of the recommended services for publisher nodes, see Recommended Services for Publisher Nodes, on page 36. For a list of the recommended services for subscriber nodes, see Recommended Services for Subscriber Nodes, on page 38.
Step 2	Configure Service Parameters, on page 39	Configure service parameters for the Cisco Unified Communications Manager publisher node and for subscriber nodes in the cluster.
Step 3	View Clusterwide Service Parameter Settings , on page 39	You can display the services for your nodes using Cisco Unified Communications Manager Administration and Cisco Unified Serviceability. To view service parameter settings and parameter descriptions, use Cisco Unified Communications Manager Administration.

Activate Essential Services

Use this procedure to activate services across the cluster.

For a list of recommended services for publisher nodes and subscriber nodes, see the following topics:

- Recommended Services for Publisher Nodes, on page 36
- Recommended Services for Subscriber Nodes, on page 38

Procedure

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

Step 2 Select a **Server** from the drop-down menu and click **Go**.

The services and their current status display.

Step 3 Activate and deactivate the services that you want:

- To activate a service, check the check box beside the service that you want to activate.
- To deactivate a service, uncheck the check box beside the service that you want to deactivate.

Step 4 Click **Save**.
Service activation may take a few minutes to complete. refresh the page to confirm the status change.

Recommended Services for Publisher Nodes

The following table lists recommended services for a Unified Communications Manager publisher node when using a non-dedicated TFTP server.

Table 3: Recommended Publisher Node Services for Non-Dedicated TFTP Server Deployments

Type	Service Name
CM Services	Cisco CallManager
	Cisco Unified Mobile Voice Access Services
	Cisco IP Voice Media Streaming App
	Cisco CTIManager
	Cisco Extended Functions
	Cisco Intercluster Lookup Service
	Cisco Location Bandwidth Manager
	Cisco TFTP
CTI Services	Cisco IP Manager Assistant
	Cisco WebDialer Web Service
CDR Services	Cisco SOAP - CDRonDemand Service
	Cisco CAR Web Service
Database and Admin Services	Cisco Bulk Provisioning Service
	AXL Web Service
	Cisco URL Web Service
Performance and Monitoring Services	Cisco Serviceability Reporter
Security Services	Cisco Certificate Authority Proxy Function (CAPF)
Directory Services	Cisco DirSync Cisco Certificate Authority Proxy Function

Tip You can safely disable the following services if you do not plan to use them:

- Cisco Messaging Interface
- Cisco DHCP Monitor Service
- Cisco TAPS Service
- Cisco Directory Number Alias Sync
- Cisco Directory Number Alias SyncCisco Dialed Number Analyzer Server
- Cisco Dialed Number Analyzer
- Self Provisioning IVR

Recommended Services for Subscriber Nodes

The following table lists recommended services for a Unified Communications Manager subscriber node when using a non-dedicated TFTP server.

Tip You can safely disable the other services if you don't plan to use them.

Table 4: Recommended Subscriber Node Services for Non-Dedicated TFTP Server Deployments

Type	Service Name
CM Services	Cisco CallManager
	Cisco IP Voice Media Streaming App
	Cisco CTIManager
	Cisco Extension Mobility
	Cisco Extended Functions
	Cisco TFTP

You must activate the following services on each IM and Presence Service node in your cluster.

- Cisco SIP Proxy
- Cisco Presence Engine
- Cisco XCP Connection Manager
- Cisco XCP Authentication Service

Configure Service Parameters

You can configure the service parameters on the node using Cisco Unified Communications Manager Administration. Service parameters that are marked as cluster-wide affect all nodes in the cluster.

⚠ **Caution** Some changes to service parameters can cause system failure. We recommend 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.

Before you begin

- Make sure that the Unified Communications Manager nodes are configured.
- Make sure that the service is active. For details, see Activate Essential Services, on page 36.

Procedure

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

Step 2 Select a node in the **Server** drop-down list.

Step 3 Select a service in the **Service** drop-down list.

Tip Click the **?** icon in the **Service Parameter Configuration** window to view a list of service parameters along with their descriptions.

Step 4 Click **Advanced** to view the full list of parameters.

Step 5 Modify the service parameters and then click **Save**.

The window refreshes and the service parameter values are updated.

You can click the **Set to Default** button to update all parameters to the suggested value that appears after the **Parameter Value** field. If a parameter does not have a suggested value, the service parameter value does not change when you click the **Set to Default** button.

View Clusterwide Service Parameter Settings

You can use Cisco Unified Communications Manager Assistant and Cisco Unified Serviceability to view the status of services for nodes in your cluster. To view service parameter settings and parameter descriptions, use Cisco Unified Communications Manager Assistant.

Procedure

Step 1 To display services and view service parameter settings for a node using Cisco Unified Communications Manager Assistant, perform the following steps.

a) Select **System** > **Service Parameters**.
b) In the **Service Parameters Configuration** window, select a node in the **Server** drop-down box.

c) Select a service in the **Service** drop-down box.

All parameters that apply to the selected node appear. Parameters that appear in the **Clusterwide Parameters (General)** section apply to all nodes in the cluster.

d) Click the (**?**) icon in the **Service Parameter Configuration** window to view a list of service parameters along with their descriptions.

Step 2 To display the service parameters for a particular service on all nodes in a cluster, select **Parameters for All Servers** in the **Related Links** drop-down box in the **Service Parameters Configuration** window, then click **Go**.

The **Parameters for All Servers** window appears. You can click on a server name that is listed or on a parameter value to open the related **Service Parameter Configuration** window.

Step 3 To display out-of-sync service parameters for a particular service on all nodes in a cluster, select **Out of Sync Parameters for All Servers** in the **Related Links** drop-down box in the **Parameters for All Servers** window, then click **Go**.

The **Out of Sync Parameters for All Servers** window appears. You can click on a server name that is listed or on a parameter value to open the related **Service Parameter Configuration** window.

CHAPTER 7

Configure Core Settings for Device Pools

Device Pools Overview

Device pools provide a common set of configurations for a group of devices. You can assign a device pool to devices such as phones, gateways, trunks and CTI route points. After you create a device pool, you can associate devices so that they inherit the device pool settings, rather than configuring each device individually.

Device pools let you configure devices according to their location, by assigning location-related information such as Date/Time Groups, Regions, and Phone NTP References. You can create as many device pools as you need, typically one per location. However, you can also apply device pools to apply configurations according to a job function (for example, if your company has a call center, you may want to assign call center phones to one device pool and administration office phones to another).

This section covers the steps that are required to set up core settings for device pools, such as:

- Network Time Protocol—Configure Phone NTP References to provide NTP support for SIP devices in the device pool.
- Regions—Manage bandwidth and supported audio codecs for calls to and from certain regions.
- Cisco Unified Communications Manager Groups—Configure call processing redundancy and distributed call processing for your devices.

Network Time Protocol Overview

The Network Time Protocol (NTP) allows network devices such as SIP phones to synchronize their clocks to a network time server or network-capable clock. NTP is critical for ensuring that all network devices have the same time and that the timestamps in audit logs match the network time. Features such as billing and call detail records rely on accurate timestamps across the network. In addition, system administrators need accurate timestamps in audit logs for troubleshooting. This allows them to compare audit logs from different systems and create a reliable timeline and sequence of events for whatever issue they are facing.

During installation, you must set up an NTP server for the Unified Communications Manager publisher node. The subscriber nodes then sync their time from the publisher node.

You can assign up to five NTP servers.

Phone NTP References

- **For SIP Phones**: It is mandatory that you configure Phone NTP References and assign them through the device pool. These references direct the SIP phone to an appropriate NTP server that can provide the network time. If a SIP phone cannot get its date/time from the provisioned “Phone NTP Reference” the phone receives this information when it registers with Unified Communications Manager.
- **For SCCP Phones**: Phone NTP References are not required as SCCP phones obtain their network time from Unified Communications Manager directly through SCCP signaling.

Authenticated NTP

To provide more network security to the NTP portion of your network, you can configure authenticated NTP. If you choose this option, the devices in your network use a symmetric key to encrypt and authenticate NTP messages. This feature is suported as of Release 11.5(1)SU3.

Authenticated NTP is configured on the Cisco Unified Communications Manager publisher node. The subscriber nodes and IM and Presence nodes sync the time from the Unified CM publisher node.

Regions Overview

Regions provide capacity controls for Unified Communications Manager multi-site deployments where you may need to limit the bandwidth for certain calls. For example, you can use regions to limit the bandwidth for calls that are sent across a WAN link, while maintaining a higher bandwidth for internal calls. You can use regions to limit the bandwidth for audio and video calls by setting the maximum bitrate for intraregional or interregional calls to whatever the region(s) can provide.

Additionally, the system uses regions to set the audio codec priority where you have applications that support specific codecs only. You can configure a prioritized list of supported audio codecs and apply it to calls to and from specific regions.

When you configure the maximum audio bit rate setting in the **Region Configuration** window (or use the service parameter in the **Service Parameter Configuration** window), this setting serves as a filter. When an audio codec is selected for a call, Unified Communications Manager takes the matching codecs from both sides of a call leg, filters out the codecs that exceed the configured maximum audio bit rate, and then picks the preferred codec among the codecs that are remaining in the list.

Unified Communications Manager supports up to 2000 regions.

Supported Audio Codecs

Unified Communications Manager supports video stream encryption and the following audio codecs:

Audio Codec	Description
G.711	The most commonly supported codec, used over the public switched telephone network.

Audio Codec	Description
G.722	Wideband codec often used in video conferences. This is always preferred by Unified Communications Manager over G.711, unless G.722 is disabled.
G.722.1	Low complexity wideband codec operating at 24 and 32 kb/s. The audio quality approaches that of G.722 while using, at most, half the bit rate.
G.728	Low bit rate codec that video endpoints support.
G.729	Low bit rate codec with 8 kb/s compression that is supported by Cisco IP Phone 7900, and typically used for calls across a WAN link.
GSM	The global system for mobile communications (GSM) codec. GSM enables the MNET system for GSM wireless handsets to operate with Unified Communications Manager.
L16	Advanced Audio Coding-Low Delay (AAC-LD) is a super-wideband audio codec that provides superior sound quality for voice and music. This codec provides equal or improved sound quality over older codecs, even at lower bit rates.
AAC-LD (mpeg4-generic)	Supported for SIP devices, in particular, Cisco TelePresence systems.
AAC-LD (MP4A-LATM)	Low-overhead MPEG-4 Audio Transport Multiplex (LATM) is a super-wideband audio codec that provides superior sound. Supported for SIP devices including Tandberg and some third-party endpoints. **Note** AAC-LD (mpeg4-generic) and AAC-LD (MPA4-LATM) are not compatible.
Internet Speech Audio Codec (iSAC)	An adaptive wideband audio codec, specially designed to deliver wideband sound quality with low delay in both low and medium bit rate applications.
Internet Low Bit Rate Codec (iLBC)	Provides audio quality between G.711 and G.729 at bit rates of 15.2 and 13.3 kb/s while allowing for graceful speech quality degradation in a lossy network due to independently encoded speech frames. iLBC is supported for SIP, SCCP, H323, and MGCP devices. **Note** H.323 Outbound FastStart does not support the iLBC codec.
Adaptive Multi-Rate (AMR)	The required standard codec for 2.5G/3G wireless networks based on GSM (WDMA, EDGE, GPRS). This codec encodes narrowband (200-3400 Hz) signals at variable bit rates ranging from 4.75 to 12.2 kb/s with toll quality speech starting at 7.4 kb/s. AMR is supported only for SIP devices.
Adaptive Multi-Rate Wideband (AMR-WB)	Codified as G.722.2, an ITU-T standard speech codec formally known as Wideband, codes speech at about 16 kb/s. This codec is preferred over other narrowband speech codecs such as AMR and G.711 because it provides better speech quality due to a wider speech bandwidth of 50 Hz to 7000 Hz. AMR-WB is supported only for SIP devices.

Audio Codec	Description
Opus	Opus codec is an interactive speech and audio codec, specially designed to handle a wide range of interactive audio applications such as voice over IP, video conferencing, in-game chat, and live distributed music performance. This codec scales from narrowband low bit rate to a very high quality bit rate ranging from 6 to 510 kb/s. Opus codec support is enabled by default for all SIP devices. You can reconfigure Opus support via the **Opus Codec Enabled** service parameter (the default setting is **Enabled for All Devices**). You can reconfigure this parameter to disable Opus codec support, or to enable support in non-recording devices only. **Note** Opus has a dependency on the G.722 codec. The **Advertise G.722 Codec** enterprise parameter should also be set to **Enabled** for SIP devices to use Opus.

Cisco Unified CM Groups Overview

A Unified Communications Manager Group is a prioritized list of up to three redundant servers to which devices can register. Each group contains a primary node and up to two backup nodes. The order in which you list the nodes determines their priority with the first node being the primary node, the second being the backup node, and the third being the tertiary node. You can assign a device to a Cisco Unified Communictions Manager Group via the **Device Pool Configuration**.

Unified Communications Manager groups provide two important features for your system:

- Call processing redundancy—When a device registers, it attempts to connect to the primary (first) Unified Communications Manager in the group that is assigned to its device pool. If the primary Unified Communications Manager is not available, the device tries to connect to the first backup node and if that node is unavailable, it tries to connect to the tertiary node. Each device pool has one Unified Communications Manager group that is assigned to it.
- Distributed call processing—You can create multiple device pools and Unified Communications Manager groups to distribute device registrations evenly across multiple Unified Communications Managers.

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

Call Processing Redundancy

Unified Communications Manager groups provide call preccsing redundancy and recovery:

- Failover—Occurs when the primary Unified Communications Manager in a group fails, and the devices reregister with the backup Unified Communications Manager in that group.
- Fallback—Occurs when a failed primary Unified Communications Manager comes back into service, and the devices in that group reregister with the primary Unified Communications Manager.

Under normal operation, the primary Unified Communications Manager in a group controls call processing for all the registered devices (such as phones and gateways) that are associated with that group.

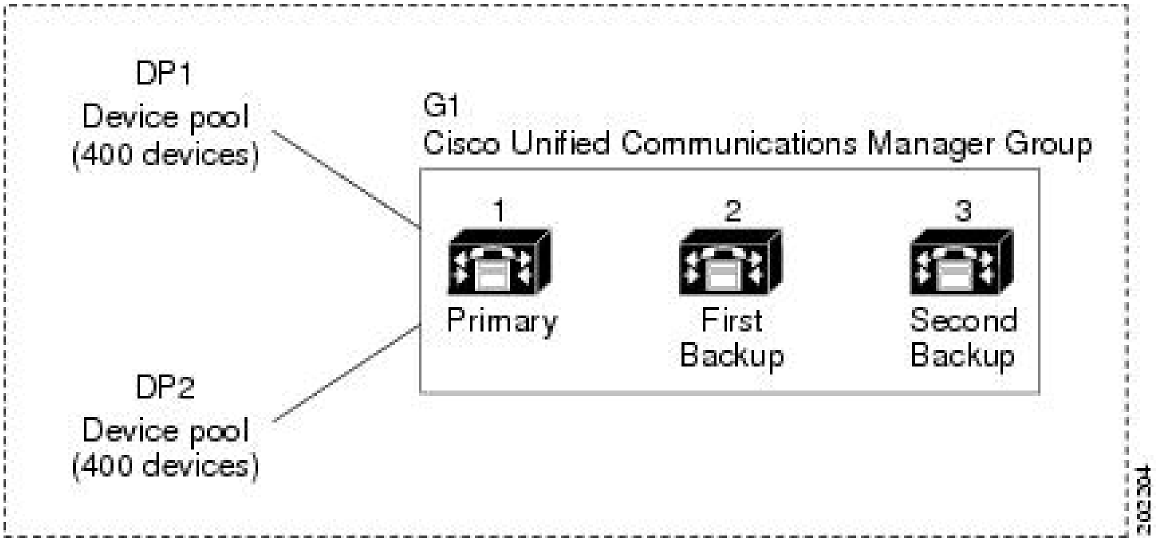
If the primary Unified Communications Manager fails for any reason, the first backup Unified Communications Manager in the group takes control of the devices that were registered with the primary Unified Communications Manager. If you specify a second backup Unified Communications Manager for the group, it takes control of the devices if both the primary and the first backup Unified Communications Managers fail.

When a failed primary Unified Communications Manager comes back into service, it takes control of the group again, and the devices in that group automatically reregister with the primary Unified Communications Manager.

Example

For example, the following figure shows a simple system with three Unified Communications Managers in a single group that is controlling 800 devices.

Figure 1: Unified Communications Manager Group



The figure depicts Unified Communications Manager group G1 that is assigned with two device pools, DP1 and DP2. Unified Communications Manager 1, as the primary Unified Communications Manager in group G1, controls all 800 devices in DP1 and DP2 under normal operation. If Unified Communications Manager 1 fails, control of all 800 devices transfers to Unified Communications Manager 2. If Unified Communications Manager 2 also fails, control of all 800 devices transfers to Unified Communications Manager 3.

The configuration provides call-processing redundancy, but it does not distribute the call-processing load very well among the three Unified Communications Managers in the example. Refer to the following topic for information on how to use Unified Communications Manager groups and device pools to provide distributed call processing within the cluster.

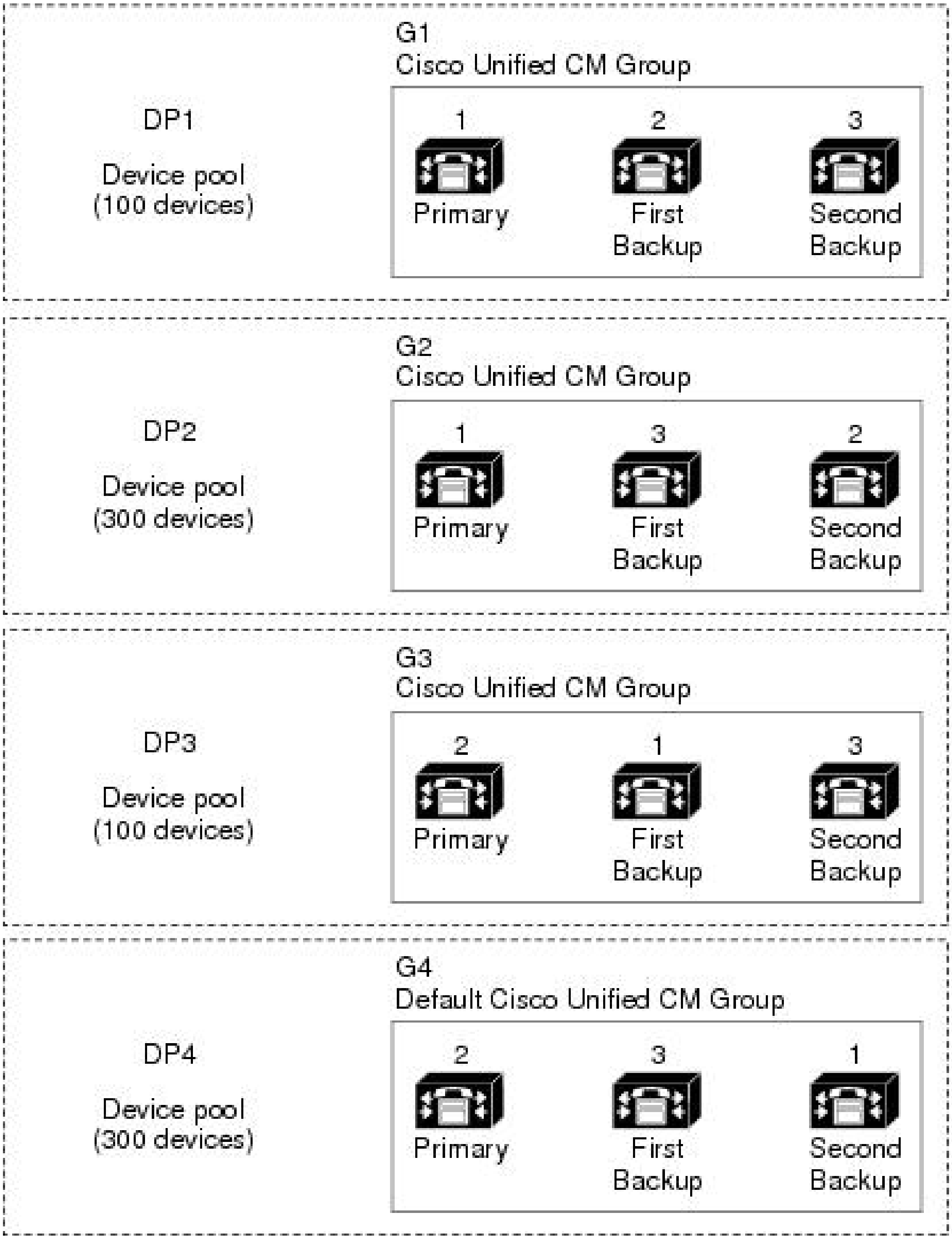
Note Empty Unified Communications Manager groups will not function.

Distributed Call Processing

Unified Communications Manager groups provide both call-processing redundancy and distributed call processing. How you distribute devices, device pools, and Unified Communications Managers among the groups determines the level of redundancy and load balancing in your system.

In most cases, you would want to distribute the devices in a way that prevents the other Unified Communications Managers from becoming overloaded if one Unified Communications Manager in the group fails. The following figure shows one possible way to configure the Unified Communications Manager groups and device pools to achieve both distributed call processing and redundancy for a system of three Unified Communications Managers and 800 devices.

Figure 2: Redundancy Combined with Distributed Call Processing



The previous figure depicts the Unified Communications Manager groups as they are configured and assigned to device pools, so Unified Communications Manager 1 serves as the primary controller in two groups, G1 and G2. If Unified Communications Manager 1 fails, the 100 devices in device pool DP1 reregister with

Unified Communications Manager 2, and the 300 devices in DP2 reregister with Unified Communications Manager 3. Similarly, Unified Communications Manager 2 serves as the primary controller of groups G3 and G4. If Unified Communications Manager 2 fails, the 100 devices in DP3 reregister with Unified Communications Manager 1, and the 300 devices in DP4 reregister with Unified Communications Manager 3. If Unified Communications Manager 1 and Unified Communications Manager 2 both fail, all devices reregister with Unified Communications Manager 3.

Device Pool Prerequisites

Make sure to properly plan out your device pools before you configure them. When configuring device pools and redundant Unified Communications Manager Groups, you will want to provide server redundancy for phones while distributing registrations evenly across your cluster. For additional information that you can use to plan your system, refer to the *Cisco Collaboration System Solution Reference Network Design* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html.

To ensure that Unified Communications Manager includes the latest time zone information, you can install a Cisco Options Package (COP) file that updates the time zone information after you install Unified Communications Manager. After major time zone change events, we will contact you to let you know that you can download the latest COP file at https://software.cisco.com/download/navigator.html.

Change the settings for CMLocal to your local date and time.

Additional Device Pool Configurations

This chapter focuses on core settings such as phone NTP references, regions and call processing redundancy via Unified Communications Manager Groups. However, you can also apply these optional features and components to devices via the device pool configuration:

- Media Resources—Assign media resources such as conference bridges, and music on hold to the devices in your device pool. Refer to the "Configure Media Resources" section of this book for details on configuring media resources. See Media Resources Configuration Task Flow, on page 467.
- Survivable Remote Site Telephony (SRST)—If your deployment uses WAN connections, configure SRST so that in the event of a WAN outage, IP gateways can provide limited call support. See Survivable Remote Site Telephony Configuration Task Flow, on page 106.
- Call Routing Information—For information on how to route calls between clusters, see Call Routing Configuration Task Flow, on page 128.
- Device Mobility—Configure Device Mobility groups to allow devices to assume the settings based on their physical location. For details, see the "Configure Device Mobility" chapter in the *Feature Configuration Guide for Cisco Unified Communications Manager*.

Core Settings for Device Pools Configuration Task Flow

Complete these tasks to set up device pools and apply settings such as Regions, Phone NTP references, and redundancy for the devices that use those device pools.

Procedure

	Command or Action	Purpose
Step 1	Configure the Network Time Protocol, on page 49	Complete the tasks in this task flow to set up NTP on your system. Configure Phone NTP references and apply them to a Date/Time Group that you can assign to a device pool.
Step 2	Configure Region Relationships, on page 54	Complete these tasks to set up Regions for your system. You can create up to 2000 regions and configure customized settings, such as customized audio codec preferences and bitrate restrictions based on what the region can provide.
Step 3	Configure Cisco Unified CM Groups, on page 55	Configure Unified Communications Manager groups for call processing redundancy and load balancing.
Step 4	Configure Device Pools, on page 56	Set up device pools for your system devices. Apply the other core settings that you configured to the device pools in order to apply those settings to the devices that use this device pool.

Configure the Network Time Protocol

Complete these tasks to configure the Network Time Protocol (NTP) for your system. Configure Phone NTP References and apply them to a Date/Time Group which you can then apply to a device pool.

Procedure

	Command or Action	Purpose
Step 1	Add an NTP Server, on page 50	Optional. Use this procedure if you need to add an NTP server. You can add up to five NTP servers. **Note** During system installation, you were required to point Unified Communications Manager to an NTP server. You can use this procedure if you want to add additional NTP servers. Otherwise, you can skip this task.
Step 2	Configure NTP Authentication via Symmetric Key, on page 50	Optional. Configure authenticated NTP via a symmetric key to further enhance system security.

	Command or Action	Purpose
Step 3	Configure Phone NTP References, on page 51	For SIP phones, it's mandatory that you configure phone NTP references and then apply them via a Date/Time Group and Device Pool.
Step 4	Add a Date/Time Group, on page 52	Define time zones for the various devices that are connected to your system and assign the Phone NTP references that you've set up to the appropriate Date/Time Group.

Note For additional information on CLI commands that you can use to troubleshoot and configure NTP such as the `utils ntp*` set of commands, refer to the *Command Line Interface Reference Guide* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Add an NTP Server

Add an NTP Server to Unified Communications Manager.

Note You can also add an NTP Server in the NTP Server Configuration window of the Cisco Unified OS Administration winodw at **Settings** > **NTP Servers**.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 To confirm that the publisher node can reach the NTP server, run the **utils network ping <ip_address>** where the ip_address represents the address of the NTP server.

Step 3 If the server is reachable, run the `utils ntp server add <ip_address>` to add the server.

Step 4 Restart the NTP service with the `utils ntp restart` command.

Configure NTP Authentication via Symmetric Key

Use this procedure to authenticate NTP messages in your network using a symmetric key.

Note Ensure that you enter the SHA1 Key character by character. Currently, the CLI framework doesn't read the pasted value.

Procedure

Step 1 Log in to the Command Line Interface on the Cisco Unified Communications Manager publisher node.

Step 2 Run the `utils ntp auth symmetric-key status` command to verify the status of the current NTP authentication setting.

Step 3 Do either of the following:

- To enable NTP authentication with a symmetric key, run the `utils ntp auth symmetric-key enable` CLI command.
- To disable NTP authentication with a symmetric key, run the `utils ntp auth symmetric-key disable` CLI command.

Step 4 Follow the prompts to enter the key ID and symmetric key of the NTP server.

Configure Phone NTP References

Use this procedure to configure Phone NTP References, which are mandatory for SIP phones. You can assign the NTP references that you create to a device pool via the Date/Time Group. The reference points the SIP phone to an appropriate NTP server that can provide the network time. For SCCP phones, this configuration is not required.

Note Unified Communications Manager does not support the multicast and anycast modes. If you choose either of these modes, your system defaults to the directed broadcast mode.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Phone NTP Reference**.

Step 2 Click **Add New**.

Step 3 Enter the NTP server's **IPv4 Address** or **IPv6 Address**, depending on which addressing system your phones use.

Note It is mandatory to enter either IPv4 address or IPv6 address to save the Phone NTP References. If you are deploying both IPv4 phones and IPv6 phones, then provide both the IPv4 address and the IPv6 address for the NTP server.

Step 4 In the **Description** field, enter a description for the phone NTP reference.

Step 5 From the **Mode** drop-down list, choose the mode for the phone NTP reference from the following list of options:

- **Unicast**—If you choose this mode, the phone sends an NTP query packet to that particular NTP server.
- **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.

Note Cisco TelePresence and Cisco Spark device types support Unicast mode only.

Step 6 Click **Save**.

What to do next

Assign the Phone NTP Reference(s) to a Date/Time Group. For details, see Add a Date/Time Group, on page 52

Add a Date/Time Group

Configure Date/Time Groups to define time zones in your system. Assign the Phone NTP references that you configured to the appropriate group. 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 all devices in that device pool.

You must reset devices to apply any changes that you make.

Tip For a worldwide distribution of Cisco IP Phones, create a date/time group for each time zones.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Date/Time Group**.

Step 2 Click **Add New**.

Step 3 Assign NTP References to this group:

a) Click **Add Phone NTP References**.
b) In the **Find and List Phone NTP References** popup, click **Find** and select the phone NTP reference(s) that you configured in the previous task.
c) Click **Add Selected**.
d) If you added multiple references, use the up and down arrows to changed the prioritized order. The references at the top have the higher priority.

Step 4 Configure the remaining fields in the **Date/Time Group Configuration** window. See the online help for more information about the fields and their configuration options.

Step 5 Click **Save**.

Configure Regions

Complete the following tasks to configure regions for your device pools. Configure relationships between regions to better manage bandwidth. You can use Regions to control the maximum bit rates for certain types of calls (for example, video calls) and to prioritize specific audio codecs.

Procedure

	Command or Action	Purpose
Step 1	Customize Audio Codec Preferences, on page 53	Optional. Use this procedure if you want to customize priorities for your audio codecs. You

	Command or Action	Purpose
		may want to do this in order to prioritize specific audio codecs ahead of other codecs. Otherwise, you can assign one of the default audio codec lists to your device pools.
Step 2	Configure Clusterwide Defaults for Regions, on page 54	Configure the clusterwide defaults for Regions. All Regions will use these default settings unless you configure otherwise within the Region Configuration.
Step 3	Configure Region Relationships, on page 54	Set up new regions or edit settings for existing regions. Configure relationships for both interregional and intraregional calls.

Customize Audio Codec Preferences

Use this procedure to customize priorities for your audio codecs. Create a new audio codec preferences list by copying settings from an existing list, and then editing the order of priority within your new list.

Note If you don't need to customize audio codec priorities, you can skip this task. When you configure your device pools, you can assign one of the default audio codec preference lists.

Procedure

Step 1 From Cisco Unified CM Administration choose **System** > **Region Information** > **Audio Codec Preference List**.

Step 2 Click **Add New**.

Step 3 From the **Audio Codec Preference Lists** drop-down list box, select one of the existing audio codec preference lists.
The prioritized list of audio codecs displays for the list that you selected.

Step 4 Click **Copy**. The prioritized list of codecs from the copied list is applied to a newly created list.

Step 5 Edit the **Name** for your new audio codec list. For example, `customizedCodecList`.

Step 6 Edit the **Description**.

Step 7 Use the up and down arrows to move codecs in the prioritized order that appears in the **Codecs in List** list box.

Step 8 Click **Save**.

You must apply the new list to a region and then apply that region to a device pool. All devices in the device pool will use this audio codec preference list.

Configure Clusterwide Defaults for Regions

Use this procedure to configure default settings clusterwide for Regions. These settings apply by default to calls to and from all regions unless you configure region relationships for individual regions within the **Region Configuration** window.

Procedure

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

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

Step 3 From the **Service** drop-down list, select the **Cisco CallManager** service.
The **Service Parameter Configuration** window displays.

Step 4 Under **Clusterwide Parameters (System - Location and Region)**, configure any new service parameter settings that you want. For service parameter descriptions, click any of the parameter names to view the help description.

Step 5 Click **Save**.

Configure Region Relationships

Use this procedure to create Regions and to assign custom settings for calls between specific regions. You can edit settings such as preffered audio codecs and maximum bitrates. For example, if you have a region with lower bandwidth capacities than the rest of the network, you may want to edit the maximum session bit rate for video calls to and from the region. You could reset this value to whatever that region can provide.

Note For enhanced scalability, and to ensure that the system uses fewer resources, we recommend that you use the default values from the **Service Parameters Configuration** window wherever possible.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Region Information** > **Regions**.

Step 2 Do either of the following:

- Click **Find** and select a region.
- Click **Add New** ro create a new region.
- Enter a **Name** for the Region. For example, `NewYork`.
- Click **Save**.

The read-only **Region Relationships** area displays any customized settings that you've set up between the selected region and another region.

Step 3 To modify the settings between this region and another region (or the same region for intraregional calls), edit the settings in the **Modify Relationships to other Regions** area:

a) In the **Regions** area, highlight the other region (for intraregional calls, highlight the same region that you are configuring).

b) Edit the settings in the adjacent fields. For help with the fields and their settings, see the online help.

c) Click **Save**.
The new settings now display as a custom rule in the **Region Relationships** area.

Note If you edit a region relationship within one region there is no need to duplicate that configuration in the other region as the settings will update in the other region automatically. For example, let's say that you open Region 1 in the **Region Configuration** window and configure a custom relationship to Region 2. If you were to then open Region 2, you would see the custom relationship displayed in the **Region Relationships** area

Configure Cisco Unified CM Groups

Use this procedure to set up Unified Communications Manager Groups for call processing redundancy, load balancing and failover for the devices in the device pool.

Tip Set up multiple groups and device pools where the primary server is different in each group so as to provide distributed call processing where device registrations are balanced evenly across the cluster nodes.

Note Do not use the default server group because it is not descriptive and can cause confusion.

Procedure

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

Step 2 Enter a **Name** for the group.

Note Consider identifying the order of the nodes in the name so that you can easily distinguish the group from others. For example, CUCM_PUB-SUB.

Step 3 Check the **Auto-registration Cisco Unified Communications Manager Group** check box if you want this Unified Communications Manager group to be the default Unified Communications Manager group when auto-registration is enabled.

Step 4 From the **Available Cisco Unified Communications Managers** list, choose the nodes that you want to add to this group, and click the down arrow to select them. You can add up to three servers to a group.
The servers in this group appear in the **Selected Cisco Unified Communications Managers** list box. The top server in the list is the primary server

Step 5 Use the arrows beside the **Selected Cisco Unified Communications Managers** list box to change which servers are the primary, and backup servers.

Step 6 Click **Save**.

Configure Device Pools

Set up device pools for your system devices. Apply the other core settings that you configured to the device pools in order to apply those settings to the devices that use this device pool. You can configure multiple device pools to meet your deployment needs.

Before you begin

If you want to assign an SRST configuration, refer to Survivable Remote Site Telephony Configuration Task Flow, on page 106.

Procedure

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

Step 2 Do either of the following:

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

Step 3 In the **Device Pool Name** field, enter a name for the device pool.

Step 4 From the **Cisco Unified Communications Manager Group** drop-down, select the group that you set up to handle call processing redundancy and load balancing.

Step 5 From the **Date/Time Group** drop-down, select the group that you set up to handle date, time, and phone NTP references for the devices that use this device pool.

Step 6 From the **Region** drop-down list box, select the region that you want to apply to this device pool.

Step 7 From the **Media Resource Group List** drop-down, select a list that contains the media resources that you want to apply to this device pool.

Step 8 Apply SRST settings for this device pool:

a) From the **SRST Reference** drop-down, assign an SRST reference.

b) Assign a value for the **Connection Monitor Duration** field. This This setting defines the time that the phone monitors its connection to Unified Communications Manager before it unregisterring from SRST and reregisterring to Unified Communications Manager.

Step 9 Complete the remaining fields in the **Device Pool Configuration** window. For help with the fields and their settings, see the online help.

Step 10 Click **Save**.

What to do next

Configure multiple device pools according to your deployment requirements.

Basic Device Pool Configuration Fields

Table 5: Basic Device Pool Configuration Fields

Field	Description
Device Pool Name	Enter the name of the new device pool. You can enter up to 50 characters, which include alphanumeric characters, periods (.), hyphens (-), underscores (_), and blank spaces.
Cisco Unified Communications Manager Group	Choose the Cisco Unified Communications Manager group to assign to devices in this device pool. A Cisco Unified Communications Manager group specifies a prioritized list of up to three Unified Communications Manager nodes. The first node in the list serves as the primary node for that group, and the other members of the group serve as backup nodes for redundancy.
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 region to assign to devices in this device pool. The region settings specify voice and video codecs that can be used for communications within a region and between other regions.

Call Preservation

The call preservation feature of Unified Communications Manager ensures that an active call does not get interrupted when a Unified Communications Manager fails or when communication fails between the device and the Unified Communications Manager that set up the call.

Unified Communications Manager supports full call preservation for an extended set of Cisco Unified Communications devices. This support includes call preservation between Cisco Unified IP Phones, Media Gateway Control Protocol (MGCP) gateways that support Foreign Exchange Office (FXO) (non-loop-start trunks) and Foreign Exchange Station (FXS) interfaces, and, to a lesser extent, conference bridge, MTP, and transcoding resource devices.

Enable H.323 call preservation by setting the advanced service parameter, Allow Peer to Preserve H.323 Calls, to True.

The following devices and applications support call preservation. If both parties connect through one of the following devices, Unified Communications Manager maintains call preservation:

- Cisco Unified IP Phones
- SIP trunks
- Software conference bridge
- Software MTP
- Hardware conference bridge (Cisco Catalyst 6000 8 Port Voice E1/T1 and Services Module, Cisco Catalyst 4000 Access Gateway Module)
- Transcoder (Cisco Catalyst 6000 8 Port Voice E1/T1 and Services Module, Cisco Catalyst 4000 Access Gateway Module)

- Non-IOS MGCP gateways (Catalyst 6000 24 Port FXS Analog Interface Module, Cisco DT24+, Cisco DE30+, Cisco VG200)
- Cisco IOS H.323 gateways (such as Cisco 2800 series, Cisco 3800 series)
- Cisco IOS MGCP Gateways (Cisco VG200, Catalyst 4000 Access Gateway Module, Cisco 2620, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 3810)
- Cisco VG248 Analog Phone Gateway

The following devices and applications do not support call preservation:

- Annunciator
- H.323 endpoints such as NetMeeting or third-party H.323 endpoints
- CTI applications
- TAPI applications
- JTAPI applications

Call Preservation Scenarios

The below table describes how call preservation is handled in various scenarios.

Table 6: Call Preservation Scenarios

Scenario	Call Preservation Handling
Cisco Unified Communications Manager fails.	A Cisco Unified Communications Manager failure causes the call-processing function for all calls that were set up through the failed Cisco Unified Communications Manager to be lost. Cisco Unified Communications Manager maintains affected active calls until the end user hangs up or until the devices can determine that the media connection has been released. Users cannot invoke any call-processing features for calls that are maintained due to this failure.

Scenario	Call Preservation Handling
Communication failure occurs between Cisco Unified Communications Manager and the device.	When communication fails between a device and the Cisco Unified Communications Manager that controls it, the device recognizes the failure and maintains active connections. The Cisco Unified Communications Manager recognizes the communication failure and clears call-processing entities that are associated with calls in the device where communication was lost. The Cisco Unified Communications Manager still maintain control of the surviving devices that are associated with the affected calls. Cisco Unified Communications Manager maintains affected active calls until the end user hangs up or until the devices can determine that the media connection has been released. Users cannot invoke any call-processing features for calls that are maintained due to this failure. **Note** • If there is a failover, when you bring up the Cisco Unified Communications Manager node within the KeepAlive timer, the phone remains registered to the current node although the call is in preservation mode. This is possible as KeepAliver time is active. • Consider a scenario where the peer is a SIP trunk and a call is established between an IP phone and the SIP trunk. If the phone loses communication with the Cisco Unified Communications Manager, then any media change from the trunk side results in 488 (not acceptable media) response with a cause value 38 (network error) in its reason header.
Device failure (Phone, gateway, conference bridge, transcoder, MTP)	When a device fails, the connections that exist through the device stop streaming media. The active Cisco Unified Communications Manager recognizes the device failure and clears call-processing entities that are associated with calls in the failed device. The Cisco Unified Communications Manager maintain control of the surviving devices that are associated with the affected calls. Cisco Unified Communications Manager maintains the active connections (calls) that are associated with the surviving devices until the surviving end users hang up or until the surviving devices can determine that the media connection has been released.

PART II

Enable Inbound and Outbound Calling

CHAPTER 8

Inbound Outbound Calling Overview

About Inbound and Outbound Calling

This part describes how to set up the inbound and outbound calling for your system.

Inbound and Outbound Calling Configuration

Complete the following task flows to configure Inbound and Outbound Calling for your system.

Procedure

	Command or Action	Purpose
Step 1	Gateway Configuration Task Flow, on page 68	Add gateways to your system.
Step 2	SIP Normalization and Transparency Configuration Task Flow, on page 82	Optional. Configure SIP Normalization and transparency scripts that you can assign to SIP trunks or SIP devices in order to resolve SIP interoperability issues.
Step 3	Configure SDP Transparency Profile, on page 88	Optional. If your SIP deployment requires support for SDP attributes that are not natively supported by Unified Communications Manager, set up an SDP transparency profile that includes the non-supported attributes.
Step 4	SIP Profile Overview, on page 89	Configure SIP profiles for your SIP trunks and SIP devices.
Step 5	IPv6 Configuration Task Flow, on page 92	Optional. If your SIP deployment requires support for IPv6 devices, configure dual stack IPv6 support in your system. Dual stack can be configured for SIP deployments only.

	Command or Action	Purpose
Step 6	SIP Trunk Configuration Task Flow, on page 99	Configure SIP trunks for your system.
Step 7	H.323 Trunk Overview, on page 103	Configure H.323 trunks for your system.
Step 8	Survivable Remote Site Telephony Configuration Task Flow, on page 106	Configure your system for SRST.

CHAPTER 9

Configure Gateways

Gateway Overview

Cisco offers a wide variety of voice and video gateways. A gateway provides interfaces that allow the Unified Communications network to communicate with an external network. Traditionally, gateways have been used to connect the IP-based Unified Communications network to legacy telephone interfaces such as the PSTN, a private branch exchange (PBX), or legacy devices such as an analog phone or fax machine. In its simplest form, a voice gateway has an IP interface and a legacy telephony interface, and the gateway translates messages between the two networks so that the two networks can communicate.

Gateway Protocols

Most Cisco gateways offer multiple deployment options and can be deployed using any one of a number of protocols. Depending on the gateway that you want to deploy, your gateway may be configurable using any of the following communication protocols:

- Media Gateway Control Protocol (MGCP)
- Skinny Call Control Policy (SCCP)
- Session Initiation Protocol (SIP)
- H.323

Vendor Interface Cards

The Vendor Interface Card (VIC) must be installed on the gateway to provide a connection interface for external networks. Most gateways offer multiple VIC options and each VIC may offer many different ports and connection types for both analog and digital connections.

Refer to your gateway documentation for the protocols, cards, and connections that are offered with your gateway.

Port and Trunk Connection Types

Following are the main types of port connections that you can configure on gateways:

- Foreign Exchange Station (FXS)—FXS ports offer connections to analog stations such as an analog phone, speakerphone, or legacy voicemail system.
- Foreign Exchange Office (FXO)—FXO ports offer analog connections to the PSTN or a legacy PBX.
- T1 Channel Assocatied Signaling (T1/E1 CAS) —T1/E1 CAS connections offer digital trunk connections to a central office, PBX, or other analog device.
- Primary Rate Interface (T1/E1 PRI)—Digital access PRI connections are widely used in corporate communications. T1 PRI is widely used in North America and Japan and offers 23 B-channels for voice and data and one D-channel for common channel signaling at a rate of 1.544 Mb/s. E1 is widely used in Europe, offering 30 B-channels for voice and data, one D-channel for common signaling, and one framing channel. E1 uses of rate of 2.048 Mb/s.
- Basic Rate Interface (BRI)—BRI is a digital telephony protocol, which is used for small office and home communications links, provides two B-channels for voice and data and one D-channel for signaling.

Connection Types per Protocol

MGCP gateways offer the following connection types:

- TI/E1 PRI Digital access
- T1 CAS
- BRI
- FXO
- FXS

SCCP gateways offer the following connection types:

- FXS
- BRI

SIP gateways offer the following connections:

- FXS
- FXS-DID
- E&M
- BRI
- BRI QSIG
- T1 CAS
- T1 FGD
- E1 CAS

- T1/E1 PRI
- T1/E1 QSIG
- T1/E1 NFAS
- T1/E1 PRI (MegacomISDN)
- Centralized Automatic Message Accounting (CAMA)
- J1

H.323 gateways offer the following connection types:

- FXS
- FXS-DID
- E&M
- BRI
- BRI QSIG
- T1 CAS
- T1 FGD
- E1 CAS
- T1/E1 PRI
- T1/E1 QSIG
- T1/E1 NFAS
- T1/E1 PRI (MegacomISDN)
- Centralized Automatic Message Accounting (CAMA)
- J1

Gateway Setup Prerequisites

Install the Hardware

Before you configure the gateway in Cisco Unified Communications Manager, you must perform the following tasks on your gateway hardware:

- Install and configure the gateway
- Install any vendor interface cards (VICs) on the gateway.
- Use the CLI to configure IOS on the gateway.

For details, refer to the hardware and software documentation that comes with your gateway.

Note To get to the default web pages for many gateway devices, you can use the IP address of that gateway. Make your hyperlink url = http://x.x.x.x/, where x.x.x.x is the dot-form IP address of the device. The web page for each gateway contains device information and the real-time status of the gateway.

Plan the Gateway Deployment

Before configuring the gateway in Cisco Unified Communications Manager, make sure that you adequately plan the types of connections that you want to configure on the gateway. Many gateways can be configured using any one of MGCP, SIP, H.323, or SCCP as the gateway protocol. The connection types for each type of deployment vary according to the protocol that you choose and the VICs that are installed on the gateway. Be sure to understand the following:

- Which gateway protocols does your gateway support.
- What types of port connections the VICs on the gateway support.
- What types of connections are you planning on configuring?
- For analog connections, are you connecting to the PSTN, legacy PBX, or to legacy devices.
- For digital access connections, are you connecting to a T1 CAS interface, or to a PRI interface?
- For FXO connections, how do you want to direct incoming calls? Are you directing incoming calls to an automated IVR or to an attendant?

Gateway Configuration Task Flow

Perform the following tasks to add your network gateways to Unified Communications Manager.

Before you begin

Review the Gateway Setup Prerequisites, on page 67.

Procedure

	Command or Action	Purpose
Step 1	Configure your gateways in Unified Communications Manager. Perform any of the following procedures depending on the protocol that you wan to deploy: • Configure MGCP Gateway, on page 69 • Configure SCCP Gateway, on page 76 • Configure SIP Gateway, on page 76 • Configure H.323 Gateway, on page 78	Many Cisco gateways can be deployed using any one of MGCP, SCCP, SIP, or H.323 as the gateway protocol. Review your gateway documentation to determine which protocols your gateway supports and which protocol is best for your deployment. SCCP gateways can connect only to analog access or ISDN BRI connections.
Step 2	Configure Clusterwide Call Classification for Gateway, on page 79	Optional. Configure a clusterwide service parameter to classify all calls coming from the

	Command or Action	Purpose
		gateway ports in your network to be internal (OnNet) or external (OffNet). **Note** The call classification setting in the Port Configuration for individual gateway port interfaces overrides the clusterwide setting. However, the default setting for gateway ports is to use the setting from the clusterwide service parameter.
Step 3	Block OffNet Gateway Transfers, on page 79	Optional. If you want to block Unified Communications Manager from transferring calls from one external (OffNet) gateway to another external gateway, configure the **Block OffNet to Offnet Transfer** service parameter. By default, this service parameter is configured to allow transfers from one external (OffNet) gateway to another.

Configure MGCP Gateway

Perform the following tasks to configure a Cisco gateway to use an MGCP configuration.

Before you begin

Gateway Setup Prerequisites, on page 67

Procedure

	Command or Action	Purpose
Step 1	Configure MGCP (IOS) Gateway, on page 70	Add the gateway in Cisco Unified CM Administration and choose **MGCP** as the gateway protocol. Configure the gateway with the appropriate slots and vendor interface cards (VICs).
Step 2	Configure the gateway port interface. Select any of the following tasks, depending on the type of interface that you want to configure: • Configure Digital Access PRI Ports, on page 74	Configure the port connections for the devices that connect to the VICs that are installed on the gateway. Most VICs include multiple port connections and options so you may have to configure a few different port interface types.

	Command or Action	Purpose
	• Configure Digital Access T1 Ports for MGCP Gateway, on page 72 • Configure FXS Ports, on page 70 • Configure FXO Ports, on page 71 • Configure BRI Ports, on page 74	**Tip** After you configure a port interface, from the **Related Links** drop-down list box, select the **Back to MGCP Configuration** option to return to the **Gateway Configuration** window, where you can select and configure another port interface.
Step 3	Add Digital Access T1 Ports for MGCP Gateway, on page 73	Optional. If you have configured a digital access T1 CAS port interface, add T1 CAS ports to the gateway. You can add ports on an individual basis or add a range of ports simultaneously.
Step 4	Reset Gateway, on page 75	The configuration changes take effect after you reset the gateway

Configure MGCP (IOS) Gateway

Perform the following procedure to add and configure an MGCP (IOS) gateway on the Unified Communications Manager.

Procedure

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

Step 2 Click **Add New**.

Step 3 From the **Gateway Type** drop-down list, select the gateway and click **Next**.

Step 4 From the **Protocol** drop-down list, choose **MGCP** and click **Next**.

Step 5 In the **Configured Slots, VICs and Endpoints** area, perform the following steps:

a) From each **Module** drop-down list, select the slot that corresponds to the Network Interface Module hardware that is installed on the gateway.

b) From each **Subunit** drop-down list, select the VIC that is installed on the gateway.

c) Click **Save**.
The **Port** icons appear. Each Port icon corresponds to an available port interface on the gateway. You can configure any port interface by clicking the corresponding port icon.

Step 6 Complete the remaining fields in the **Gateway Configuration** window. For more information on the fields, see the system Online Help.

Step 7 Click **Save**.

Configure FXS Ports

Configure Foreign Exchange Station (FXS) ports on an MGCP gateway. You can use FXS ports to connect the gateway to a Plain Old Telephone Service (POTS) legacy phone or to another legacy device such as a fax machine, speakerphone, legacy voice-messaging system, or Interactive Voice Response (IVR).

Before you begin

You must add a gateway before configuring ports.

Procedure

Step 1 In the Cisco Unified CM Administration, choose **Device** > **Gateway**.

Step 2 Click **Find** and select the gateway on which you want to configure FXS ports.

Step 3 In the **Configured Slots, VICs, and Endpoints** area, click the **FXS Port** icon for the port that you want to configure.
The Port Selection area displays.

Step 4 From the **Port Type** drop-down list, choose the type of connection that you want to configure:

- **POTS**—Select this option if you want to connect this port to a POTS device such as a legacy phone.
- **Ground Start**—Select this option if you want to use ground a start signaling to connect this port to an unattended legacy device such as a fax machine, legacy voice-messaging system, or IVR.
- **Loop Start**—Select this option if you want to use a loop start signaling to connect this port to an unattended legacy device such as a fax machine, legacy voice-messaging system, or IVR.

Step 5 Click **Next**.
The **Port Configuration** window displays the configuration for the port interface with an analog access as the device protocol.

Step 6 From the **Device Pool** drop-down list, select a device pool.

Step 7 Complete the remaining fields in the **Port Configuration** window.

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

Step 8 Click **Save**.

Step 9 (Optional) To configure more port interfaces on the MGCP IOS gateway, from the **Related Links** drop-down list, select **Back to Gateway** and click **Go**.

The **Gateway Configuration** window displays the available ports for the gateway.

When you have completed configuring more ports interfaces, see Reset Gateway, on page 75.

Configure FXO Ports

Configure Foreign Exchange Office (FXO) ports on an MGCP (IOS) gateway. You can use FXO ports to connect the gateway to the PSTN or a legacy PBX.

Note Unified Communications Manager assumes all loop-start trunks lack the positive disconnect supervision. Configure trunks with the positive disconnect supervision as ground start, so that the active calls can be maintained during a server failover.

Before you begin

Configure MGCP (IOS) Gateway, on page 70

Procedure

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

Step 2 Click **Find** and select the gateway for which you want to configure FXO ports.

Step 3 From the **Configured Slots, VICs, and Endpoints** area, locate the **Module** and **Subunit** that contain the FXO port on which you want to set up an FXO port interface and click the **Port** icon for the port that you want to configure.

Step 4 From the **Port Type** drop-down list, select either **Ground-Start** or **Loop-Start**.

Note If you are configuring the VIC-2 FXO port, you must select the same port type for both ports of the subunit module.

Step 5 From the **Device Pool** drop-down list, select a device pool.

Step 6 In the **Attendant DN** text box, enter the directory number to which you want to route all incoming calls from this port connection. For example, a zero or the directory number for an attendant.

Step 7 Complete any remaining fields in the **Port Configuration** window. Refer to the online help for field descriptions.

Step 8 Click **Save**.

Step 9 (Optional) To configure more port interfaces on the MGCP IOS gateway, from the **Related Links** drop-down list, select **Back to Gateway** and click **Go**.

The **Gateway Configuration** window displays the available ports for the gateway.

When you have completed configuring more ports interfaces, see Reset Gateway, on page 75.

Configure Digital Access T1 Ports for MGCP Gateway

Configure the port interface for digital access T1 CAS ports on an MGCP (IOS) gateway.

Before you begin

Configure MGCP (IOS) Gateway, on page 70

Procedure

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

Step 2 Click **Find** and select the gateway on which you want to configure a T1 port.

Step 3 In the **Configured Slots, VICs and Endpoints** area, locate the Module and Subunit on which you want to set up a Digital Access T1 (T1-CAS) port and click the corresponding **Port** icon.

Step 4 From the **Device Protocol** drop-down list, choose **Digital Access T1** and click **Next**.

Step 5 Enter the appropriate gateway configuration settings.

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

Step 6 Click **Save**.

For more information on adding ports to the Digital Access T1 CAS port interface, see Add Digital Access T1 Ports for MGCP Gateway, on page 73.

Add Digital Access T1 Ports for MGCP Gateway

Add and configure T1 CAS ports to a T1 Digital Access port interface for an MGCP gateway. You can add and configure up to 24 T1 CAS ports. You can also add ports on an individual basis or add and configure a range of ports simultaneously. If you enter a range of ports, Unified Communications Manager applies the configuration to the entire range of ports.

Before you begin

Configure Digital Access T1 Ports for MGCP Gateway, on page 72

Procedure

Step 1 In Cisco Unified CM Administration, choose **Device** > **Gateway**.

Step 2 Click **Find** and select the gateway that contains the T1 CAS port interface.

Step 3 Click **Add a New Port**.

Step 4 From the **Port Type** drop-down list, select the type of port that you want to add and click **Next**.

Step 5 Enter port numbers in the **Beginning Port Number** and **Ending Port Number** fields to specify the range of ports that you want to add and configure.

For example, enter `1` and `10` to add ports 1 through 10 to the port interface simultaneously.

Step 6 From the **Port Direction** drop-down list, configure the direction of calls passing through this port:

- **Bothways**—Select this option if the port allows both inbound and outbound calls.
- **Inbound**—Select this option if the port allows inbound calls only.
- **Outbound**—Select this option if the port allows outbound calls only.

Step 7 For EANDM ports, from the **Calling Party Selection** drop-down list, choose how you want the calling number to display for outbound calls from the device that is attached to this port:

- **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 an external phone mask applied.
- **Last Redirect Number (External)**—Send the directory number of the last redirecting device with the external phone mask applied.

Step 8 Click **Save**.

Step 9 If you want to configure more ports for the MGCP gateway, from **Related Links** select **Back to Gateway** and click **Go**. When the Digital Access T1 port interface appears, perform either of the following steps:

- If you want to add additional Digital Access T1 CAS ports to this port interface, return to step 3 (**Add a New Port**) of this procedure.

- If you want to configure more port interfaces on the gateway, from **Related Links** select **Back to MGCP Configuration** and click **Go**. The **Gateway Configuration** window displays the available ports for the gateway subunit modules.
- When you have completed configuring more ports interfaces, see Reset Gateway, on page 75.

Configure Digital Access PRI Ports

Configure the PRI port interface for an MGCP (IOS) gateway.

Before you begin

Configure MGCP (IOS) Gateway, on page 70

Procedure

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

Step 2 Click **Find** and select the gateway on which you want to configure PRI ports.

Step 3 In the **Configured Slots, VICs, and Endpoints** area, locate the Module and Subunit that contains the BRI port that you want to configure and click the **Port** icon that corresponds to the BRI port that you want to configure.
The **Gateway Configuration** window displays the BRI port interface.

Step 4 From the **Device Pool** drop-down list, select a device pool.

Step 5 Complete the remaining fields in the **Gateway Configuration** window. Refer to the online help for field descriptions.

Step 6 Click **Save**.

Step 7 (Optional) If you want to configure more port interfaces for the gateway, from the **Related Links** drop-down list, choose **Back to MGCP Configuration** and click **Go**.

The **Gateway Configuration** window displays the available port interfaces for the gateway.

When you have completed configuring more ports interfaces, see Reset Gateway, on page 75.

Configure BRI Ports

Configure a BRI port interface for an MGCP (IOS) gateway.

Before you begin

Configure MGCP (IOS) Gateway, on page 70

Procedure

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

Step 2 Click **Find** and select the gateway on which you want to configure BRI ports.

Step 3 In the **Configured Slots, VICs, and Endpoints** section, locate the subunit that uses BRI ports and click the **Port** icon for the port that you want to configure.
The **Gateway Configuration** window displays the information for the BRI port interface.

Step 4 From the **Device Pool** drop-down list, select a device pool.

Step 5 Enter the appropriate Gateway Information and Port Information settings. For more information on the fields and their configuration options, see the system Online Help.

Step 6 Click **Save**.

Step 7 (Optional) If you want to configure more port interfaces for the gateway, from the **Related Links** drop-down list, choose **Back to MGCP Configuration** and click **Go**.

The **Gateway Configuration** window displays the available port interfaces for the MGCP gateway.

When you have completed configuring more ports interfaces, see Reset Gateway, on page 75.

Reset Gateway

Most gateways need to be reset for configuration changes to take effect. We recommend that you complete all necessary gateway configuration before performing a reset.

Note Resetting an H.323 gateway only reinitializes the configuration that Unified Communications Manager loaded and does not physically restart or reset the gateway.

Procedure

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

Step 2 Click **Find** and select the gateway.

Step 3 Click the check box beside the gateway that you want to reset and click **Reset Selected**. The **Device Reset** dialog box appears. Do one of the following actions:

Step 4 Click **Reset**.

MGCP Caller-ID Restriction

If FROM header contains a special character(s) in the incoming SIP requests, it impacts the SIP-MGCP/323 call flow and the system disconnects the call or displays issues. Hence fix the networking node from where the request is reaching out to Unified Communications Manager.

For Example:

- Special characters present along with alphabets like "Per%cent" affect the display name.
- Many special characters present like "0%09%0A%01%05%0A%01%03%0A%01%04" could disconnect the call as the remote name being sent to MGCP side as CRCX can have issues.

Configure SCCP Gateway

You can configure a Cisco gateway to use SCCP as the gateway protocol. You can use this deployment option to connect Unified Communications Manager to analog access devices or ISDN BRI devices using FXS or BRI ports. You cannot connect an SCCP gateway to digital access T1 or E1 trunks.

Procedure

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

Step 2 Click **Add New**.

Step 3 From the **Gateway Type** drop-down list, choose a gateway that uses SCCP and click **Next**.

Step 4 From the **Protocol** drop-down list, choose **SCCP**.

Step 5 In the **Configured Slots, VICs and Subunits** section, perform the following steps:

a) For each **Module** drop-down list, select the slot that corresponds to the Network Interface Module hardware that is installed on the gateway.

b) For each **Subunit**, select the VIC that is installed on the gateway.

Step 6 Complete the remaining fields in the **Gateway Configuration** window.

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

Step 7 Click **Save**.
The **Port** icons appear alongside the subunit modules. Each port icon corresponds to a configurable port interface on the gateway. You can configure an analog access or ISDN BRI phone on a port by clicking the corresponding port icon.

Step 8 Apply the changes to the gateway when you complete the update:

a) Click **Reset Gateway**. The **Restart Gateway** pop-up appears.

b) Click **Reset**.

Configure SIP Gateway

Perform the following tasks to configure a SIP gateway in Unified Communications Manager. Many Cisco gateways and third-party gateways can be configured to use SIP. Unified Communications Manager does not contain a gateway device type for SIP gateways.

Before you begin

You must install the gateway hardware in your network and configure the IOS software on the gateway before you add the gateway in Unified Communications Manager.

Procedure

	Command or Action	Purpose
Step 1	Configure SIP Profile, on page 77	Configure SIP settings and apply to a SIP profile. Trunk uses this settings to connect to the SIP gateway.

	Command or Action	Purpose
Step 2	Configure SIP Trunk Security Profile., on page 77	Configure a SIP Trunk Security Profile so that trunk uses this to connect to the SIP gateway. You can configure security settings, such as device security mode, digest authentication, and incoming/outgoing transport type settings.
Step 3	Configure SIP Trunk for SIP Gateway, on page 78	Configure a SIP trunk that points to the SIP gateway. Apply the SIP Profile and the SIP Trunk Security Profile to the SIP trunk.

Configure SIP Profile

Configure a SIP profile for your SIP gateway connection.

Procedure

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

Step 2 Perform either of the following steps:

- Click **Add New** to create a new profile.
- Click **Find** to select an existing SIP profile.

Step 3 Complete the fields in the **SIP Profile Configuration** window.

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

Step 4 Click **Save**.

Configure SIP Trunk Security Profile.

Configure a SIP trunk security profile with security settings for a trunk that connects to a SIP gateway.

Procedure

Step 1 In Cisco Unified CM Administration, choose **System** > **Security** > **SIP Trunk Security Profile.**

Step 2 Perform either of the following steps:

a) Click **Find** to select an existing profile.
b) Click **Add New** to create a new profile.

Step 3 Complete the fields in the **SIP Trunk Security Profile Configuration** window.

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

Step 4 Click **Save**.

Configure SIP Trunk for SIP Gateway

Configure a SIP trunk to connect Unified Communications Manager to a Cisco or third party gateway that uses SIP. Under this configuration, do not enter the gateway as a device in the **Gateway Configuration** window.

Procedure

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

Step 2 Click **Add New** to set up a new SIP trunk.

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

Step 4 From the **Protocol** drop-down list, choose **None**.

Step 5 In the **Destination Address** field of the SIP Information pane, enter an IP address, fully qualified domain name, or DNS SRV record for the SIP gateway.

Step 6 From the **SIP Trunk Security Profile** drop-down list, choose the SIP trunk security profile that you configured for this gateway.

Step 7 From the **SIP Profile** drop-down list box, choose the SIP profile that you configured for this gateway.

Step 8 Complete the fields in the **SIP Trunk Configuration** window. Refer to the online help for field descriptions.

Step 9 Click **Save**.

Configure H.323 Gateway

Configure an H.323 gateway in Unified Communications Manager for a non-gatekeeper H.323 deployment.

Note If your deployment includes H.323 gatekeepers, you can also add an H.323 gateway by setting up a gatekeeper-controlled H.225 trunk. This scenario is not documented in this guide because gatekeeper usage has been in steady decline recent years. If you want to configure gatekeepers and H.225 gatekeeper-controlled trunks, refer to the *Cisco Unified Communications Manager Administration Guide,* Release 10.0(1).

Note When a gateway is registered with Unified Communications Manager, the registeration status may display in Unified Communications Manager Administration as unknown.

Procedure

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

Step 2 Click **Add New**.

Step 3 From the **Gateway Type** drop-down list, choose **H.323 Gateway**.

Step 4 In the **Device Name** field, enter the IP address or hostname of the gateway.

Step 5 If you want to use H.235 to configure a secure channel, check the **H.235 Data Passthrough** check box.

Step 6 Configure the fields in the **Gateway Configuration** window.

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

Step 7 Click **Save**.

Step 8 Click **Reset** to reset the gateway and apply the changes.

Most gateways need to be reset for configuration changes to take affect. We recommend that you complete all necessary gateway configuration before performing a reset.

Configure Clusterwide Call Classification for Gateway

Configure the **Call Classification** setting for your network gateways. This setting determines whether the system considers the gateways in the network to be internal (OnNet) or external (OffNet).

The **Call Classification** field also appears in the configuration window for individual gateway port interfaces. By default, each gateway port interface is configured to use the setting from the clusterwide service parameter. However, if **Call Clasification** on a port is configured differently from the clusterwide service parameter, the setting on that port overrides the service parameter setting.

Procedure

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

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

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

Step 4 Under **Clusterwide Parameters (Device - General)**, configure one of the following values for the **Call Classification** service parameter.

- **OnNet**—Calls from this gateway are classified as originating from inside the company network.
- **OffNet**—Calls from this gateway are classified as originating from outside the company network.

Step 5 Click **Save**.

Block OffNet Gateway Transfers

Use this procedure if you want to configure the system to block calls that are transferred from one external (OffNet) gateway to another external (OffNet) gateway. By default, the system allows transfers from one external gateway to another external gateway.

The setting that determines whether a gateway is external (OffNet) or internal (OnNet) is determined by the Call Classification setting. It is configured using a clusterwide service parameter, or by configuring any of the following port interfaces:

- MGCP T1/E1 port interfaces
- MGCP FXO port interface
- H.323 gateways

- SIP trunks

Procedure

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

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

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

Step 4 Configure a setting for the **Block OffNet to Offnet Transfer** service parameter:

- **True**—Select this option to cancel transfers between two external (OffNet) gateways.
- **False**—Select this option to allow transfers between two external (OffNet) gateways. This is the default option.

Step 5 Click **Save**.

Note You can also classify calls through a gateway as OnNet or OffNet by associating the gateway to a route pattern and configure **Call Classification** in the **Route Pattern Configuration** window.

CHAPTER 10

Configure SIP Normalization and Transparency

SIP Normalization and Transparency Overview

SIP normalization and transparency is an optional feature that handles SIP interoperability issues between Unified Communications Manager and endpoints, service providers, PBXs, or gateways that implement SIP differently. To configure SIP normalization and transparency, apply a customized LUA script to a SIP trunk or SIP line. Unified Communications Manager applies the script to the SIP messaging that passes through the SIP trunks or SIP lines.

Upon installation, Unified Communications Manager contains default normalization and transparency scripts that you can assign to the SIP trunks and SIP profiles in your system. You can also create and import your own customized scripts.

SIP Normalization

SIP normalization scripts modify incoming and outgoing SIP messages. For example, if you are interoperating Unified Communications Manager with a Cisco TelePresence Video Communications Server, apply the *vcs-interop* script to the SIP trunk that connects the two. The script resolves the differences in the SIP messaging so that the two products can communicate.

You can apply a normalization script to any SIP trunk connection, regardless of which protocol is being used by the endpoint that connects to that SIP trunk.

SIP Transparency

SIP transparency scripts enable Unified Communications Manager to transparently pass SIP information, such as proprietary headers, from one call leg to the other. For transparency to work, both call legs must be SIP.

Another feature of SIP transparency is REFER transparency, which allows Unified Communications Manager to pass on REFER requests without acting on them. You can use REFER transparency in call center environments where a centralized agent may answer a call and then transfer the call to an agent who resides in the same geographical area as the caller. REFER transparency allows the centralized Unified Communications Manager to drop the call and shift call control to the new agent.

Default Scripts for SIP Normalization and Transparency

Upon installation, Cisco Unified Communications Manager contains the following default scripts for SIP Normalization and Transparency. You can apply these scripts to a SIP trunk or SIP profile, but you cannot edit these scripts. If none of these scripts meet your needs, you can create your own scripts:

- **cisco-meeting-server-interop**—Provides interoperability between Cisco Unified Communications Manager and Cisco Meeting Server (CMS).
- **cisco-telepresence-conductor-interop**—Provides interoperability for endpoints that are registered to TelePresence Conductor.
- **cisco-telepresence-mcu-ts-direct-interop**—Provides interoperability between Cisco Unified Communications Manager and either Cisco TelePresence MCU or Cisco TelePresence Server.
- **diversion-counter**—Provides capability to adjust the diversion counter.
- **HCS-PCV-PAI passthrough**—Provides Cisco HCS platform integration with Enterprise IMS.
- **refer-passthrough**—Removes Cisco Unified Communications Manager from the call due to a blind transfer between SIP trunks.
- **vcs-interop**—Provides interoperability for endpoints that are registered to the Cisco TelePresence Video Communications Server.

SIP Normalization and Transparency Prerequisites

- Cisco Unified Communications Manager provides default scripts for SIP Normalization and Transparency. Make sure to review the existing scripts and system settings to verify whether they meet your needs. For information on the available default scripts, see Default Scripts for SIP Normalization and Transparency, on page 82.
- Make sure that you understand your deployment's SIP requirements in addition to the SIP requirements for any third-party products. For information on Cisco Unified Communications Manager's implementation of SIP, review the *SIP Line Messaging Guide for Cisco Unified Communications Manager (Standard Edition)* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-programming-reference-guides-list.html.
- If you plan to develop customized SIP Normalization scripts, review the *Developer Guide for SIP Normalization and Transparency* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-programming-reference-guides-list.html.

SIP Normalization and Transparency Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Create New SIP Normalization and Transparency Scripts, on page 83	Optional. If none of the preinstalled scripts meet your needs, use this procedure to configure a customized script. You can create your new

	Command or Action	Purpose
		script in the **SIP Normalization Script Configuration** window or you can import a customized script.
Step 2	Apply Normalization or Transparency Script to SIP Trunk, on page 84	In the Trunk Configuration window, apply a script directly to a SIP trunk. Cisco Unified Communications Manager applies the script to all the SIP messaging that passes through the trunk
Step 3	Apply Normalization or Transparency to SIP Devices, on page 84	If you want to apply a normalization or transparency script to a SIP line, apply a script to the SIP profile that is associated to that SIP line. Cisco Unified Communications Manager applies the script to all SIP messaging that uses that SIP profile.

Create New SIP Normalization and Transparency Scripts

If the default normalization and transparency scripts do not meet your needs, use this procedure to create a new LUA script. You can either write the new script in Cisco Unified Communications Manager or import a file into the system.

Tip If the script that you want to create closely resembles a default script, open the default script in the **SIP Normalization Script Configuration** window and copy the **Contents** text box. Create a new script and paste the contents into the **Contents** text box. You can then edit the content in the new script.

Note The memory utilization of the SIP Normalization Script is based on each trunk and not on each script.

Procedure

Step 1 In Cisco Unified CM Administration, choose **Device** > **Device Settings** > **SIP Normalization Script**.

Step 2 Click **Add New**.
The SIP Normalization Script Configuration window appears.

Step 3 Enter a **Name** and **Description** for your script.

Step 4 If you are writing a new script, edit the script in the **Contents** text box.

Step 5 Optional. If you have an external file that you want to import, do the following

a) Click **Import File**.
b) **Browse** to locate the file and select the file.
c) Click **Import File**.
The **SIP Normalization Script Configuration** window displays the contents of the imported file in the **Contents** text box.

Step 6 Complete the fields in the **SIP Normalization Script Configuration** window. For help with the fields and their contents, refer to the online help.

Step 7 Click **Save**.

What to do next

Assign the script to a SIP profile or SIP trunk:

- Apply Normalization or Transparency to SIP Devices, on page 84
- Apply Normalization or Transparency Script to SIP Trunk, on page 84

Apply Normalization or Transparency Script to SIP Trunk

Use this procedure to apply a SIP normalization or transparency script to a SIP trunk. Cisco Unified Communications Manager applies the script to all SIP messaging that passes through the trunk.

Procedure

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

Step 2 Click **Find** and select the trunk to which you want to apply a script.

Step 3 From the **Normalization Script** drop-down list, choose the script that you want to apply to the trunk.

Step 4 (Optional) If you want to normalize specific parameters within the SIP messaging, do the following:

a) Enter the **Parameter Name** that you want to normalize, and the **Parameter Value** for the value that you want to apply to the parameter. For example, you could enter a **`Location`** parameter and **`North Carolina`** as the value.

b) To add additional parameters, click the **(+)** to create additional lines where you can enter additional parameters and values.

Step 5 (Optional) If you want to produce SDI traces against the script, check the **Enable Trace** check box.

Note Cisco recommends that you enable tracing while debugging your scripts.

Step 6 Click **Save**.

Apply Normalization or Transparency to SIP Devices

You can apply a customized SIP Normalization and Transparency script, or a customized SDP Transparency Profile to a SIP phone by applying the script to the SIP Profile that is used by that device.

Procedure

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

Step 2 Click **Find** and select the SIP profile to which you want to apply a script.

Step 3 In the **SDP Information** area, from the **SDP Transparency Profile** drop-down list, choose a profile.

Step 4 From the **Normalization Script** drop-down list, choose the script that you want to apply to the trunk.

Step 5 (Optional) If you want to normalize specific parameters within the SIP messaging, do the following:

a) Enter the **Parameter Name** that you want to normalize, and the **Parameter Value** for the value that you want to apply to the parameter. For example, you could enter a **`Location`** parameter and **`North Carolina`** as the value.

b) To add additional parameters, click the **(+)** to create additional lines where you can enter additional parameters and values.

Step 6 (Optional) If you want to produce SDI traces against the script, check the **Enable Trace** check box.

Note Cisco recommends that you enable tracing while debugging your scripts.

Step 7 Click **Save**.

CHAPTER 11

Configure SDP Transparency Profiles

SDP Transparency Profile Overview

SDP Transparency Profiles contain a set of rules for declarative SDP attributes that allow the system to pass through declarative attributes that are not natively supported by Unified Communications Manager from the ingress to the egress call leg. Without an SDP transparency profile, Unified Communications Manager drops non-supported SDP attributes.

You can configure SDP transparency profiles with multiple rules and apply them to SIP devices via the SIP profile. In order for the SDP transparency profile to be applied, both call legs must be SIP. You can configure the following types of rules for SDP attributes:

- Property—If a rule is configured for a property attribute, Unified Communications Manager passes through the SDP attribute unless the attribute has a value.
- Any Value—If a rule is configured for any value, the SDP attribute gets passed through so long as it has a value that consists of at least one non-white space character.
- Value From List—If a rule is configured using this option, the SDP attribute gets passed through so long as it matches one of the specified values. You can configure up to five possible values

SDP Transparency Profile Restrictions

The following restrictions apply to SDP transparency profiles. If any of these situations occur on the egress call leg, Cisco Unified Communications Manager will not pass through the declarative SDP attribute:

- One or more Media Termination Points (MTPs) or Trusted Relay Points (TRPs) that do not support passthrough are allocated
- The Media Termination Point Required check box is checked for the SIP trunk
- A transcoder is being used
- RSVP is being used

- The ingress call leg is using Delayed Offer while the egress call leg is using Early Offer
- The media line has been rejected (port=0)
- Either call leg is using a protocol other than SIP

SDP Transparency Profile Prerequisites

If you plan to deploy any third-party SIP products, make sure that you understand how the products implement the Session Description Protocol (SDP).

Configure SDP Transparency Profile

Configure a customized SDP Transparency Profile with a set of rules for declarative SDP attributes that are not natively supported by Cisco Unified Communications Manager.

Procedure

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

Step 2 Click **Add New**.

Step 3 Enter a **Name** and **Description**.

Step 4 In the **Attribute Information** pane, create the rules for the SDP attributes that you want to pass through:

- To pass through a property attribute, enter the attribute in the **Name** text box (for example, a=recvonly) and from the **Type** drop-down list, select **Property**.
- To pass through a value attribute, enter the attribute in the **Name** text box (for example, a=rtpmap), and select **Any Value** from the **Type** drop-down list box.
- To pass through a value attribute with any of up to five values, enter the attribute in the **Name** field (for example, a=rtpmap) and select **Any Value** from the **Type** drop-down list. In the resulting **Value** text box, enter the value of the attribute. You can click **+** to add up to five possible values for this attribute.

Step 5 Click the **(+)** to create new lines where you can enter additional SDP attributes for this transparency profile.

Step 6 Click **Save**.

Note You must apply this profile to a SIP Profile so that the devices that use the SIP Profile can use the SDP Transparency Profile.

CHAPTER 12

Configure SIP Profiles

SIP Profile Overview

A SIP Profile is a template that comprises common SIP settings. If you are deploying SIP devices or SIP trunks in your network, you can apply common SIP settings to groups of devices through the SIP Profile. You can configure multiple profiles for groups of SIP endpoints. You can choose from a variety of default SIP Profiles or create your own.

Without the SIP Profile, you would have to configure SIP settings individually for every SIP trunk and SIP device in your network. However, you can use the SIP profile to assign many SIP settings, such as the following:

- MTP Telephony Payload Types
- SIP header details
- Timers and counters for SIP messages
- SDP transparency profiles for SDP interoperability
- SIP Normalization and Transparency scripts for SIP lines
- SIP OPTIONS settings
- SIP Early Offer support
- Call Pickup URIs

Configure SIP Profiles

Use this procedure to configure a SIP profile with common SIP settings that you can assign to SIP devices and trunks that use this profile.

Procedure

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

Step 2 Perform one of the following steps:

- Click **Find** and select the SIP profile to edit an existing profile, .
- Click **Add New** to create a new profile.

Step 3 If you want your SIP phones and trunks to support IPv4 and IPv6 stacks, check the **Enable ANAT** check box.

Step 4 If you want to assign an SDP transparency profile to resolve SDP interoperability, from the **SDP Transparency Profile** drop-down list.

Step 5 If you want to assign a normalization or transparency script to resolve SIP interoperability issues, from the **Normalization Script** drop-down list, select the script.

Step 6 (Optional) Check the **Send ILS Learned Destination Route String** check box for Global Dial Plan Replication deployments where you may need to route calls across a Cisco Unified Border Element.

Step 7 Complete the remaining fields in the **SIP Profile Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 8 Click **Save**.

CHAPTER 13

Configure IPv6 Stack

IPv6 Stack Overview

IPv6 is an expanded IP addressing protocol that uses 128 bits instead of the 32 bits that IPv4 addresses use. IPv6 provides a much broader range of IP address than IPv4, which greatly reduces the risk of IP address exhaustion, which is among the main concerns with IPv4 addressing.

By default, Cisco Unified Communications Manager is configured to use IPv4 addressing. However, you can also configure the system to support the IPv6 stack thereby allowing you to deploy a SIP network with IPv6-only endpoints. In addition to reducing the risk of IP address exhaustion, IPv6 provides some of the following benefits:

- Stateless address autoconfiguration
- Simplified multicasting functionality
- Simplified routing, minimizing the need for routing tables
- Delivery of services optimization
- Better handling of mobility
- Greater privacy and security

IPv6 at the System Level

If you are deploying an IPv6 network, the Cisco Unified Communications Manager server still uses IPv4 for some internal communications. This is because some internal system components and applications support only IPv4. As a result, even if all of your devices operate in IPv6-only mode, the Cisco Unified Communications Manager server will still have both an IPv4 and IPv6 address as the server must use IPv4 for some internal communications.

Note If you need your SIP devices to operate in both IPv4 and IPv6 networks, you will need to configure two stacks. After you complete the tasks in this chapter to enable the IPv6 stack in Cisco Unified Communications Manager, you will then have to also enable your SIP network for two stacks. See Two Stacks (IPv4 and IPv6) Overview, on page 689.

IPv6 Prerequisites

Before you configure Cisco Unified Communications Manager with IPv6 support, you must configure the following network servers and devices to support IPv6. For details, refer to your device user documentation:

- Provision a DHCP and DNS server with IPv6 support. The Cisco Network Registrar server supports IPv6 for DHCP and DNS.
- Configure the IOS for network devices such as gateways, routers, and MTPs with IPv6 support.
- Configure your TFTP server to run IPv6.

IPv6 Configuration Task Flow

Complete the following tasks to configure the system for IPv6.

Procedure

	Command or Action	Purpose
Step 1	Configure IPv6 in Operating System, on page 93	Configure the operating system with support for IPv6 addresses.
Step 2	Configure Server for IPv6, on page 93	Configure the servers in your cluster with IPv6 addresses.
Step 3	Enable IPv6, on page 94	Configure enterprise parameters that enable the system for IPv6.
Step 4	Perform any of the following: • Configure IP Addressing Preference for Cluster, on page 94 • Configure IP Addressing Preferences for Devices, on page 95	You can configure an enterprise parameter to assign a clusterwide IP Addressing preference. If you want to assign different preferences for different groups of endpoints, configure the addressing preference within a Common Device Configuration. Configure cluster settings for which IP addressing method is preferred.
Step 5	Restart Services, on page 96	Restart the following network services: • Cisco CallManager

	Command or Action	Purpose
		- Cisco CTIManager - Cisco IP Voice Media Streaming App - Cisco Certificate Authority Proxy Function

What to do next

To configure dual stack trunks, refer to the chapters for configuring SIP trunks.

To configure dual stack for SIP devices, refer to the sections for the SIP devices that you want to configure.

Configure IPv6 in Operating System

Use this procedure to set up Ethernet IPv6 in Cisco Unified OS Administration.

Note Use Cisco IOS IPv6 DHCP server because the IPv6 DHCP server configuration is not supported on Windows.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Settings** > **IPv6** > **Ethernet**.

Step 2 Check the **Enable IPv6** check box.

Step 3 From the **Address Source** drop-down list box, configure how the system acquires the IPv6 address:

- **Router Advertisement**—The system uses stateless autoconfiguration to acquire an IPv6 address.
- **DHCP**—The system acquires an IPv6 address from a DHCP server.
- **Manual Entry**—Choose this option if you want to enter the IPv6 address manually.

Step 4 If you have configured Manual Entry as the means of acquiring an IPv6 address, complete the following fields:

- Enter an **IPv6 Address**. For example, `fd62:6:96:21e:bff:fecc:2e3a`.
- Enter an **IPv6 Mask**. for example, `64`.

Step 5 Check the **Update with Reboot** check box to ensure that the system reboots after you save.

Step 6 Click **Save**.

Configure Server for IPv6

Configure the servers in your cluster with IPv6 addresses.

Procedure

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

Step 2 In the **IPv6 Address (for dual IPv4/IPv6)** field, enter one of the following values:

- If you have DNS configured, and your DNS server supports IPv6, enter the server hostname.
- Otherwise, enter the non-link local IPv6 address.

Step 3 Click **Save**.

Step 4 Repeat these steps for each cluster node.

Enable IPv6

If you want to set up IPv6 support in your system, you must enable the system to support IPv6 devices.

Procedure

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

Step 2 Set the value of the **Enable IPv6** enterprise parameter to **True**.

Step 3 Click **Save**.

What to do next

Configure IP addressing preferences for the devices in your cluster. You can apply settings via a clusterwide enterprise parameter or you can use a Common Device Configuration to apply settings to a group of devices that uses that configuration:

- Configure IP Addressing Preference for Cluster, on page 94
- Configure IP Addressing Preferences for Devices, on page 95

Configure IP Addressing Preference for Cluster

Use this procedure to use enterprise parameters to configure clusterwide IP addressing preferences for IPv6. The system applies these settings to all SIP trunks and devices unless an overriding Common Device Configuration is applied to a specific trunk or device.

Note The IP address preferences in a Common Device Configuration override the clusterwide enterprise parameter settings for the devices that use that Common Device Configuration.

Procedure

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

Step 2 Set the value of the **IP Addressing Mode Preference for Media** enterprise parameter to **IPv4** or **IPv6**

Step 3 Set the value of the **IP Addressing Mode Preference for Signaling** enterprise parameter to **IPv4** or **IPv6**.

Step 4 Click **Save**.

Configure IP Addressing Preferences for Devices

You can configure IP addressing preferences for individual devices by configuring a Common Device Configuration with the preference settings. You can apply the Common Device Configuration to SIP and SCCP devices that support IPv6 addressing such as trunks, phones, conferences bridges, and transcoders.

Note The IP address preferences in a Common Device Configuration override the clusterwide enterprise parameter settings for the devices that use that Common Device Configuration.

Procedure

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

Step 2 Click **Add New**.

Step 3 For SIP trunks, SIP Phones or SCCP phones, choose a value for the **IP Addressing Mode** drop-down list:

- **IPv4 Only**—The device uses only an IPv4 address for media and signaling.
- **IPv6 Only**—The device uses only an IPv6 address for media and signaling.
- **IPv4 and IPv6 (Default)**—The device is a dual-stack device and uses whichever IP address type is available. If both IP address types are configured on the device, for signaling the device uses the **IP Addressing Mode Preference for Signaling** setting and for media the device uses the **IP Addressing Mode Preference for Media** enterprise parameter setting.

Step 4 If you configure IPv6 in your previous step, then configure an IP addressing preference for the **IP Addressing Mode for Signaling** drop-down list:

- **IPv4**—The dual stack device prefers IPv4 address for signaling.
- **IPv6**—The dual stack device prefers IPv6 address for signaling.
- **Use System Default**—The device uses the setting for the **IP Addressing Mode Preference for Signaling** enterprise parameter.

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

Step 6 Click **Save**.

What to do next

If your IPv6 configuration is complete, Restart Services, on page 96.

If you want your SIP devices to support both IPv4 and IPv6 networks simultaneously, you must configure the system to support both stacks at the device level. For details, see Two Stacks (IPv4 and IPv6) Overview, on page 689.

Restart Services

After configuring your system for IPv6, restart essential services.

Procedure

Step 1 Log into Cisco Unified Serviceability and choose **Tools** > **Control Center - Feature Services**.

Step 2 Check the check box corresponding to each of the following services:

- Cisco CallManager
- Cisco CTIManager
- Cisco Certificate Authority Proxy Function
- Cisco IP Voice Media Streaming App

Step 3 Click **Restart**.

Step 4 Click **OK**.

CHAPTER 14

Configure SIP Trunks

SIP Trunk Overview

If you are deploying SIP for call control signaling, configure SIP trunks that connect Cisco Unified Communications Manager to external devices such as SIP gateways, SIP Proxy Servers, Unified Communications applications, remote clusters, or a Session Management Edition.

Within Cisco Unified CM Administration, the **SIP Trunk Configuration** window contains the SIP signaling configurations that Cisco Unified Communications Manager uses to manage SIP calls.

You can assign up to 16 different destination addresses for a SIP trunk, using IPv4 or IPv6 addressing, fully qualified domain names, or you can use a single DNS SRV record.

You can configure the following features on SIP trunks:

- Line and Name Identification Services
- Delayed Offer, Early Offer and Best Effort Early Offer
- Signaling encryption and authentication
- Media encryption with SRTP
- IPv6 dual stack support
- Video
- Presentation sharing with BFCP
- Far end camera control
- DTMF relay
- Calling party normalization
- URI dialing
- Q.SIG support

- T.38 fax support
- SIP OPTIONS
- Choice of DTMF signaling

Note When Q.SIG is enabled in Small-scale IP telephony (SIPT) from Cluster A to Cluster B, and if "INVITE" is received with anonymous or any text, then the Cisco Unified Communications Manager does not encode it to Q.SIG data. When you decode the same in the leaf cluster, it displays empty and empty number is forwarded.

Note When Q.SIG is enabled, URI dialing does not respond as expected and if Q.SIG is disabled, then the Cisco Call Back does not respond between two clusters.

IPv6 Dual Stack Support

You can also configure your SIP trunks with IPv6 dual stack support by configuring the IP Addressing Mode in a Common Device Configuration and then applying that configuration to the SIP trunk.

Note You can also configure IPv6 clusterwide via a clusterwide service parameter. However, the Common Device Configuration setting overrides the clusterwide defaults.

Secure SIP Trunks

You can also configure your trunks with security such as digest authentication and signaling and media encryption by configuring a SIP trunk security profile that includes security features such as digest authentication and TLS signaling and associate that profile to the SIP trunks in your network. For the trunk to allow encrypted o encrypt call media, you must also configure the trunk to allow SRTP media.

SIP Trunk Security Profile Overview

You must assign a SIP trunk security profile to each SIP trunk in your network. By default, Cisco Unified Communications Manager applies a predefined, nonsecure SIP trunk security profile for autoregistration to all SIP trunks.

The SIP trunk security profile allows you to configure security settings such as digest authentication and TLS signaling encryption for the SIP trunks in your network. When you configure a SIP trunk security profile, and then assign that profile to a SIP trunk, the security settings from the profile get applied to the trunk.

You can configure multiple SIP trunk security profiles to cover the different security requirements that you have for different sets of SIP trunks in your network.

Note To configure your network with security, you must also set up a CTL client and configure IPSec. For details, see the *Security Guide for Cisco Unified Communications Manager*.

SIP Trunk Configuration Prerequisites

Before you configure your SIP trunks, do the following:

- Plan your network topology so that you understand your trunk connections.
- Make sure that you understand the devices to which you want to connect your trunks and how those devices implement SIP. If those devices implement SIP, you may need to apply a SIP normalization script.
- Configure SIP profiles for your trunks.

In addition, configure the following before you configure your SIP trunks:

- SIP Normalization and Transparency Configuration Task Flow, on page 82
- Configure SIP Profiles, on page 89

SIP Trunk Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure SIP Trunk Security Profile, on page 100	Configure SIP trunk security profiles with any security settings that you want to apply to your SIP trunks. For example, you can configure digest authentication, device security mode, and TLS encryption for SIP signaling. If you don't configure SIP trunk security profiles, by default, Cisco Unified Communications Manager applies a nonsecure sip trunk security profile.
Step 2	Configure Common Device Configuration, on page 100	Set up a Common Device Configuration for the trunk. For dual-stack trunks, configure the IP addressing preference.
Step 3	Configure SIP Trunks, on page 101	Configure the SIP trunks in your network. In the **Trunk Configuration** window, configure the SIP settings for your trunks. Assign a SIP profile, SIP trunk security profile, and a Common Device Configuration to your SIP trunk. In addition, assign any SIP normalization or transparency scripts that your trunk connection requires. For example, if your SIP trunk connects to a Cisco TelePresence VCS, you must assign the *vcs-interop* script to the SIP trunk.

Configure SIP Trunk Security Profile

Configure a SIP Trunk Security Profile with security settings such as digest authentication or TLS signaling encryption. When you assign the profile to a SIP trunk, the trunk takes on the settings of the security profile.

Note If you don't assign a SIP trunk security profile to your SIP trunks, Cisco Unified Communications Manager assigns a nonsecure profile by default.

Procedure

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

Step 2 Click **Add New**.

Step 3 To enable SIP signaling encryption with TLS, perform the following:

a) From the **Device Security Mode** drop-down list, select **Encrypted**.

b) From the **Incoming Transport Type** and **Outgoing Transport Type** drop-down lists, choose **TLS**.

c) For device authentication, in the **X.509 Subject Name** field, enter the subject name of the X.509 certificate.

d) In the **Incoming Port** field, enter the port on which you want to receive TLS requests. The default for TLS is 5061.

Step 4 To enable digest authentication, do the following

a) Check the **Enable Digest Authentication** check box

b) Enter a **Nonce Validity Timer** value to indicate the number of seconds that must pass before the system generates a new nonce. The default is 600 (10 minutes).

c) To enable digest authentication for applications, check the **Enable Application Level Authorization** check box.

Step 5 Complete the additional fields in the **SIP Trunk Security Profile Configuration** window.For more information on the fields and their configuration options, see Online Help.

Step 6 Click **Save**.

Note You must assign the profile to a trunk in the **Trunk Configuration** window so that the trunk can uses the settings.

Configure Common Device Configuration

A common device configuration comprises a set of optional set of user-specific feature attributes. If you are deploying IPv6, you can use this configuration to assign IPv6 preferences for SIP trunks or SCCP phones.

Procedure

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

Step 2 Click **Add New**.

Step 3 For SIP trunks, SIP Phones or SCCP phones, choose a value for the **IP Addressing Mode** drop-down list:

- **IPv4 Only**—The device uses only an IPv4 address for media and signaling.
- **IPv6 Only**—The device uses only an IPv6 address for media and signaling.
- **IPv4 and IPv6 (Default)**—The device is a dual-stack device and uses whichever IP address type is available. If both IP address types are configured on the device, for signaling the device uses the **IP Addressing Mode Preference for Signaling** setting and for media the device uses the **IP Addressing Mode Preference for Media** enterprise parameter setting.

Step 4 If you configure IPv6 in your previous step, then configure an IP addressing preference for the **IP Addressing Mode for Signaling** drop-down list:

- **IPv4**—The dual stack device prefers IPv4 address for signaling.
- **IPv6**—The dual stack device prefers IPv6 address for signaling.
- **Use System Default**—The device uses the setting for the **IP Addressing Mode Preference for Signaling** enterprise parameter.

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

Step 6 Click **Save**.

Configure SIP Trunks

Use this procedure to configure a SIP trunk. You can assign up to 16 destination addresses for a SIP trunk.

Procedure

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

Step 2 Click **Add New**.

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

Step 4 From the **Protocol Type** drop-down list, choose the type of SIP trunk that matches your deployment and click **Next**:

- **None (Default)**
- **Call Control Discovery**
- **Extension Mobility Cross Cluster**
- **Cisco Intercompany Media Engine**
- **IP Multimedia System Service Control**

Step 5 (Optional) If you want to apply a **Common Device Configuration** to this trunk, select the configuration from the drop-down list.

Step 6 Check the **SRTP Allowed** check box if you want to allow encypted media over the trunk.

Step 7 Check the **Run on All Active Unified CM Nodes** check box if you want to enable the trunk for all cluster nodes.

Step 8 Configure the destination address for the SIP trunk:

a) In the **Destination Address** text box, enter an IPv4 address, fully qualified domain name, or DNS SRV record for the server or endpoint that you want to connect to the trunk.

b) If the trunk is a dual stack trunk, in the **Destination Address IPv6** text box, enter an IPv6 address, fully qualified domain name, or DNS SRV record for the server or endpoint that you want to connect to the trunk.

c) If the destination is a DNS SRV record, check the **Destination Address is an SRV** check box.

d) To add additional destinations, click the **(+)**.

Step 9 From the **SIP Trunk Security Profile** drop-down, assign a security profile. If you don't select this option, a nonsecure profile will be assigned.

Step 10 From the **SIP Profile** drop-down list, assign a SIP profile.

Step 11 (Optional) If you want to assign a normalization script to this SIP trunk, from the **Normalization Script** drop-down list, select the script that you want to assign.

Step 12 Configure any additional fields in the **Trunk Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 13 Click **Save**.

CHAPTER 15

Configure H.323 Trunks

H.323 Trunk Overview

If you have an H.323 deployment, H.323 trunks provide connectivity to remote clusters and other H.323 devices, such as gateways. H.323 trunks support most of the audio and video codecs that Unified Communications Manager supports for intra-cluster communications, with the exception of wideband audio and wideband video. H.323 trunks use the H.225 protocol for call control signaling and the H.245 protocol for media signaling.

Within Cisco Unified CM Administration, H.323 trunks can be configured using the Inter-cluster Trunk (Non-Gatekeeper Controlled) trunk type and protocol options.

If you have a non-gatekeeper H.323 deployment, you must configure a separate intercluster trunk for each device pool in the remote cluster that the local Unified Communications Manager can call over the IP WAN. The intercluster trunks statically specify either the IPv4 addresses or hostnames of the remote devices.

You can configure up to 16 destination addresses for a single trunk.

Intercluster Trunks

When configuring intercluster trunk connections between two remote clusters, you must configure an intercluster trunk on each cluster and match the trunk configurations so that the destination addresses used by one trunk match the call processing nodes that are used by the trunk from the remote cluster. For example:

- Remote cluster trunk uses Run on all Active Nodes—The remote cluster trunk uses all nodes for call processing and load balancing. In the local intercluster trunk that originates in the local cluster, add in the IP addresses or hostnames for each server in the remote cluster.
- Remote cluster does not use Run on all Active Nodes—The remote cluster trunk uses the servers from the Unified Communications Manager Group that is assigned to the trunk's device pool for call processing and load balancing. In the local intercluster trunk configuration, you must add the IP address or hostname of each node from the Unified Communications Manager group used by the remote cluster trunk's device pool.

Secure Trunks

To configure secure signaling for H.323 trunks, you must configure IPSec on the trunk. For details, see the *Security Guide for Cisco Unified Communications Manager*. To configure the trunk to allow media encryption, check the SRTP allowed check box in the **Trunk Configuration** window.

Note Gatekeepers are no longer widely used, but you can also configure your H.323 deployment to use gatekeeper-controlled trunks. For details on how to set up gatekeeper-controlled trunks, refer to *Cisco Unified Communications Manager Administration Guide,* Release 10.0(1).

H.323 Trunk Prerequisites

Plan out your H.323 deployment topology. For intercluster trunks, make sure you know which servers the corresponding remote cluster trunks use for call processing and load balancing. You will have to configure your local intercluster trunk to connect to each call processing server used by the trunk in the remote cluster.

If you are using Cisco Unified Communications Manager groups assigned to a trunk device pool for load balancing on the trunk, complete the configuration in chapter "Configure Trunks", *Core Settings for Device Pools Configuration Task Flow* section.

Configure H.323 Trunks

Use this procedure to configure trunks for an H.323 deployment.

Procedure

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

Step 2 Click **Add New**.

Step 3 From the **Trunk Type** drop-down list box, choose **Inter-Cluster Trunk (Non-Gatekeeper Controlled)**.

Step 4 From the **Protocol** drop-down list box, choose **Inter-Cluster Trunk**.

Step 5 In the **Device Name** text box, enter the unique identifier for the trunk.

Step 6 From the **Device Pool** drop-down list box, select the device pool that you configured for this trunk.

Step 7 If you want to use every node in the local cluster for processing for this trunk, check the **Run on all Active Unified CM Nodes** check box.

Step 8 If you want to allow encrypted media across the trunk, check the **SRTP Allowed** check box.

Step 9 If you want to configure H.235 pass through, check the **H.235 Pass Through Allowed** check box.

Step 10 In the **Remote Cisco Unified Communications Manager Information** section, enter an IP address or hostname for each remote server to which this trunk connects.

CHAPTER 16

Configure SRST

Survivable Remote Site Telephony Overview

Survivable Remote Site Telephony (SRST) is an optional feature for sites that depend on a Wide Area Network (WAN) connection to aUnified Communications Manager node. SRST references, which are configured in theUnified Communications Manager Administration interface, allow IP gateways to provide limited telephony service to IP phones at the remote site in the event of a WAN outage:

- IP phones at the remote site can call each other
- calls from the PSTN can reach the IP phones
- calls from the IP phones can reach the external world through the PSTN

When phones at the remote site lose connectivity to all associatedUnified Communications Manager nodes, the phones connect to the SRST reference IP gateway. The status line indication on the IP phone shows the phone has failed over to the backup SRST gateway. When the connection toUnified Communications Manager is restored, the IP phones reregister withUnified Communications Manager and full telephony services are restored.

SRST supports remote sites that may have a mix of SCCP and SIP endpoints in addition to PSTN gateway access.

Connection Monitor Duration

An IP phone that connects to an SRST gateway over a Wide Area Network (WAN) reconnects itself to Unified Communications Manager as soon as it can establish a connection withUnified Communications Manager over the WAN link. However, if the WAN link is unstable, the IP phone switches back and forth between the SRST gateway andUnified Communications Manager. This situation causes temporary loss of phone service (no dial tone). These reconnect attempts, known as WAN link flapping issues, continue until the IP phone successfully reconnects itself toUnified Communications Manager.

To resolve the WAN link flapping issues betweenUnified Communications Manager and an SRST gateway, you can define the number of seconds (Connection Monitor Duration) that the IP Phone monitors its connection toUnified Communications Manager before it unregisters from the SRST gateway and reregisters toUnified

Communications Manager. The IP phone receives the connection monitor duration value in the XML configuration file.

Survivable Remote Site Telephony Configuration Task Flow

Before you begin

Examine the dial plan. If there are 7 or 8 digits in the dial plan, you may need to configure translation rules. For more information about translation rules, see Configure Translation Patterns, on page 160.

Procedure

	Command or Action	Purpose
Step 1	Configure an SRST Reference, on page 106	Configure the gateway that can provide limited call control functionality when all other Unified Communications Manager nodes are unreachable.
Step 2	Assign the SRST Reference to a Device Pool, on page 107	For each device pool, assign the gateways that calling devices search when they attempt to complete a call if Unified Communications Manager is unavailable.
Step 3	Perform one of the following tasks: • Configure Connection Monitor Duration for the Cluster, on page 107 • Configure Connection Monitor Duration for a Device Pool, on page 108	**Optional**: Configure the connection monitor duration. You can apply a cluster-wide default value, or apply the configuration to the devices in a device pool.
Step 4	Enable SRST on the SRST Gateway, on page 108	Configure SRST parameters on the gateway.

Configure an SRST Reference

An SRST reference comprises the gateway that can provide limited Cisco Unified Communications Manager functionality when all other Cisco Unified Communications Manager nodes for a device are unreachable.

Procedure

Step 1 Log into Cisco Unified CM Administration and choose **System** > **SRST**.

Step 2 Click **Add New**.

Step 3 Configure the fields in the **SRST Reference Configuration** window. For more information on the fields and their configuration options, see the system Online Help.

Step 4 Click **Save**.

Assign the SRST Reference to a Device Pool

You can configure SRST for each device pool of phones. When you assign an SRST reference to a device pool, all phones in the device pool try to connect to the assigned SRST gateway if they cannot reach any Cisco Unified Communications Manager node.

Procedure

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

Step 2 Click **Find** and choose the device pool to which the remote IP phones are registered.

Step 3 In the Roaming Sensitive Settings area, choose the SRST reference from the **SRST Reference** drop-down list.

The **SRST Reference** drop-down list contains the following options:

- **Disable**—If a phone cannot reach any Cisco Unified Communications Manager node, it does not try to connect to an SRST gateway.
- **Use Default Gateway**—If a phone cannot reach any Cisco Unified Communications Manager node, it tries to connect to its IP gateway as an SRST gateway.
- **User-Defined**—If a phone cannot reach any Cisco Unified Communications Manager node, it tries to connect to this SRST gateway.

Step 4 Click **Save**.

Configure Connection Monitor Duration for the Cluster

This procedure is optional. Complete this procedure only if you want to change the system value (enterprise parameter) for the connection monitor duration.

Procedure

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

Step 2 Enter a value in the **Connection Monitor Duration** field. The default value is 120 seconds. The maximum number of seconds that you can enter in the field is 2592000.

Step 3 Click **Save**.

Note You must restart all services for the change to take effect.

The enterprise parameter forms the cluster default for the Connection Monitor Duration. However, if an overriding configuration exists within a device pool, that setting overrides the enterprise parameter setting for the devices that use the device pool.

Configure Connection Monitor Duration for a Device Pool

This procedure is optional. Complete this procedure only if the following is true:

- You do not want to use the cluster-wide value for the connection monitor duration.
- You want to define a separate connection monitor duration value for this device pool.

Tip When you change the value of the connection monitor duration for a device pool, 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 cluster-wide value that is configured in the Connection Monitor Duration enterprise parameter.

Procedure

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

Step 2 Click **Find** and choose the device pool to which the remote IP phones are registered.

Step 3 In the Roaming Sensitive Settings area, enter a value in the **Connection Monitor Duration** field. The maximum number of seconds that you can enter in the field is 2592000.

Note This setting overrides the enterprise parameter setting for connection monitor duration.

Step 4 Click **Save**.

Enable SRST on the SRST Gateway

Before you begin

- Assign the SRST Reference to a Device Pool, on page 107
- (Optional) Perform one of the following tasks:
  - Configure Connection Monitor Duration for the Cluster, on page 107
  - Configure Connection Monitor Duration for a Device Pool, on page 108

Procedure

Step 1 Log into the SRST gateway (router).

Step 2 Enter the command **call-manager-fallback**
This command enables SRST on the router.

Step 3 Enter the command **max-ephones** max-phones, where max-phones is the maximum number of supported Cisco IP phones.

Step 4 Enter the command **max-dn** max-directory-numbers where max-directory-numbers is the maximum number of directory numbers (DN) or virtual voice ports that can be supported by a router.

Step 5 Enter the command **ip source-address** ip-address where ip-address is a preexisting router IP address, typically one of the addresses of the Ethernet port of the router.
This command enables the SRST router to receive messages from Cisco IP Phones through the specified IP address.

SRST Restrictions

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

PART III

Configure the Dial Plan

CHAPTER 17

Dial Plan Overview

About the Dial Plan

The dial plan is responsible for instructing the Cisco Unified Communications Manager system about how to route calls. When you configure a dial plan, you define such rules as:

- the type of calls that are allowed
- the preferred path that the system uses to place a call, as well as alternate paths
- how extensions are dialed
- how called and calling numbers are presented

Dial Plan Prerequisites

Before you configure the dial plan, complete these tasks:

- Initial Configuration Task Flow, on page 5
- Inbound and Outbound Calling Configuration, on page 63

Dial Plan Configuration

Complete the following task flows to configure the dial plan for your system.

Procedure

	Command or Action	Purpose
Step 1	Partition Configuration Task Flow, on page 119	Configure partitions to create a logical grouping of directory numbers (DNs) and route

	Command or Action	Purpose
		patterns with similar reachability characteristics. Partitions facilitate call routing by dividing the route plan into logical subsets that are based on organization, location, and call type.
Step 2	National Numbering Plan Installation Task Flow, on page 124	Optional. Cisco Unified Communications Manager provides a default North American Numbering Plan (NANP). For countries with different dial plan requirements, you can install a Cisco International Dial Plan and use it to create a unique numbering plan that is specific to your requirements. When you use a national numbering plan, you can configure route patterns that use the @ symbol, along with route filters, to create patterns for local, national, long distance, and emergency calling. Using a national numbering dial plan is optional. If you do not use a national numbering plan, you can configure one manually.
Step 3	Call Routing Configuration Task Flow, on page 128	Configure a route plan to route internal calls and external calls to a private network or the public switched telephone network (PSTN).
Step 4	Hunt Pilot Configuration Task Flow, on page 151	Configure a hunt pilot when you want to extend a call to one or more lists of numbers, where each list specifies a hunting order. When a call extends to a hunt party from these lists and the party fails to answer or is busy, hunting resumes with the next hunt party.
Step 5	Translation Pattern Configuration Task Flow, on page 160	Configure translation patterns to manipulate inbound numbers from your voice gateway to the Cisco Unified Communications Manager. You can use translation patterns to change the calling and called number before the system forwards the call to the receiving endpoint. This translation is transparent and allows you to map extensions from the public to the private network.
Step 6	Transformation Pattern Configuration Task Flow, on page 161	Configure transformation patterns for phones when you want to modify the calling number display on an inbound call. Configure transformation patterns for gateways or trunks when you want to modify the outgoing calling or called number display sent out for outbound calls. You can also use transformation patterns

	Command or Action	Purpose
		to modify the outbound redirecting number (known as a diversion header in SIP devices).
Step 7	Dial Rules Configuration Task Flow, on page 166	You can configure different types of dial rules: application dial rules, directory lookup dial rules, and SIP dial rules. • Configure application dial rules to add and sort the priority of dialing rules for applications such as Cisco Web Dialer and Cisco Unified Communications Manager Assistant. • Configure directory lookup dial rules to transform caller identification numbers into numbers that can be looked up in the directory. • Configure the SIP Dial Rules to create dial patterns for phones that are running SIP. This procedure is typically for legacy SIP phones.
Step 8	ILS Configuration Task Flow, on page 174	Configure Intercluster Lookup Service (ILS) to create networks of remote Cisco Unified Communications Manager clusters. You can configure ILS on a pair of clusters and then join those clusters to form an ILS network.
Step 9	Global Dial Plan Replication Task Flow, on page 188	If you have configured an Intercluster Lookup Service (ILS) network, you can configure global dial plan replication to create a global dial plan that spans across the ILS network and includes intercluster dialing of directory URIs and alternate numbers.
Step 10	URI Dialing Configuration Task Flow, on page 197	Configure URI dialing when you want to route calls to an endpoint using the directory URI as the call address. The directory URI follows the username@host format, where the host portion is an IPv4 address or a fully qualified domain name.

CHAPTER 18

Configure Partitions

Partitions Overview

Partitions are logical groups of any of the following:

- Route patterns
- Directory numbers (DNs)
- Translation patterns
- Transformation patterns
- Universal resource indicators (URIs)
- Hunt pilots

Partitions facilitate call routing by dividing the route plan into logical subsets that are based on similar accessibility requirements, organization, location, and call type.

Calling Search Space Overview

A Calling Search Space (CSS) is a prioritized list of partitions. Calling Search Spaces determine the call destinations that are available for a caller to call. The call destination must be in a partition that is available to the caller's calling search space, or the caller cannot call that destination. You can assign calling search spaces to directory numbers and to devices such as phones and gateways.

If a calling search space is assigned both to the caller's phone and to the caller's directory number, the system concatenates the two to provide the CSS for the caller.

You can use partitions and calling search spaces to organize your system according to call privileges. For example, you could:

- Limit some employees from placing long-distance calls
- Limit a lobby phone from place a direct call to the CEO

Class of Service

You can use partitions and calling search spaces (CSS) to configure classes of service. The table below provides an example of partitions and calling search spaces that you can create for classes of service that provide PSTN access to:

- Emergency calls
- Local calls
- National calls
- International dialing

Table 7: Examples of Partitions and Calling Search Spaces

Calling Search Space	Route Partition 1	Route Partition 2	Route Partition 3	Capabilities
Base_CSS	Base_PT	—	—	• Emergency • On-net
LocalPSTN_CSS	PSTN_Local_PT	—	—	• Emergency • On-net • Local
NationalPSTN_CSS	PSTN_Local_PT	PSTN_National_PT	—	• Emergency • On-net • Local • National
InternationalPSTN_CSS	PSTN_Local_PT	PSTN_National_PT	PSTN_Intl_PT	• Emergency • On-net • Local • National • International

Devices automatically register with a calling search space such as Base_CSS. This allows all devices to dial both on-net and emergency off-net numbers. You must assign the remaining calling search spaces to the directory number on the user device profile to provide local 7-digit or local 10-digit, national, and international dialing capabilities.

Partition Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure Partitions, on page 119	Configure partitions to create a logical groupings of system resources with similar reachability characteristics.
Step 2	Configure Calling Search Spaces, on page 120	Configure the partitions that calling devices search when they are attempting to complete a call.

Configure Partitions

Configure partitions to create a logical group of system resources with similar reachability characteristics. You can create partitions for any of the following:

- Route patterns
- Directory numbers (DNs)
- Translation patterns
- Transformation patterns
- Universal resource indicators (URIs)
- Hunt pilots

Partitions facilitate call routing by dividing the route plan into logical subsets that are based on organization, location, and call type. You can configure multiple partitions.

Procedure

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

Step 2 Click **Add New** to create a new partition.

Step 3 In the **Partition Name, Description** field, enter a name for the partition that is unique to the route plan.

Partition names can contain alphanumeric characters, as well as spaces, hyphens (-), and underscore characters (_). See the online help for guidelines about partition names.

Step 4 Enter a comma (,) after the partition name and enter a description of the partition on the same line.

The description can contain up to 50 characters in any language, but it cannot include double quotes ("), percentage sign (%), ampersand (&), backslash (\), angle brackets (<>), or square brackets ([ ]).

If you do not enter a description, Cisco Unified Communications Manager automatically enters the partition name in this field.

Step 5 To create multiple partitions, use one line for each partition entry.

Step 6 From the **Time Schedule** drop-down list, choose a time schedule to associate with this partition.

The time schedule specifies when the partition is available to receive incoming calls. If you choose **None**, the partition remains active at all times.

Step 7 Select one of the following radio buttons to configure the **Time Zone**:

- **Originating Device**—When you select this radio button, the system compares the time zone of the calling device to the **Time Schedule** to determine whether the partition is available is available to receive an incoming call.
- **Specific Time Zone**—After you select this radio button, choose a time zone from the drop-down list. The system compares the chosen time zone to the **Time Schedule** to determine whether the partition is available is available to receive an incoming call.

Step 8 Click **Save**.

Partition Name Guidelines

The list of partitions in a calling search space is limited to a maximum of 1024 characters. This means that the maximum number of partitions in a CSS varies depending on the length of the partition names. Use the following table to determine the maximum number of partitions that you can add to a calling search space if partition names are of fixed length.

Table 8: Partition Name Guidelines

Partition Name Length	Maximum Number of Partitions
2 characters	340
3 characters	256
4 characters	204
5 characters	172
...	...
10 characters	92
15 characters	64

Configure Calling Search Spaces

A calling search space is an ordered list of route partitions that are typically assigned to devices. Calling search spaces determine the partitions that calling devices can search when they are attempting to complete a call.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **Calling Search Space**.

Step 2 Click **Add New**.

Step 3 In the **Name** field, enter a name.

Ensure that each calling search space name is unique to the system. The name can include up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_).

Step 4 In the **Description** field, enter a description.

The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).

Step 5 From the **Available Partitions** drop-down list, perform one of the following steps:

- For a single partition, select that partition.
- For multiple partitions, hold down the **Control (CTRL)** key, then select the appropriate partitions.

Step 6 Select the down arrow between the boxes to move the partitions to the **Selected Partitions** field.

Step 7 (Optional) Change the priority of selected partitions by using the arrow keys to the right of the **Selected Partitions** box.

Step 8 Click **Save**.

Partition Interactions and Restrictions

Table 9: Partition Restrictions

Function or Action	Restriction
Delete a Partition	Ensure that you complete one of the following tasks, before you delete a partition: • 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. Check carefully to ensure that you are deleting the correct partition, because you cannot retrieve deleted partitions. If you accidentally delete a partition, you must rebuild it.
Translation Patterns	A translation pattern contains digit manipulations and is assigned to a partition. When a call matches the translation pattern, Unified CM performs the translation and then reroutes the call using the calling search space that the translation pattern specifies. For details on translation patterns, see the Configure Call Routing chapter.
Time of Day Routing	Configure a schedule for when a partition is available to accept incoming calls. For details on configuring time of day routing, see the Configure Call Routing chapter.
Logical Partitioning	**Optional**: Allows you split your internal VoIP network from your external network with gateway and trunk access. Logical partitioning is optional for most deployments, but is mandatory in countries such as India where regulations mandate that all calls that leave the internal network go to a local PSTN gateway. For details on Configuring Logical Partitioning, refer to the "*Configure Logical Partitioning*" section in the *Feature Configuration Guide for Cisco Unified Communications Manager*.

CHAPTER 19

Install a National Numbering Plan

National Numbering Plan Overview

Unified Communications Manager provides a default North American Numbering Plan (NANP). For countries with different dial plan requirements, you can install a Cisco International Dial Plan and use it to create a unique numbering plan that is specific to your requirements.

The numbering plan contains the Discard Digits Instructions (DDIs) and tags specific to that numbering plan. You can use these items when configuring call routing to create routing rules that are applicable to the numbering plan.

This chapter describes how to install a National Numbering Plan. For more information about using a national numbering plan, see the *Unified Communications Manager Dial Plan Deployment Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

National Numbering Plan Prerequisites

If you are installing a National Numbering Plan for countries outside of North America, download the Cisco Option Package (COP) file that contains the international dial plans for the current release. The COP file uses the naming convention IDP v.*x*, and is available from the Cisco website:

- https://software.cisco.com/download/navigator.html

Place the file on an external FTP or SFTP server that Unified Communications Manager can access.

National Numbering Plan Installation Task Flow

Procedure

	Command or Action	Purpose
Step 1	Install the COP file, on page 124	**Optional**. To install a numbering plan for countries outside of North America, download the Cisco Option Package (COP) file that contains the international dial plans for the current release.
Step 2	Install a National Numbering Plan, on page 125	Install the national numbering plan on each Unified Communications Manager node in the cluster. Perform this procedure only if you are installing a National Numbering Plan for countries outside of North America.
Step 3	Restart the CallManager Service, on page 125	The changes take effect after you restart the service.

Install the COP file

Use this procedure to install a Cisco Option Package (COP) file that contains international dial plans.

Procedure

Step 1 Begin this procedure on the Unified Communications Manager publisher node. From Cisco Unified Communications OS Administration, choose **Software Upgrades** > **Install**.
The **Software Installation/Upgrade** window appears.

Step 2 In the **Source** field, choose **Remote File System**.

Step 3 Configure the fields on the **Software Installation/Upgrade** window. See the Related Topics for more information about the fields and their configuration options.

Step 4 Click **Next**.
The window refreshes with a list of available software options and upgrades.

Step 5 From the **Options/Upgrades** drop-down list, choose the **DP COP** file and click **Next**.
The **Installation File** window opens and downloads the file from the FTP server. The window displays the progress of the download.

Step 6 When the **Checksum** window appears, verify the checksum value against the checksum for the file that you downloaded.

Step 7 Click **Next** to proceed with the software upgrade.
A warning message displays the DP COP file that you selected to install.

Step 8 Click **Install**.
The **Install Status** window appears.

Step 9 Click **Finish**.

Step 10 Repeat this procedure on the Unified Communications Manager subscriber nodes. You must install the COP file on all the nodes in the cluster.

Related Topics

COP File Installation Fields, on page 125

COP File Installation Fields

Field	Description
Directory	Enter the directory where the COP file is located.
Remote Server	Enter the host name or IP address of the server where COP file is located.
Remote User	Enter the user name for the remote server.
Remote Password	Enter the password for the remote server.
Transfer Protocol	Select a protocol to use when connecting with the remote server.

Install a National Numbering Plan

Perform this procedure only if you are installing a national numbering plan for countries outside of North America.

Install the national numbering plan on each Unified Communications Manager node in the cluster. Begin with the Unified Communications Manager publisher node.

Procedure

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

Step 2 Enter search criteria and click **Find**.

Step 3 Choose the dial plan version that you want to install from the **Available Version** drop-down list.

Step 4 Click **Install**.
The Status displays that the dial plan has been installed.

Step 5 Repeat this procedure for every subscriber node in the cluster.

Restart the CallManager Service

Procedure

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

Step 2 Choose the Unified Communications Manager server from the **Servers** drop-down list.
In the CM Services area, Cisco CallManager displays in the **Service Name** column.

Step 3 Click the radio button that corresponds to the Cisco CallManager service.

Step 4 Click **Restart**.

The service restarts and displays the message, `Service Successfully Restarted`.

CHAPTER 20

Configure Call Routing

Call Routing Overview

The system uses route plans to determine how to route calls between clusters, and how to route external calls to a private network or to the Public Switched Telephone Network (PSTN). The route plan that you configure specifies the path that the system uses to route each type of call. For example, you can create a route plan that uses the IP network for on-net calls, or that uses one carrier for local PSTN calls and another for international calls.

The system has a three-tiered approach to route planning that uses the following components:

- Route Patterns—The system searches for a configured route pattern that matches the external dialed string and uses it to select a gateway or a corresponding route list.
- Route Lists—A prioritized list of the available paths for the call.
- Route Groups—The available paths; the route group distributes the call to gateways and trunks.

In addition to these building blocks, the route plan can also include the following components:

- Local Route Groups—Decouple the location of a PSTN gateway from the route patterns that are used to access the gateway.
- Route Filters—Restrict certain numbers that are otherwise allowed by the route pattern.
- Automated Alternate Routing—Automatically reroute calls through the PSTN or other network when the system blocks a call due to insufficient bandwidth.
- Time-of-day Routing—Create a time schedule that specifies when a partition is available to receive incoming calls.

Call Routing Prerequisites

- Complete the tasks in the Partition Configuration Task Flow, on page 119.
- Ensure that you have the following information:
  - Internal number extensions
  - A plan listing the calls that route to each gateway

Call Routing Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure Local Route Groups, on page 129	**Optional**. Configure local route groups to reduce the number of route lists that you need. Route lists point to the PSTN gateway that the system uses to route the call, based on the location of the PSTN gateway. As an alternative, you can use local route groups to decouple the location of a PSTN gateway from the route patterns that are used to access the gateway. This configuration allows phones and other devices from different locations to use a single set of route patterns, while Unified Communication Manager selects the correct gateway to route the call.
Step 2	Configure Route Groups, on page 131	**Optional**. Configure route groups to set the selection order of the gateway devices. Route groups contain one or more devices.
Step 3	Configure Route Lists, on page 131	**Optional**. Route lists contain one or more route groups. Configure route lists to control the selection order of the route groups. If you configure a route list, you must configure at least one route group.
Step 4	Configure Route Filters, on page 132	**Optional**. Use route filters to restrict certain numbers that are otherwise allowed by a route pattern. Route filters are mandatory if you are using a dial plan installer; that is, if you install a dial plan file and then configure a route pattern based on that numbering plan. Route filters are optional if you are configuring a dial plan manually.

	Command or Action	Purpose
		If you are configuring a dial plan manually, you need to configure route filters whenever you have a route pattern that contains the @ wildcard. When the route pattern contains the @ wildcard, the system routes calls according to the numbering plan that you specify with a route filter.
Step 5	Configure Route Patterns, on page 135	Configure route patterns to direct calls to specific devices and to include or exclude specific digit patterns. You can assign route patterns to gateways, to trunks, or to a route list that contains one or more route groups.
Step 6	Configure Time of Day Routing, on page 139	**Optional**. Create a time schedule that specifies when a partition is available to receive incoming calls.

Configure Local Route Groups

Optional. You can configure local route groups to reduce the number of route lists that you need. Route lists point to the PSTN gateway that the system uses to route the call, based on the location of the PSTN gateway. As an alternative, you can use local route groups to decouple the location of a PSTN gateway from the route patterns that are used to access the gateway. This configuration allows phones and other devices from different locations to use a single set of route patterns, while Cisco Unified Communication Manager selects the correct gateway to route the call.

For example, a local route group allows you to have a single dial plan for a whole country rather than have separate dial plans for every city in the country. This approach works for centralized call-deployment scenarios only.

Procedure

	Command or Action	Purpose
Step 1	Configure Local Route Group Names, on page 130	**Optional**. The system provides a default local route group called Standard Local Route Group, but you can configure additional local route groups. Use this procedure to name the additional local route groups.
Step 2	Associate a Local Route Group with a Device Pool, on page 130	To ensure that each device in the system is provisioned to know its local route group, associate the local route group with a device pool.
Step 3	Add Local Route Group to a Route List, on page 130	**Optional**. Configure a local route group that you can add to your route list. When you create a local route group, the system routes outgoing calls to the gateways that are defined for the user at the device pool level.

Configure Local Route Group Names

Optional. The system provides a default local route group called Standard Local Route Group, but you can configure additional local route groups. Use this procedure to name the additional local route groups.

Procedure

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

Step 2 Click **Add Row**.

Step 3 Enter a name and description for the new local route group.

Step 4 Click **Save**.

Associate a Local Route Group with a Device Pool

You can assign a local route group to use an existing route group, based on the device pool setting of the originating device. This configuration allows phones and other devices from different locations to use a single set of route patterns, while Unified Communications Manager selects the correct gateway to route the call.

To ensure that each device in the system is provisioned to know its local route group, associate the local route group with a device pool.

Procedure

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

Step 2 Enter search criteria, click **Find**, and select a device pool from the resulting list.

Step 3 In the **Local Route Group Settings** area, select a route group from the **Standard Local Route Group** drop-down list.

Step 4 Click **Save**.

Add Local Route Group to a Route List

Configure a local route group that you can add to your route list. When you create a local route group, the system routes outgoing calls to the gateways that are defined for the user at the device pool level.

Procedure

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

Step 2 Choose one of the following options:

- Click **Add New** button to add a new route list.
- Click **Find** and select a route list from the resulting list, to modify the settings for an existing route list.

The **Route List Configuration** window appears.

Step 3 To add a local route group to the route list, click the **Add Route Group** button.

Step 4 From the **Route Group** drop-down list, select a local route group to add to the route list. You can add the standard local route group, or you can add a custom local route group that you have created.

Step 5 Click **Save**.

Step 6 Click **Apply Config**.

Configure Route Groups

Configure a route group to prioritize the order in which the system selects gateways for outgoing calls. Use this procedure to group together gateways that have similar characteristics, so that any gateway in the group can dial the call. The system selects the gateway to use based on the order that you specify when you configure the route group.

You can assign a device to multiple route groups.

Procedure

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

The **Route Group Configuration** window appears.

Step 2 Choose one of the following options:

- Click **Add New**, to add a new route group.
- Click **Find** and choose a route group from the resulting list, to modify the settings for an existing route group.

The **Route Group Configuration** window appears.

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

Step 4 Click **Save**.

Configure Route Lists

Configure a route list to identify a set of route groups and place them in priority order. Unified Communications Manager uses the order in the route list to search for available devices for outgoing calls.

If you configure a route list, you must configure at least one route group. A route list can contain only route groups and local route groups.

Note When an outbound call is sent through a route list, the route list process locks the outbound device to prevent sending an alert message before the call is completed. After the outbound device is locked, the Hunt List stops hunting down the incoming calls.

Procedure

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

Step 2 Choose one of the following options:

- Click **Add New**, to add a new route list.
- Click **Find** and select a route list from the resulting list, to modify the settings for an existing route list.

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

Step 4 To add a route group to the route list, click the **Add Route Group** button.

Step 5 From the **Route Group** drop-down list, choose a route group to add to the route list.

Step 6 Click **Save**.

Step 7 Click **Apply Config**.

Configure Route Filters

Route filters use dialed-digit strings to determine how a call is handled. Route filters apply only when you configure a route pattern that contains the @ wildcard. When the route pattern contains the @ wildcard, Unified Communications Manager routes calls according to the numbering plan that you specify in this procedure.

Route filters are mandatory if you are using a dial plan installer; that is, if you install a dial plan file and then configure a route pattern based on that numbering plan. Route plans are optional when configuring dial plans manually.

If you are configuring a dial plan manually, you need to configure route filters whenever you have a route pattern that contains the @ wildcard. When the route pattern contains the @ wildcard, the system routes calls according to the numbering plan that you specify with a route filter.

Note When configuring your call routing, ensure that you do not assign a single route filter to many route patterns. A system core could result if you were to edit a route filter that has hundreds of associated route patterns. This is due to the extra system processing that is required to update call routing for all of the route patterns that use the route filter. Create duplicate route filters and associate any single route filter with no more than 250 Route Patterns.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing > Route Filter**.

Step 2 From the **Numbering Plan** drop-down list, choose a dial plan and click **Next**.

Step 3 Enter a name in the **Route Filter Name** field.

Ensure each route filter name is unique to the route plan.

Step 4 Choose the route filter tags and operators and enter the data to create a clause for this route filter.

For more information about available route filter tags, see Route Filter Tags, on page 133.

Note Do not enter route filter tag values for tags that are using the operators EXISTS, DOES-NOT-EXIST, or NOT-SELECTED.

Step 5 Choose the route filter operators and enter data, where appropriate, to create a clause for this route filter.

For more inforation about available route filter operators, see Route Filter Operators, on page 134.

Step 6 Click **Save**.

Step 7 Click **Apply Config**.

Route Filter Settings

Route filtering is the process where certain routes are not considered for inclusion in the local route database. It is applied only when a route pattern is configured.

The following topics list the information on route filter preferences.

- Route Filter Tags, on page 133
- Route Filter Operators, on page 134
- Route Filter Examples , on page 135

Route Filter Tags

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. The descriptions in the following table use the notations [2-9] and XXXX to represent actual digits. In this notation, [2-9] represents any single digit in the range 2 through 9, and X represents any single digit in the range 0 through 9. Therefore, the three-digit area code in the form [2-9]XX means that you can enter the actual digits 200 through 999, or all wildcards, or any mixture of actual digits and wildcards that results in a pattern with that range.

Route filter tags vary depending on the numbering plan that you choose from the Numbering Plan drop-down list box on the Route Filter Configuration window. The following table describes the route filter tags for the North American Numbering Plan.

Table 10: 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.

Tag	Description
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.
TRANSIT-NETWORK	This four-digit value identifies a long-distance carrier. Do not include the leading 101 carrier access code prefix in the TRANSIT-NETWORK value. See TRANSIT-NETWORK-ESCAPE for more information.
TRANSIT-NETWORK-ESCAPE	This three-digit value precedes the long-distance carrier identifier. The value for this field specifies 101. Do not include the four-digit carrier identification code in the TRANSIT-NETWORK-ESCAPE value. See TRANSIT-NETWORK for more information.

Route Filter Operators

Route filter tag operators determine whether a call is filtered based on the dialed-digit string that is associated with that tag. The operators EXISTS and DOES-NOT-EXIST simply check for the existence of that part of the dialed-digit string. The operator == matches the actual dialed digits with the specified value or pattern. The following table describes the operators that you can use with route filter tags.

Table 11: 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.

Route Filter Examples

Example 1: A route filter that uses AREA-CODE and the operator DOES-NOT-EXIST selects all dialed-digit strings that do not include an area code.

Example 2: A route filter that uses AREA-CODE, the operator ==, and the entry 515 selects all dialed-digit strings that include the 515 area code.

Example 3: A route filter that uses AREA-CODE, the operator ==, and the entry 5[2-9]X selects all dialed-digit strings that include area codes in the range of 520 through 599.

Example 4: A route filter that uses TRANSIT-NETWORK, the operator ==, and the entry 0288 selects all dialed-digit strings with the carrier access code 1010288.

Configure Route Patterns

Unified Communications Manager uses route patterns to route or block internal and external calls. You can assign route patterns to gateways, to trunks, or to a route list that contains one or more route groups.

Note Although the route pattern can point directly to a gateway, we recommend that you configure route lists and route groups. This approach provides the greatest flexibility in call routing and scalability.

If a route pattern is assigned directly to a gateway or trunk, then the gateway or trunk is not available for association to a route group. Similarly, a gateway or trunk that is already a member of a Route List is not available for association to a route pattern.

Procedure

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

Step 2 Perform one of the following:

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

The **Route Pattern Configuration** Window appears.

Step 3 In the **Route Pattern** field, enter the number pattern that the dial string must match.

Step 4 From the **Gateway/Route** drop-down list, select the destination where you want to send calls that match this route pattern.

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

Step 6 Click **Save**.

Route Patterns Settings

You can create different route patterns that comprises a string of digits (an address) and a set of associated digit(s) to enable Unified CM to manipulate that route calls to a route list or a gateway.

The following are the examples of the type of route pattern that you want to configure:

- Wildcards and Special Characters in Route Patterns, on page 136
- Example of Pre-dot Digit Removal, on page 138
- Example of Digit Prefixing, on page 139
- Example of On-Net and Off-Net Patterns, on page 139
- Example of Block and Route Patterns, on page 139

Wildcards and Special Characters in Route Patterns

Wildcards and special characters in route patterns allow a single route pattern to match a range of numbers (addresses). Use these wildcards and special characters also to build instructions that enable the Unified Communications Manager to manipulate a number before sending it to an adjacent system.

The following table describes the wildcards and special characters that Unified Communications Manager supports.

Table 12: Wildcards and Special Characters

Character	Description	Examples
@	The at symbol (@) wildcard matches all National Numbering Plan numbers. Each route pattern can have only one @ wildcard.	The route pattern 9.@ routes or blocks all numbers that the National Numbering Plan recognizes. The following route patterns examples show National Numbering Plan numbers that the @ wildcard encompasses: • 0 • 1411 • 19725551234 • 101028819725551234 • 01133123456789
X	The X wildcard matches any single digit in the range 0 through 9.	The route pattern 9XXX routes or blocks all numbers in the range 9000 through 9999.
!	The exclamation point (!) wildcard matches one or more digits in the range 0 through 9.	The route pattern 91! routes or blocks all numbers in the range 910 through 91999999999999999999999.
?	The question mark (?) wildcard matches zero or more occurrences of the preceding digit or wildcard value. **Note** If the question mark (??) wildcard is used, the second question mark does not match the empty input. Example router pattern: *33X?*X?*X?#	The route pattern 91X? routes or blocks all numbers in the range 91 through 91999999999999999999999.
+	The plus sign (+) wildcard matches one or more occurrences of the preceding digit or wildcard value.	The route pattern 91X+ routes or blocks all numbers in the range 910 through 91999999999999999999999.
[ ]	The square bracket ([ ]) characters enclose a range of values.	The route pattern 813510[012345] routes or blocks all numbers in the range 8135100 through 8135105.
-	The hyphen (-) character, used with the square brackets, denotes a range of values.	The route pattern 813510[0-5] routes or blocks all numbers in the range 8135100 through 8135105.

Character	Description	Examples
^	The circumflex (^) character, used with the square brackets, negates a range of values. Ensure that it is the first character following the opening bracket ([). Each route pattern can have only one ^ character.	The route pattern 813510[^0-5] routes or blocks all numbers in the range 8135106 through 8135109.
.	The dot (.) character, used as a delimiter, separates the Cisco Unified Communications Manager access code from the directory number. Use this special character, with the discard digits instructions, to strip off the Cisco Unified Communications Manager access code before sending the number to an adjacent system. Each route pattern can have only one dot (.) character.	The route pattern 9.@ identifies the initial 9 as the Cisco Unified Communications Manager access code in a National Numbering Plan call.
*	The asterisk (*) character can provide an extra digit for special dialed numbers.	You can configure the route pattern *411 to provide access to the internal operator for directory assistance.
#	The octothorpe (#) character generally identifies the end of the dialing sequence. Ensure the # character is the last character in the pattern.	The route pattern 901181910555# routes or blocks an international number that is dialed from within the National Numbering Plan. The # character after the last 5 identifies this digit as the last digit in the sequence.
\+	A plus sign preceded by a backslash, that is, \+, indicates that you want to configure the international escape character +.	Using \+ means that the international escape character + is used as a dialable digit, not as a wildcard.

Example of Pre-dot Digit Removal

One example of using pre-dot digit removal in a route pattern is when you want the phone users to dial an access code to reach an outside line. In North America, users typically dial 9 to access an outside line. You can specify using the following route patterns:

- Local calls: `9.@` or `9.[2-9]XXXXXX`
- National calls: `9.1[2-9]XX`
- International calls: `9.011!#`

In these patterns, 9 is the access code for an external line, and the dot (.) is a separator that helps format the route pattern by indicating which digits are internal to the network, and which ones are outside digits. When the system sends the dialed digits to the PSTN, you can use the Discard Digits option to strip the pre-dot digit from the dialed string so that the PSTN can route the call.

Example of Digit Prefixing

One example of using digit prefixing in a route pattern is when you configure On-Net dialing between sites. You can create a route pattern so that users within your organization dial 8 + XXX-XXXX to call between sites. For Off-Net calls, you can remove the prefix digit (8) and add a new prefix of 1<area code> so that you can route the call to the PSTN in E.164 format.

Example of On-Net and Off-Net Patterns

You can configure a route pattern as OnNet or OffNet using the **Call Classification** field. You can classify calls as Off-Net in cases where you want your users to get a secondary dial tone to let them know that their call is going outside your organization. For example, if you create a route pattern that requires users to dial 9 to access an outside line, and you classify it as an Off-Net pattern, the system provides the following dial tones:

- A dial tone when the phone is off-hook, before the you dial 9.
- A secondary dial tone, after the you dial 9 to indicate that the system is ready to call the Public Switched Telephone Network (PSTN) number.

Ensure that you deselect the **Allow Device Override** check box when you use this option.

Example of Block and Route Patterns

Use block and route patterns to prevent outgoing or incoming calls that you do not want to route. Use block patterns to:

- Block specific patterns. For example, blocking the pattern 91900XXXXXXX prevents users from placing calls to 900 services.
- Prevent toll fraud by blocking calls to specific area codes and locations.

Configure Time of Day Routing

Optional. Create a time schedule that specifies when a partition is available to receive incoming calls.

Note Time of Day routing is not implemented for Message Waiting Indication (MWI) intercept.

Procedure

	Command or Action	Purpose
Step 1	Configure a Time Period, on page 140	Use this procedure to define time periods. You can define a start time and an end time, and also specify repetition interval either as days of the week or a specified date on the yearly calendar.

	Command or Action	Purpose
Step 2	Configure a Time Schedule, on page 140	Use this procedure to create a schedule. The time periods that you configured in the previous procedure are building blocks for this schedule. You can assign time periods to multiple schedules.
Step 3	Associate a Time Schedule with a Partition, on page 140	Associate time schedules with partitions to determine where calling devices search when they are attempting to complete a call during a particular time of day.

Configure a Time Period

Use this procedure to define time periods. You can define a start time and an end time, and also specify repetition interval either as days of the week or a specified date on the yearly calendar.

Procedure

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

Step 2 Configure the fields in the **Time Period Configuration** window. For more information on the fields and their configuration options, see the system Online Help.

Step 3 Click **Save**.

Configure a Time Schedule

Use this procedure to create a schedule. The time periods that you configured in the previous procedure are building blocks for this schedule. You can assign time periods to multiple schedules.

Procedure

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

Step 2 Configure the fields in the **Time Schedule Configuration** window. For more information on the fields and their configuration options, see the system Online Help.

Step 3 Click **Save**.

Associate a Time Schedule with a Partition

Associate time schedules with partitions to determine where calling devices search when they are attempting to complete a call during a particular time of day.

Procedure

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

Step 2 From the **Time Schedule** drop-down list, choose a time schedule to associate with this partition.
The time schedule specifies when the partition is available to receive incoming calls. If you choose **None**, the partition remains active at all times.

Step 3 Click **Save**.

Call Routing Restrictions

Feature	Restriction
Route Filter Associations	When configuring your call routing, be careful not to assign a single route filter to too many route patterns. A system core crash could result if you were to edit a route filter that has hundreds of associated route patterns. This is due to the extra system processing that is required to update call routing for all of the route patterns that use the route filter. Create duplicate route filters to ensure that this does not happen.
External Call Control	External call control lets an adjunct route server make call routing decisions for Unified Communications Manager by using the Cisco Unified Routing Rules Interface. When you configure external call control, Unified Communications Manager issues a route request that contains the calling party and called party information to the adjunct route server. That server receives the request, applies appropriate business logic, and returns a route response that instructs your system on how to route the call along with any additional call treatment to apply. For details, see the *Configure External Call Control* chapter of the *Feature Configuration Guide for Cisco Unified Communications Manager*.
Call Control Discovery	With Call Control Discovery, Unified Communications Manager clusters can automatically exchange the DN ranges they host by subscribing to a Cisco IOS service routing protocol called the Service Advertisement Framework (SAF). This feature enables clusters to advertise their own hosted DN ranges into the network as well as to subscribe to advertisements that are generated by other call agents in the network. The main benefits of using SAF CCD are: • Automated distribution of call routing information between call agents participating in the same SAF CCD network, thus avoiding incremental configuration work when new call agents are added or when new DN ranges are added to a call agent. • No reliance on a centralized dial plan resolution control point. • Automated recovery of inter-call agent call routing information when routing changes occur, including when multiple Unified CM clusters are combined. To configure Call Control Discovery, refer to the *Configure Call Control Discovery* chapter of the *Feature Configuration Guide for Cisco Unified Communications Manager*.

Feature	Restriction
Route Plan Report	You can view a detailed route plan within the Route Plan Report window of Cisco Unified CM Administration (Call Routing > Route Plan Report). The route plan report allows you to view either a partial or full list of your route plan and to go directly to the associated configuration windows by clicking the entry in the Pattern/Directory Number, Partition, or Route Detail columns of the report. In addition, the route plan report allows you to save report data into a .csv file that you can import into other applications. The .csv file contains more detailed information than the web pages, including directory numbers for phones, route patterns, pattern usage, device name, and device description.

Line Group Setup

This chapter provides information to add or delete a line group or to add directory numbers to or to remove directory numbers from a line group.

For additional information, see topics related to understanding route plans in the *Cisco Unified Communications Manager System Guide*.

About Line Group Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Route/Hunt** > **Line Group** menu path to configure line groups.

A line group allows you to designate the order in which directory numbers are chosen. Cisco Unified Communications Manager distributes a call to idle or available members of a line group based on a call distribution algorithm and on the Ring No Answer Reversion (RNAR) Timeout setting.

Note Users cannot pick up calls to a DN that belongs to a line group by using the Directed Call Pickup feature.

Tip Although you can configure an empty line group with no members (directory numbers), Cisco Unified Communications Manager does not support this configuration for routing calls. If the line group contains no members, the hunt list stops hunting when the call gets routed to the empty line group. To avoid this situation, make sure that you configure at least one member in the line group.

Line Group Configuration Tips

You must define one or more directory numbers before configuring a line group.

After you configure or update a line group, you can add or remove members from that line group.

Line Group Deletion

You can delete a line group that one or more route/hunt lists references. If you try to delete a line group that is in use, Cisco Unified Communications Manager displays an error message.

Tip Dependency Records is not supported for line groups. As a best practice, always check the configuration before you delete a line group.

Line Group 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. **Timesaver** Use concise and descriptive names for your line groups. The CompanynameLocationGroup format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a line group. For example, CiscoDallasAA1 identifies a Cisco Access Analog line group for the Cisco office in Dallas.
RNA Reversion Timeout	Enter a time, in seconds, after which 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.

Field	Description
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, 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, Unified Communications Manager distributes a call to idle or available members starting from the (n+1)th member of a route group, where the nth member is the next sequential member in the list who is either idle or busy but not “down.” If the nth member is the last member of a route group, Unified Communications Manager distributes a call starting from the top of the route group. • Longest Idle Time—If you choose this distribution algorithm, 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, 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.
Hunt Options	

Field	Description
No Answer	For a given distribution algorithm, choose a hunt option for 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, 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, 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, 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. 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, Unified Communications Manager skips the remaining members of this line group when the RNA reversion timeout value elapses for the first member. Unified Communications Manager then proceeds directly to the next line group in a hunt list. • Stop hunting—If you choose this hunt option, 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.
Automatically Logout Hunt Member on No Answer	If this check box is checked, line members will be logged off the hunt list automatically. Line members can log back in using the "HLOG" softkey or PLK.

Field	Description
Busy	For a given distribution algorithm, choose a hunt option for 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, 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, 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, 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. 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, Unified Communications Manager skips the remaining members of this line group upon encountering a busy member. Unified Communications Manager proceeds directly to the next line group in a hunt list. • Stop hunting—If you choose this hunt option, Unified Communications Manager stops hunting after trying to distribute a call to the first busy member of this line group.

Field	Description
Not Available	For a given distribution algorithm, choose a hunt option for 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, 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, 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, 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. 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, Unified Communications Manager skips the remaining members of this line group upon encountering the first unavailable member. Unified Communications Manager proceeds directly to the next line group in a hunt list. • Stop hunting—If you choose this hunt option, 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.
Current Line Group Members	

Field	Description
Broadcast algorithm with shared line DNs	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. **Note** When adding DNs and Route Partitions to your line group, do not put DNs that are shared lines in a line group that uses the Broadcast distribution algorithm. 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.

Add Members to Line Group

You can add members to a new line group or to an existing line group. The following procedure describes adding a member to an existing line group.

Before you begin

You must define one or more directory numbers before performing this procedure.

Procedure

Step 1 Choose **Call Routing** > **Route/Hunt** > **Line Group**.

Step 2 Locate the line group to which you want to add a member.

Step 3 If you need to locate a directory number, choose a route partition from the Partition drop-down list box, enter a search string in the Directory Number Contains field, and click Find. To find all directory numbers that belong to a partition, leave the Directory Number Contains field blank and click Find.

A list of matching directory numbers displays in the Available DN/Route Partition list box.

Step 4 In the Available DN/Route Partition list box, choose a directory number to add and click Add to Line Group to move it to the Selected DN/Route Partition list box. Repeat this step for each member that you want to add to this line group.

Step 5 In the Selected DN/Route Partition list box, choose the order in which the new directory number(s) is to be accessed in this line group. To change the order, click a directory number and use the Up and Down arrows to the right of the list box to change the order of directory numbers.

Step 6 Click Save to add the new directory numbers and to update the directory number order for this line group.

Remove Members From Line Group

You can remove members from a new line group or from an existing line group. The following procedure describes removing a directory number from an existing line group.

Procedure

Step 1 Choose **Call Routing** > **Route/Hunt** > **Line Group**.

Step 2 Locate the line group from which you want to remove a directory number.

Step 3 In the Selected DN/Route Partition list box, choose a directory number to be deleted and click the down arrow below the list box to move the directory number to the Removed DN/Route Partition list box. Repeat this step for each member that you want to remove from this line group.

Step 4 To remove the members, click Save.

CHAPTER 21

Configure Hunt Pilots

Hunt Pilot Overview

A hunt pilot comprises a number or pattern and a set of associated digit manipulations that can route calls to a group of phones or directory numbers in a line group.

Hunt pilots work in conjunction with hunt lists, which are prioritized lists of eligible paths (line groups) for incoming calls. When a call is placed to a hunt pilot DN, the system offers the call to the first line group specified in the hunt list. If no one in the first line group answers the call, the system offers the call to the next line group specified in the hunt list. Line groups control the order in which the call is distributed to phones within the group. They point to specific extensions, which are typically IP phone extensions or voicemail ports. Line groups cannot point to Computer Telephony Integration (CTI) ports and CTI route points, so you cannot use hunt pilots to distribute calls to endpoints that are controlled through CTI applications such as Cisco Customer Response Solution (CRS) or IP Interactive Voice Response (IP IVR).

A hunt pilot can distribute calls to any of its assigned line groups, even if the line groups and the hunt pilot reside in different partitions. A call distributed by the hunt pilot overrides all the partitions and calling search space restrictions.

Hunt Pilot Configuration Task Flow

Complete these tasks to configure hunt pilots for your system. Hunt pilots can be used to route calls to a group of phones or directory numbers in a line group.

Procedure

	Command or Action	Purpose
Step 1	Configure Line Groups, on page 152	Create a line group to enable multiple phones to answer calls that are directed to a single directory number (DN).

	Command or Action	Purpose
Step 2	Configure Hunt Lists, on page 152	Configure a hunt list with a prioritized order of line groups.
Step 3	Configure Hunt Pilots, on page 153	Configure a hunt pilot number or pattern that the system uses to direct calls to a hunt list.

Configure Line Groups

Line groups let multiple phones answer calls that are directed to a single directory number. The Distribution Algorithm controls the order in which an incoming call gets distributed to the phones in the group.

Procedure

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

Step 2 Choose one of the following options:

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

Step 3 Enter a **Line Group Name**.

Step 4 From the **Distribution Algorithm** field, select the type of algorithm that you want to use to distribute calls.

Step 5 Configure the fields in the **Line Group Members to Add to Line Group** section to add directory numbers to the line group:

a) Select a **Partition** where the directory numbers that you want to add reside.
b) Optional. Filter the search by completing the **Directory Number Contains** field.
c) Click **Find**. The list of Directory Numbers from the Partition appears in the box
d) In the **Available DN/Route Partition** list box, select each directory number that you want to add to the group and click **Add to Line Group**.

Step 6 Configure the remaining fields in the **Line Group Configuration** window. See the online help for more information about the fields and their configuration options.

Step 7 Click **Save**.

Configure Hunt Lists

A hunt list is a prioritized list of line groups. When the system routes a call through a hunt list, it uses the line groups in the order that you define in the hunt list.

Procedure

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

Step 2 Choose one of the following options:

- Click **Add New** to create a new list.

- Click **Find** and select an existing list.

Step 3 Enter the **Name** for the Hunt List.

Step 4 Select a **Cisco Unified Communications Manager Group** to which you want to register the Hunt List.

Step 5 Check the **Enable this Hunt List** check box to enable the hunt list immediately when you click Save.

Step 6 Check the **For Voice Mail Usage** check box if the hunt list is for voice mail.

Step 7 Click **Save**.

Step 8 Add line groups to your hunt list:

a) Click **Add Line Group**.
b) From the **Line Group** drop-down, select a line group to add to the hunt list.
c) Click **Save**.
d) Repeat these steps to add additional line groups.

Configure Hunt Pilots

Configure a hunt pilot number or pattern that the system uses to route calls to a line group.

Note For information about wildcards and special characters that you can use for the hunt pilot, see Wildcards and Special Characters in Hunt Pilots, on page 154.

Procedure

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

Step 2 Choose one of the following options:

- Click **Add New** to create a new hunt pilot.
- Click **Find** and select an existing hunt pilot.

Step 3 In the **Hunt Pilot** field, enter the number or pattern that you want to use to route calls.

Step 4 From the **Hunt List** drop-down, select the hunt list to which you want to direct calls that match the hunt pilot number.

Step 5 Complete the remaining fields in the **Hunt Pilot Configuration** window. For help with the fields and their settings, see the online help.

Step 6 If you want to enable Call Queuing, check the **Queue Calls** check box and configure the fields in the **Queuing** section.

Step 7 Assign any digit transformation patterns that you want to apply to calling, connected or called parties.

Step 8 Click **Save**.

Wildcards and Special Characters in Hunt Pilots

Wildcards and special characters in hunt pilots allow a hunt pilot to match a range of numbers (addresses). Use these wildcards and special characters also to build instructions that enable the Cisco Unified Communications Manager to manipulate a number before sending it to an adjacent system.

The following table describes the wildcards and special characters that Cisco Unified Communications Manager supports.

Table 13: Wildcards and Special Characters

Character	Description	Examples
@	The at symbol (@) wildcard matches all National Numbering Plan numbers. Each route pattern can have only one @ wildcard.	The route pattern 9.@ routes or blocks all numbers that the National Numbering Plan recognizes. The following route patterns examples show National Numbering Plan numbers that the @ wildcard encompasses: • 0 • 1411 • 19725551234 • 101028819725551234 • 01133123456789
X	The X wildcard matches any single digit in the range 0 through 9.	The route pattern 9XXX routes or blocks all numbers in the range 9000 through 9999.
!	The exclamation point (!) wildcard matches one or more digits in the range 0 through 9.	The route pattern 91! routes or blocks all numbers in the range 910 through 91999999999999999999999.
?	The question mark (?) wildcard matches zero or more occurrences of the preceding digit or wildcard value. **Note** If the question mark (??) wildcard is used, the second question mark does not match the empty input. Example router pattern: *33X?*X?*X?#	The route pattern 91X? routes or blocks all numbers in the range 91 through 91999999999999999999999.
+	The plus sign (+) wildcard matches one or more occurrences of the preceding digit or wildcard value.	The route pattern 91X+ routes or blocks all numbers in the range 910 through 91999999999999999999999.

Character	Description	Examples
[ ]	The square bracket ([ ]) characters enclose a range of values.	The route pattern 813510[012345] routes or blocks all numbers in the range 8135100 through 8135105.
-	The hyphen (-) character, used with the square brackets, denotes a range of values.	The route pattern 813510[0-5] routes or blocks all numbers in the range 8135100 through 8135105.
^	The circumflex (^) character, used with the square brackets, negates a range of values. Ensure that it is the first character following the opening bracket ([). Each route pattern can have only one ^ character.	The route pattern 813510[^0-5] routes or blocks all numbers in the range 8135106 through 8135109.
.	The dot (.) character, used as a delimiter, separates the Cisco Unified Communications Manager access code from the directory number. Use this special character, with the discard digits instructions, to strip off the Cisco Unified Communications Manager access code before sending the number to an adjacent system. Each route pattern can have only one dot (.) character.	The route pattern 9.@ identifies the initial 9 as the Cisco Unified Communications Manager access code in a National Numbering Plan call.
*	The asterisk (*) character can provide an extra digit for special dialed numbers.	You can configure the route pattern *411 to provide access to the internal operator for directory assistance.
#	The octothorpe (#) character generally identifies the end of the dialing sequence. Ensure the # character is the last character in the pattern.	The route pattern 901181910555# routes or blocks an international number that is dialed from within the National Numbering Plan. The # character after the last 5 identifies this digit as the last digit in the sequence.
\+	A plus sign preceded by a backslash, that is, \+, indicates that you want to configure the international escape character +.	Using \+ means that the international escape character + is used as a dialable digit, not as a wildcard.

Performance and Scalability for Hunt Pilots

The following performance and scalability restrictions apply:

- A single Unified CM Cluster supports a maximum of 15,000 hunt list devices.

- A single Unified CM Subscriber supports a maximum of 100 hunt pilots with call queuing enabled per node
- Hunt list devices may be a combination of 1500 hunt lists with ten IP phones in each hunt list, 750 hunt lists with twenty IP phones in each hunt list, or similar combinations

Note When using the broadcast algorithm for call coverage, the number of hunt list devices is limited by the number of busy hour call attempts (BHCA). Note that a BHCA of 10 on a hunt pilot pointing to a hunt list or hunt group containing 10 phones and using the broadcast algorithm is equivalent to 10 phones with a BHCA of 10.

- The maximum number of hunt pilots is 100 per Unified CM subscriber node with call queue enabled when configured with 32 callers which is allowed in the queue. The total number of queue slots per node (the value of "Maximum Number of Callers Allowed in Queue" for all Call Queuing Enabled Hunt Pilots on the node combined) is limited to 3200. The maximum number of simultaneous callers in a queue for each hunt pilot is 100, meaning 100 callers per hunt pilot is allowed in a queue and the maximum number of hunt pilots is reduced to 32. The maximum number of members across all hunt lists does not change when call queuing is enabled.
- The maximum wait time in queue for each hunt pilot that you can configure ranges from 0 to 3600 seconds (default 900). An increase in the number of hunt lists can require you to increase the dial plan initialization timer that is specified in the Unified Communications Manager service parameters. We recommend that you set the dial plan initialization timer to 600 seconds if you have 1500 hunt lists configured.
- We recommend having no more than 35 directory numbers for a single line group when using broadcast algorithms with call queuing. Additionally, the number of broadcast line groups depends on the busy hour call completion rate (BHCC). If there are multiple broadcast line groups in a Unified CM system, the number of maximum directory numbers in a line group must be less than 35. The number of busy hour call attempts (BHCA) for all the broadcast line groups should not exceed 35 calls set up per second.

Hunt Pilot Interactions and Restrictions

Feature	Interactions and Restrictions
Single Number Reach with Hunt Groups	If you have a hunt group configured and one or more of the directory numbers that the hunt group points toward also has Single Number Reach (SNR) enabled, the call does not extend to the SNR remote destinations unless all devices in the hunt group are logged in. For each device within the hunt group, the **Logged Into Hunt Group** check box must be checked within the **Phone Configuration** window for that device.

Feature	Interactions and Restrictions
Call Queuing	Call Queuing is a subfeature of hunt pilots. When call queuing is enabled and the incoming call requirement to a particular hunt pilot exceeds the number of hunt members whom are available to answer a call, the system queues incoming calls until a hunt member is available to answer them. You can configure announcements and music on hold to play to callers while they are waiting. For additional configuration details, see the 'Configure Call Queuing' chapter of the Feature Configuration Guide for Cisco Unified Communications Manager.
Unified Mobility	We don’t recommend configuring Unified Mobility devices in Hunt pilot.

Calls Not Being Distributed

Table 14: Calls are not being distributed with circular algorithm

Restriction	Description
Calls are not being distributed correctly in Circular algorithm for a line group with BOT and TCT devices.	When a call is extended to an agent who is in a logged off state and the call is rejected with a different reject type other than the "**Huntlogout**" type. Then the index will not get incremented and the call will go to the same agent who had answered the previous call.
Calls are not distributed correctly in Circular algorithm for a line group.	While distributing the calls in a circular algorithm, when an agent is busy, the call is extended to the next available agent (i.e. the next agent will answer the call on behalf of the busy agent). **Note** In the case of multiple calls at the same time, the next available agent answers the call.

CHAPTER 22

Configure Translation Patterns

Translation Pattern Overview

You can configure translation patterns to manipulate digits for any type of call. Translation patterns follow the same general rules and use the same wildcards as route patterns. As with route patterns, you assign a translation pattern to a partition. However, when the dialed digits match the translation pattern, Cisco Unified Communications Manager does not route the call to an outside entity such as a gateway; instead, it performs the translation first and then routes the call again, this time using the calling search space configured within the translation pattern.

Translation Pattern Prerequisites

Before you configure a translation pattern, you must complete the following tasks:

- Partition Configuration Task Flow, on page 119
- Call Routing Configuration Task Flow, on page 128

Note For each translation pattern that you create, ensure that the combination of partition, route filter, and numbering plan is unique. If you receive an error that indicates duplicate entries, check the route pattern or hunt pilot, translation pattern, directory number, call park number, call pickup number, or meet-me number configuration windows.

Translation Pattern Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure Translation Patterns, on page 160	Configure translation patterns to specify how to route a call after it is placed.

Configure Translation Patterns

Configure translation patterns to apply digit manipulations to the calling and called numbers when the dial string matches the pattern. The system completes the digit translation and then reroutes the call.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Translation Pattern**.

Step 2 Choose one of the following options:

- Click **Add New** to add a new translation pattern.
- Click **Find**, and select an exisiting translation pattern.

Step 3 In the **Translation Pattern** field, enter the pattern that you want the system to match to dial strings that use this pattern.

Step 4 From the **Partition** drop-down list, select the partition where you want to assign this pattern.

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

Step 6 Click **Save**.

CHAPTER 23

Configure Transformation Patterns

Transformation Pattern Overview

Transformation patterns determine how the system manipulates the digits that were dialed in an incoming or outgoing call. You can configure transformation patterns when you need to change the calling or called number before the system sends it to the phone or the PSTN.

You can use transformation patterns to discard digits, prefix digits, add a calling party transformation mask, and control the presentation of the calling party number.

You can:

- Hit a Calling Party Transformation Pattern with a Called Party Transformation CSS.
- Hit a Called Party Transformation Pattern with a Calling Party Transformation CSS.

Transformation Pattern Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure Calling Party Transformation Patterns, on page 162	Use this procedure to transform the calling number. For example, you can configure a transformation pattern that replaces a caller's extension with the office's main number when calling the PSTN.
Step 2	Configure Called Party Transformation Patterns, on page 162	Use this procedure to transform the called number. For example, you can configure a transformation pattern that retains only the last five digits of a call dialed as a ten-digit number.

	Command or Action	Purpose
Step 3	Configure Transformation Profiles, on page 163	**Optional**: Perform this procedure only if you are using Cisco Intercompany Media Engine (Cisco IME). You must configure a transformation profile to convert dialed numbers into the E.164 format.

Configure Calling Party Transformation Patterns

Use this procedure to transform the calling number. For example, you can configure a transformation pattern that replaces a caller's extension with the office's main number when calling the PSTN.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Transformation** > **Transformation Pattern** > **Calling Party Transformation Pattern**.

Step 2 Choose one of the following options:

- Click **Add New** to add a new calling party transformation pattern.
- Click **Find** and select an existing pattern.

Step 3 From the **Pattern** field, enter the pattern that you want to match to the calling party number.

Note **For Outboud Calls:**

The calling party transformation mask is selected based on the pre transform calling party number. (extension assigned to the IP Phone).

While selecting the calling party transformation mask on the SIP trunk, if the calling party number is transformed to a different number on either the route pattern/group, the pre transform calling number is always used to select the calling party transformation mask.

Whereas according to the Dialed Number Analyzer (DNA), the transformed number is used to select the calling party transformation mask. However, this is the wrong behavior of DNA.

Step 4 Complete the remaining fields in the **Calling Party Transformation Pattern Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 5 Click **Save**.

Configure Called Party Transformation Patterns

Use this procedure to transform the called number. For example, you can configure a transformation pattern that retains only the last five digits of a call dialed as a ten-digit number.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Transformation** > **Transformation Pattern** > **Called Party Transformation Pattern**.

Step 2 Choose one of the following options:

- Click **Add New**, to add a new called party transformation pattern.
- Click **Find** and select an existing pattern.

Step 3 From the **Pattern** field, enter the pattern that you want to match to the called number.

Step 4 Complete the remaining fields in the **Called Party Transformation Pattern Configuration** window. For more information on the fields and their configuration options, see the system Online Help.

Step 5 Click **Save**.

Configure Transformation Profiles

Perform this procedure only if you are using Cisco Intercompany Media Engine (Cisco IME). You must configure a transformation profile to convert dialed numbers into the E.164 format. The E.164 format includes the international "+" prefix; for example, "+14085551212".

Procedure

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

Step 2 Choose one of the following options:

- Click **Add New**, to add a new transformation profile.
- Click **Find** and choose a pattern from the resulting list, to modify the settings for an existing transformation profile.

The **Transformation Profile Configuration** window appears.

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

Step 4 Click **Save**.

CHAPTER 24

Configure Dial Rules

Dial Rules Overview

The Unified CM supports the following types of dial rules:

- **Application Dial Rules**: The administrator uses application dial rules to add and sort the priority of dialing rules for applications such as Cisco web dialer and Cisco Unified Communications Manager Assistant.

- **Directory Lookup Dial Rules**: The administrator uses directory lookup dial rules to transform caller identification numbers and perform a directory search from the assistant console in application such as Cisco Unified Communications Manager Assistant.

- **SIP Dial Rules**: The administrator uses SIP dial rules to perform system digit analysis and routing. The administrator configures SIP dial rules and adds the SIP dial rule to the Cisco Unified IP Phone before the call processing takes place.

Dial Rules Prerequisites

- For SIP dial rules configuration, the devices must be running SIP

- The administrator associates the SIP dial rules with the following devices: Cisco IP Phones 7911, 7940, 7941, 7960, 7961

Dial Rules Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure Application Dial Rules, on page 166	Configure application dial rules to add and sort the priority of dialing rules for applications such as Cisco web dialer and Cisco Unified Communications Manager Assistant.
Step 2	Configure Directory Lookup Dial Rules, on page 167	Configure directory lookup dial rules to transform caller identification numbers into numbers that can be looked up in the directory.
Step 3	Configure SIP Dial Rules, on page 167	Use SIP dial rules configuration to configure dial plans for phones that are running SIP.
Step 4	Reprioritize Dial Rule, on page 170	Optional. Change the priority of the dial rules in the Cisco Unified Communications Manager Administration window, if more than one dial rule exists.

Configure Application Dial Rules

Cisco Unified Communications Manager supports application dial rules that allow you to add and sort the priority of dialing rules for applications such as Cisco web dialer and Cisco Unified Communications Manager Assistant. Application dial rules automatically strip numbers from or add numbers to telephone numbers that the 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.

Note Cisco Unified Communications Manager automatically applies application dial rules to all remote destination numbers for CTI remote devices.

Perform the following procedure to add a new application dial rule or update an existing application dial rule.

Procedure

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

Step 2 In the **Find and List Application Dial Rules** window, perform one of the following steps:

- Click **Add New**.
- Click **Find** and choose an existing application dial rule.

Step 3 Configure the fields in the **Application Dial Rule Configuration** window. For detailed field descriptions, refer to the online help.

Step 4 Click **Save**.

What to do next

Perform the following tasks:

- Configure Directory Lookup Dial Rules, on page 167
- Configure SIP Dial Rules, on page 167

Configure Directory Lookup Dial Rules

Directory lookup dial 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 dial rule that automatically removes the area code and two prefix digits from a 10-digit telephone, which would transform 4085551212 into 51212.

Perform the following procedure to add a new directory lookup dial rule or update an existing directory lookup dial rule.

Procedure

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

Step 2 In the **Directory Lookup Dial Rule Find and List** window **Directory Lookup Dial Rule Find and List** window, perform one of the following steps:

- Click **Add New**.
- Click **Find** and choose an existing directory lookup dial rule.

Step 3 Configure the fields in the **Directory Lookup Dial Rule Configuration** window. For detailed field descriptions, refer to the online help.

Step 4 Click **Save**.

What to do next

Configure SIP Dial Rules, on page 167

Configure SIP Dial Rules

SIP dial rules provide local dial plans for Cisco IP Phones that are running SIP, so users do not have to press a key or wait for a timer before the call gets processed. The administrator configures the SIP dial rule and applies it to the phone that is running SIP.

Procedure

	Command or Action	Purpose
Step 1	Set Up SIP Dial Rule, on page 169	Configure and update SIP dial rules and associate them with the phones that are running SIP.
Step 2	Reset SIP Dial Rule, on page 169	Reset or restart the phone that is running SIP when the SIP dial rule gets updated, so that the phone is updated with the new SIP dial rule.
Step 3	Synchronize SIP Dial Rules Settings With SIP Phones, on page 170	(Optional) Synchronize a SIP phone with a SIP dial rule that has undergone configuration changes, which applies any outstanding configuration settings in the least intrusive manner possible. For example, a reset or restart may not be required on some affected SIP phones.

Related Topics

Pattern Formats, on page 168

Pattern Formats

Table 15: Pattern Formats for SIP Dial Rules

Dial Rule Pattern	Value
7940_7960_OTHER	• Period (.) matches any character • Pound sign (#) acts as the terminating key, and you can apply termination only after matching hits. Alternatively asterisk (*) can also be used as a terminating key as well. **Note** You must configure the pound sign in the pattern field so that it is valid for 7940_7960_OTHER. • Asterisk (*) matches one or more characters and it 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. For example, 7.... will match any 4-digit DN that starts with 7. 8,..... will match 8, play secondary dial tone (default value), and then match any 5-digit DN.

Set Up SIP Dial Rule

To configure dial plans for phones that are running SIP.

Procedure

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

Step 2 In the **Find and List SIP Dial Rules** window. Perform one of the following steps:

- Click **Add New**
- Click **Find** and choose an existing SIP Dial Rule

Step 3 Configure the fields in the **SIP Dial Rule Configuration** window. For detailed field descriptions, refer to the online help.

Step 4 Click **Save**.

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

What to do next

Reset SIP Dial Rule, on page 169

Related Topics

Pattern Formats, on page 168

Reset SIP Dial Rule

Perform the following procedure to reset or restart the phone that is running SIP when the SIP dial rule gets updated, so the phone gets updated with the new SIP dial rule.

Before you begin

Set Up SIP Dial Rule, on page 169

Procedure

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

Step 2 In the **Find and List SIP Dial Rules** window, click **Find** and choose an existing SIP dial rule that you want to reset.

Step 3 In the **SIP Dial Rule Configuration** window, click **Reset**.

Step 4 Perform one of the following tasks in the **Device Reset** dialog box:

- To restart the chosen devices without shutting them down and reregister them with Cisco Unified Communications Manager, click **Restart**.
- To shut down, and then restart the device, click **Reset**.
- To close the Device Reset dialog box without performing any action, click **Close**.

After the administrator configures the SIP dial rule and applies it to the phone that is running SIP, the database sends the TFTP server a notification, so it can build a new set of configuration files for the phone that is running SIP. The TFTP server notifies Cisco Unified Communications Manager about the new configuration file, and the updated configuration file is sent to the phone. See **Configure TFTP Servers** for Cisco Unified IP phones that run SIP for more information.

What to do next

Synchronize SIP Dial Rules Settings With SIP Phones, on page 170

Synchronize SIP Dial Rules Settings With SIP Phones

To synchronize a SIP phone with a SIP dial rule that has undergone configuration changes, perform the following procedure.

Before you begin

Reset SIP Dial Rule, on page 169

Procedure

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

Step 2 In the **Find and List SIP Dial Rules** window, click **Find** and choose an existing SIP dial rule to which you want to synchronize applicable SIP phones.

Step 3 Make any additional configuration changes and click **Save** in the **SIP Dial Rule Configuration**.

Step 4 Click **Apply Config**.

Step 5 Click **OK**.

Reprioritize Dial Rule

To add and sort the priority of dialing rules in the **Dial Rule Configuration** window.

Procedure

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

Step 2 Select one of the following:

- **Application Dial Rules**
- **Directory Lookup Dial Rules**
- **SIP Dial Rules**

Step 3 In the Find and List window, choose a dial rule and click the dial rule name.
The **Dial Rule Configuration** window appears.

Step 4 Use the up and down arrows to move the dial rule up or down the list.

Step 5 After you complete prioritizing the order, click **Save**.

Dial Rules Interactions and Restrictions

SIP Dial Rules Interactions

SIP Dial Rules Interactions

Cisco Unified IP Phone	Interaction
7911, 7941, 7961 that are running SIP	These phones use the 7940_7960_OTHER dial rules patterns. Key Press Markup Language (KPML) allows for the digits to be sent to Cisco Unified Communications Manager digit by digit; SIP dial rules allow for 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 is 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.
7940 and 7960 that are running SIP	These phones use the 7940_7960_OTHER dial rules pattern and do not support KPML. If the administrator does not configure a SIP dial plan for these phones, the user must wait a specified time before the digits are sent to Cisco Unified Communications Manager for processing. This delays the processing of the actual call.

Directory Lookup Dial Rules Restrictions

Directory Lookup Dial Rules Restrictions

Field	Restriction
Number Begins With	This field supports only digits and the characters +,*, and #. The length cannot exceed 100 characters.
Number of Digits	This field supports only digits, and the value in this field cannot be less than the length of the pattern that is specified in the pattern field.
Total Digits to be Removed	This field supports only digits, and the value in this field cannot be more than the value in the **Number of Digits** field.
Prefix with Pattern	The prefix it with field supports only digits and the characters +,*, and #. The length cannot exceed 100 characters. **Note** You cannot allow both the **Total Digits to be Removed** field and the **Prefix with Pattern** field to be blank for a dial rule.

CHAPTER 25

Configure Intercluster Lookup Service

Intercluster Lookup Service Overview

The Intercluster Lookup Service (ILS) allows you to create networks of remote Cisco Unified Communications Manager clusters. When you configure ILS on multiple clusters, it updates Cisco Unified Communications Manager with the current status of remote clusters in the ILS network.

In Cisco Unified CM Administration, you can configure ILS on a pair of clusters and then join those clusters to form an ILS network. ILS allows you to join additional clusters to the network without having to configure the connections between each cluster.

An ILS network comprises the following components:

- Hub clusters
- Spoke clusters
- Global dial plan imported catalogs

Hub Clusters

Hub clusters form the backbone of an ILS network. Hub clusters exchange ILS updates with the other hub clusters in the ILS network, and then relay that information to and from their spoke clusters.

When a new hub cluster registers to another hub cluster in an existing ILS network, ILS automatically creates a full mesh connection between the new hub cluster and all the existing hub clusters in the ILS network.

Spoke Clusters

A spoke cluster connects to the hub cluster in an ILS network to relay ILS updates to and from the rest of the ILS network. Spoke clusters contact only their local hub cluster and never directly contact other hub clusters or other spoke clusters.

Global Dial Plan Imported Catalogs

To provide URI dialing compatibility with third-party systems, you can manually import a third-party directory URI or +E.164 number catalog from a CSV file into any hub cluster in the ILS network. ILS maintains the imported catalog and replicates that catalog out to the other clusters in the network. You can dial one of the third-party directory URIs or +E.164 numbers catalog from any server in the ILS network.

ILS Networking Capacities

Following are recommended capacities to keep in mind when planning an ILS network:

- ILS networking supports up to 10 hub clusters with 10 spoke clusters per hub, up to a 100 total cluster maximum. A hub and spoke combination topology is used to avoid many TCP connections created within each cluster.
- There may be a performance impact with utilizing your hub and spoke clusters at, or above, their maximums. Adding too many spoke clusters to a single hub creates extra connections that may increase the amount of memory or CPU processing. We recommend that you connect to a hub cluster with no more than 10 spoke clusters.
- ILS networking adds extra CPU processing to your system. The CPU utilization and sync time is dependent on the number of records that are being synced across the cluster. When planning your hub and spoke topology, make sure that your hub clusters have the CPU to handle the load.

Note These recommendations are based on system testing and taking resource utilization into account. Although the system does not prevent you from exceeding these recommendations, by doing so you would risk the overutilization of resources. Cisco recommends the above capacities for optimal performance.

ILS Prerequisites

You must study your network and design an ILS topology.

For more information about the Solution Reference Network Design, see the *Cisco Unified Communications Solution Reference Network Design* guide at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html.

ILS Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Activate Intercluster Lookup Service, on page 175	Activate Intercluster Lookup Service to configure cluster IDs and remote clusters.
Step 2	Configure Cluster IDs, on page 176	Provide a unique identifier for each cluster in the ILS network.

	Command or Action	Purpose
Step 3	Configure Remote Clusters, on page 176	Configure remote clusters in the ILS network.
Step 4	To activate ILS on the various clusters, complete the following tasks: • Activate ILS on the Hub Cluster, on page 177 • Activate ILS on the Spoke Cluster, on page 178	Activate ILS on the hub cluster and spoke cluster in the ILS network. **Note** You must configure each cluster in your ILS network as either a hub cluster or a spoke cluster.
Step 5	(Optional) Configure authentication between your cluster. Select one of the following procedures: • Enable TLS Authentication Between Clusters, on page 178 • Enable Password Authentication Between Clusters, on page 179 • Enable TLS with Password Authentication Between Clusters, on page 180	Use TLS authentication between clusters in the ILS network. Use password authentication between remote clusters in the ILS network. Use TLS and password authentication to setup a ILS network using common Certificate Authority (CA) signed certificates without exchanging self-signed certificates between clusters.
Step 6	Enable ILS Support for Global Dial Plan Replication, on page 189	(Optional) Enable ILS support for Global Dial Plan Replication to share dial plan information between participating ILS enabled clusters.
Step 7	Import Catalogs in ILS Network, on page 181	(Optional) To provide URI dialing compatibility with third party systems, you can manually import a third party directory URI or +E.164 number catalog from a csv file into any hub cluster in the ILS network.

Activate Intercluster Lookup Service

You must activate the Intercluster Lookup Service to configure Cluster IDs and Remote Clusters.

Procedure

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

Step 2 From the **Server** drop-down list, choose the node on which you want to activate Cisco Intercluster Lookup Service, and then click **Go**.

Step 3 Check the **Cisco Intercluster Lookup Service** check box.

Step 4 Click **Save**.

What to do next

Configure Cluster IDs, on page 176

Configure Cluster IDs

You must configure a unique cluster ID for each cluster in the ILS network. You must also ensure that you have a unique peer ID. The clusters use this unique cluster ID and peer ID when they exchange status messages.

For example, if you have an existing ILS network of four Cisco Unified Communications Manager clusters and you want to add an additional cluster, you can configure ILS on the new cluster and then register that cluster to any hub cluster in the existing ILS network. ILS automatically informs the new cluster of all clusters in the existing network.

Each cluster in an ILS network exchange and update messages, called peer info vectors, that are designed to inform remote clusters of the status of each cluster in the network. The update messages contain information about the known clusters in the network, including:

- Cluster IDs
- Peer IDs for the publisher
- Cluster descriptions and versions
- Fully Qualified Domain Name (FQDN) of the host
- IP addresses and host names for the cluster nodes that have ILS activated

Perform the following procedure to configure a unique identifier for each cluster in the network.

Before you begin

Activate Intercluster Lookup Service, on page 175

Procedure

Step 1 Log in to the Unified Communications Manager publisher node.

Step 2 In Cisco Unified Communications Manager Administration, choose **System** > **Enterprise Parameters**.

Step 3 In the **Enterprise Parameters Configuration** window **Cluster ID** field, enter a name of the cluster that you want to configure in your network.

You can enter up to 50 characters. You can enter alphanumeric characters, period (.), and hyphen (-). The default value is StandAloneCluster.

Step 4 Click **Save**.

What to do next

Configure Remote Clusters, on page 176

Configure Remote Clusters

Perform the following steps to configure remote clusters in the ILS network.

Before you begin

Configure Cluster IDs, on page 176

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Advanced Features** > **Cluster View**.

Step 2 In the **Find and List Remote Clusters** window, choose any previously created remote cluster.

Step 3 From the **Remote Cluster Service Configuration** window, check the appropriate check box to configure services such as Extension Mobility Cross Cluster, TFTP, and RSVP Agent for remote clusters.

What to do next

Perform one of the following procedures:

- Activate ILS on the Hub Cluster, on page 177
- Activate ILS on the Spoke Cluster, on page 178

Activate ILS on the Hub Cluster

Configure each cluster in your ILS network as either a hub cluster or a spoke cluster. Each ILS network must have at least one hub cluster. You can connect a hub cluster to other hub clusters, or you can configure a hub cluster as the only hub cluster in the network. In addition, you can connect a hub cluster to multiple spoke clusters, or you can configure the hub cluster with no spoke clusters.

Perform the following procedure to activate the ILS on the hub cluster in the ILS network.

Before you begin

Configure Remote Clusters, on page 176

Procedure

Step 1 Log in to the Cisco Unified Communications Manager publisher node.

Step 2 Choose **Advanced Features** > **ILS Configuration**.

Step 3 In the **ILS Configuration** window, in the **Role** drop-down list, select **Hub Cluster** and click **Save**.

Note To remove a specific cluster in the ILS network, in the **ILS Configuration** window, in the **Role** drop-down list, select **Standalone** and click **Save**.

Step 4 In the **ILS Configuration Registration** pop-up window, leave the **Registration Server** text box empty and click **OK**.

What to do next

- Activate ILS on the Spoke Cluster, on page 178

Activate ILS on the Spoke Cluster

A spoke cluster connects to the hub cluster in an ILS network to relay ILS updates to and from the rest of the ILS network. Follow this procedure to activate ILS on the spoke cluster.

Before you begin

- Configure Cluster IDs, on page 176
- Configure Remote Clusters, on page 176

Procedure

Step 1 Log in to the Unified Communications Manager publisher node.

Step 2 In Cisco Unified CM Administration, choose **Advanced Features** > **ILS Configuration**.

Step 3 From the **Role** drop-down list, select **Spoke Cluster** and click **Save**.

Step 4 In the **ILS Configuration Registration** popup window, enter the IP address or fully qualified domain name of the publisher node for an existing hub cluster in your ILS network in the **Registration Server** text box and click **OK**.

Step 5 Confirm that your ILS network is configured by viewing the network in the ILS Clusters and Global Dial Plan Imported Catalogs section.

When the full network appears, your ILS network is configured for cluster discovery.

What to do next

Perform any of these optional procedures:

- Enable TLS with Password Authentication Between Clusters, on page 180
- Enable TLS Authentication Between Clusters, on page 178
- Enable Password Authentication Between Clusters, on page 179
- Enable ILS Support for Global Dial Plan Replication, on page 189

Enable TLS Authentication Between Clusters

(Optional) Use this procedure for the TLS authentication to encrypt communications between remote clusters in the ILS network:

Before you begin

To use Transport Layer Security (TLS) authentication between clusters, you must exchange Tomcat certificates between the publisher node of each cluster in the ILS network. From Cisco Unified Operating System Administration, use the Bulk Certificate Management feature to:

- export certificates from the publisher node to a central location, for each cluster in your network
- consolidate exported certificates from any publisher node server in your ILS network
- import certificates into the publisher node for each cluster in your network

Note For more information about enabling TLS Authentication Between Clusters, see the *Administration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Procedure

Step 1 Log in to the Unified Communications Manager publisher node.

Step 2 In Cisco Unified CM Administration, choose **Advanced Features** > **ILS Configuration**.

Step 3 In the **ILS Configuration** window, check the **Use TLS Certificates** check box under ILS Authentication.

Step 4 Click **Save**.

What to do next

Perform any of these optional procedures:

- Enable Password Authentication Between Clusters, on page 179
- Enable ILS Support for Global Dial Plan Replication, on page 189

Enable Password Authentication Between Clusters

(Optional) To use password authentication between remote clusters, you must assign a password for all communications between clusters in your ILS network.

Procedure

Step 1 Log in to the Unified Communications Manager publisher node.

Step 2 In Cisco Unified CM Administration, choose **Advanced Features** > **ILS Configuration**.

Step 3 In the **ILS Configuration** window, check the **Use Password** check box under ILS Authentication.

Step 4 Enter a password in the **Use Password** text box.

Note You must configure all clusters in your network with the same password.

Step 5 Re-enter the password in the **Confirm Password** text box.

Step 6 Click **Save**.

What to do next

Perform any of these optional procedures:

- Enable TLS Authentication Between Clusters, on page 178
- Enable ILS Support for Global Dial Plan Replication, on page 189

Enable TLS with Password Authentication Between Clusters

Before you begin

To use Transport Layer Security (TLS) and password authentication without exchanging certificates between clusters, you must upload the certificate authority root certificates to the Tomcat trust and get the Tomcat certificate signed by the certificate authority root certificate. The certificate is then imported back on the same cluster. The clusters can be connected to Intercluster Lookup Service (ILS) network once the certificates are uploaded with the same password for all the clusters.

Note For more information about enabling TLS Authentication Between Clusters, see the *Administration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Procedure

Step 1 Log in to the Cisco Unified Communications Manager publisher node.

Step 2 In Cisco Unified CM Administration, choose **Advanced Features** > **ILS Configuration**.

Step 3 In the **ILS Configuration** window, check the **Use TLS Certificates** check box under ILS Authentication..

Step 4 In the **ILS Configuration** window, check the **Use Password** check box under ILS Authentication.

Step 5 Enter a password in the **Use Password** text box.

Note You must configure all clusters in your network with the same password.

Step 6 Re-enter the password in the **Confirm Password** text box.

Step 7 Click **Save**.

What to do next

(Optional)Enable ILS Support for Global Dial Plan Replication, on page 189

Enable ILS Support for Global Dial Plan Replication

(Optional) To enable ILS support for Global Dial Plan Replication in the local cluster, follow this procedure:

Procedure

Step 1 Log in to the Unified Communications Manager publisher node.

Step 2 In Cisco Unified Communications Manager Administration, choose **Advanced Features** > **ILS Configuration**.

Step 3 In the **ILS Configuration** window, check the **Exchange Global Dial Plan Replication Data with Remote Clusters** check box.

Step 4 In the **Advertised Route String** text box, enter a route string for the local cluster.

Step 5 Click **Save**.

Note When advertising URI patterns (`user@domain`), in the **SIP Profile Configuration** window, make sure that the **Dial String Interpretation** field is set to **Always treat all dial strings as URI addresses** to prevent the devices to dial URI learned patterns with only numbers in the user section as Directory Number patterns. Alternatively, you can advertise only URI patterns with text strings in the user section through ILS.

What to do next

Import Catalogs in ILS Network, on page 181

Import Catalogs in ILS Network

(Optional) To provide URI dialing compatibility with third party systems, you can manually import a third party directory URI or +E.164 number catalog from a csv file into any hub cluster in the ILS network. To Import Catalogs in the ILS network, follow this procedure:

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Call Routing** > **Global Dial Plan Replication** > **Imported Global Dial Plan Catalogs**.

Step 2 In the **Find and List Imported Global Dial Plan Catalogs** window, click **Add New**.

Step 3 Enter a Name, Description and Route String for the catalog and click **Save**.

Step 4 In Cisco Unified Communications Manager Administration, choose **Bulk Administration** > **Upload/Download Files**.

Step 5 Click **Choose** and select the CSV file that you want to import for the catalogs.

Step 6 From the **Select the Target** drop-down list, choose **Imported Directory URIs and Patterns**.

Step 7 From the **Select Transaction Type** drop-down list, choose **Insert Imported Directory URIs and Patterns**.

Step 8 Click **Save**.

ILS Interactions and Restrictions

ILS Interactions

Table 16: ILS Interactions

Feature	Interaction
Cluster discovery	ILS cluster discovery allows Cisco Unified Communications Manager clusters to learn dynamically about remote clusters without the need for an administrator to manually configure connections between those clusters. Each cluster in an ILS network exchange update messages, called peer info vectors, that are designed to inform remote clusters of the status of each cluster in the network. The update messages contain information about the known clusters in the network, including: • Cluster IDs • Cluster descriptions and versions • Fully qualified domain name of the host • IP addresses and hostnames for the cluster nodes that have ILS activated The ILS cluster discovery feature automatically populates the list of remote clusters that can be viewed in Cisco Unified CM Administration by choosing **Advanced Features** > **Cluster View**. From this window, you can configure services such as Extension Mobility Cross Cluster, TFTP, and RSVP Agent for remote clusters. **Note** A fully qualified domain name of the remote cluster, as seen in the Cluster View, must be DNS resolvable for ILS discovery to work.
Global Dial Plan Replication	When Global Dial Plan Replication is enabled across an ILS network, remote clusters in an ILS network share global dial plan data, including the following: • Directory URIs • Alternate numbers • Alternate number patterns • Route strings • PSTN failover numbers
Block Inbound Calls	To block Inbound calls based on calling party number in an ILS-based network, you must include the SIP route pattern's partition in the calling party's CSS. For example, if the call originates from SIP Trunk then SIP trunk inbound CSS must have SIP route pattern's partition.

ILS Restrictions

Table 17: ILS Restrictions

Restriction	Description
ILS Service	The ILS Service runs only on the Unified Communications manager publisher node.
Clusters	A hub cluster can have many spokes but, a spoke cluster can have only one hub cluster.
ILS Network	You cannot connect a third-party call control system into an ILS network.
Cluster Import	You can import a third-party catalog into a hub cluster only.
Duplicated URI	If a learned ILS cluster contains duplicated URIs from a different remote cluster and when a call is placed to that URI, it will be routed to the cluster whose URI has been learned and inserted into the database first.
Database Replication Status	Although the Global dial plan data is exchanged successfully on the ILS Network, an ILS receiving cluster will not write learned information into the database until it completes its database replication status.
Import	For imported third-party directory URIs and patterns, the CSV file format must match the exact syntax as shown in the administration window sample file otherwise, the import fails.
ILS Hub	When adding an additional hub cluster into the ILS network ensure to verify the following conditions are met for the primary ILS hub node: • Cluster ID is unique across all the hub nodes in the ILS cluster. • Fully Qualified Domain Name (FQDN) is configured. • UDS and EM services are running on the all of the hub nodes in the ILS cluster • DNS primary and reverse resolution are working fine. • Import consolidated Tomcat certificates from all the hub nodes. Else, the "version" information will not get displayed in the **Find and List Remote Clusters** window even after rebooting the clusters or correcting the errors. The workaround is to remove the hub cluster from the ILS network, comply with the above requirements and add the hub cluster back into the ILS network.

CHAPTER 26

Configure Global Dial Plan Replication

Global Dial Plan Replication Overview

Use global dial plan replication to create a global dial plan that spans across the Intercluster Lookup Service (ILS) network. When you enable Global Dial Plan Replication, you configure the dial plan component on one cluster, and ILS replicates that information throughout the ILS network.

When you enable Global Dial Plan Replication, each cluster in an ILS network advertises its global dial plan data, including the global dial plan data that was configured locally and any data that was learned from other clusters, to the ILS network. Global dial plan data includes the following:

- Directory universal resource indicators (URIs)
- Alternate numbers
- Advertised patterns
- PSTN failover
- Route strings
- Learned Global Dial Plan Data
- Imported Global Dial Plan Data

Directory URIs

ILS advertises the full catalog of locally configured directory URIs when you choose **Advertise Globally via ILS** option. See the URI Dialing Overview, on page 195 for more information on how to configure URI dialing.

Alternate Numbers

Alternate numbers allow you to configure globally routable numbers that can be dialed from anywhere within an ILS network. Cisco Unified Communications Manager allows you to create two types of alternate numbers:

- Enterprise alternate numbers

- +E.164 alternate numbers

Advertised Patterns

Advertised patterns allow you to create summarized routing instructions for a range of enterprise alternate numbers or +E.164 alternate numbers and replicate that pattern throughout an ILS network so that all clusters within the ILS network know the pattern. Advertised patterns prevent you from individually configuring routing information for each alternate number. Advertised patterns are never used by the local cluster on which they are configured; they are only used by remote clusters that learn the pattern through ILS. You can also configure Public Switched Telephone Network(PSTN) failover information for patterns that are advertised by ILS.

PSTN Failovers

Unified Communications Manager uses a PSTN failover number to reroute only those calls that are placed to patterns, alternate numbers, or directory URIs that were learned through ILS.Communications Manager does not reroute calls to the PSTN failover number for calls that are placed to locally configured patterns, alternate numbers, and directory URIs.

When you enable Global Dial Plan Replication, you can configure ILS to replicate a PSTN failover rule for learned directory URIs, learned numbers, and learned patterns. If the dial string for an outgoing call matches a learned pattern, learned alternate number, or learned directory URI, and Unified Communications Manager cannot route the call over a SIP trunk, Unified Communications Manager uses the calling party's Automatic Alternate Routing (AAR) CSS to reroute the call to the associated PSTN failover number.

Route Strings

ILS advertises the local route string to the ILS network. Each global dial plan data element associates to a route string that identifies the home cluster for that element. Remote clusters use the route string with a SIP route pattern to route to the various clusters in an ILS network. When a user in a remote cluster dials a directory URI or alternate number that was learned through ILS, Unified Communications Manager matches the associated route string to a SIP route pattern, and routes the call to the trunk that is specified by the SIP route pattern.

When a user assigns route string to a cluster, ILS associates that route string to all the global dial plan data that is local to that cluster (including locally configured directory URIs, alternate numbers, advertised patterns, and PSTN failover information).

Note If the SIP Route Pattern name contains dashes, you must ensure that there are no numerical digits between dashes. However, you can use a combination of letters and numbers or letters only, if there are more than one dash.

Examples of right and wrong SIP Route Patterns are listed in the following:

Correct Patterns:

- abc-1d-efg.xyz.com
- 123-abc-456.xyz.com

Incorrect Patterns :

- abc-123-def.xyz.com
- 1bc-2-3ef.xyz.com

Learned Global Dial Plan Data

Unified Communications Manager stores in the local database all global dial plan data that is learned through ILS. In addition to replicating locally configured data, ILS advertises all global dial plan data that the local cluster has learned from other clusters in the ILS network. This ensures that all advertised data reaches each cluster in the ILS network. Learned global dial plan data includes learned directory URIs, learned alternate numbers, learned patterns, learned PSTN failover rules, and learned route strings.

In Cisco Unified CM Administration, you can view the following types of learned global dial plan data:

- Learned Alternate Numbers
- Learned Enterprise and +E.164 Patterns
- Learned Directory URIs

Imported Global Dial Plan Data

Unified Communications Manager allows you to import global dial plan data from a CSV file into any hub cluster in an ILS network. ILS replicates the imported global dial plan data throughout the ILS network that allows you to interoperate Unified Communications Manager with a Cisco TelePresence Video Communications Server or a third-party call control system. Imported global dial plan data includes directory URIs, +E.164 patterns, and PSTN failover rules that were imported manually from a CSV file

Note Imported data includes only global dial plan data that is imported manually into Unified Communications Manager. Imported global dial plan data does not include data that was learned through ILS.

Global Dial Plan Replication Prerequisites

Follow the procedures to set up an ILS network in the ILS Configuration Task Flow, on page 174.

Global Dial Plan Replication Task Flow

Procedure

	Command or Action	Purpose
Step 1	Enable ILS Support for Global Dial Plan Replication, on page 189.	Enable ILS support for Global Dial Plan Replication to share dial plan information between participating ILS-enabled clusters.
Step 2	Set Up Alternate Number, on page 189.	(Optional) If you want to set up alternate numbers that you can dial between clusters, configure alternate number replication.
Step 3	Set Up Advertised Pattern for Alternate Numbers, on page 190.	(Optional) If you want to summarize your alternate numbers with a pattern, set up an advertised pattern, and assign a PSTN failover rule for the pattern.
Step 4	Set Up PSTN Failover, on page 191.	(Optional) If you want to set up a PSTN failover number for specific directory URIs or alternate numbers, assign an alternate number as the PSTN failover number for all the directory URIs and alternate numbers that are associated to a specific directory number.
Step 5	Assign Partitions for Learned Numbers and Patterns, on page 191.	(Optional) Assign route partitions to the alternate numbers and patterns that the local cluster learns through ILS.
Step 6	Block a Learned Pattern, on page 192.	(Optional) To prevent a local Unified Communications Manager cluster from routing calls to a learned alternate number or learned alternate number pattern, you can configure a local blocking rule on that cluster.
Step 7	Set Database Limits for Learned Data, on page 193.	Set a database limit to determine the number of learned objects that Unified Communications Manager can write to the local database.
Step 8	Import Global Dial Plan Data, on page 193.	(Optional) If you want your ILS network to interoperate with a Cisco TelePresence Video Communication Server or third-party call control system, import directory URI catalogs from a CSV file for the other system into any hub cluster in the ILS network.

What to do next

If you want to dial directory universal resource indicators (URIs) across clusters, set up URI dialing in the local cluster. For details, see the URI Dialing Overview, on page 195.

Enable ILS Support for Global Dial Plan Replication

To enable ILS support for Global Dial Plan Replication in the local cluster, follow this procedure:

Procedure

Step 1 Log in to the Cisco Unified Communications Manager publisher node.

Step 2 From Cisco Unified CM Administration, choose **Advanced Features** > **ILS Configuration**.

Step 3 Check the **Exchange Global Dial Plan Replication Data with Remote Clusters** check box.

Step 4 In the **Advertised Route String** text box, enter a route string for the local cluster.

Step 5 Click **Save**.

Set Up Alternate Number

Create an enterprise alternate number or +E.164 alternate number and associate the alternate number with a directory number. When you dial the alternate number, the phone that is registered to the associated directory number, rings.

Note Each alternate number that you set up must associate with a single directory number. However, that directory number can associate to both an enterprise alternate number and a +E.164 alternate number at the same time.

Before you begin

Enable ILS Support for Global Dial Plan Replication, on page 189.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Directory Number**.

Step 2 From the **Find and List Directory Numbers** window, find and select the directory number to which you want to associate the alternate number.

Step 3 From the **Directory Number Configuration** window, click one of the following options depending on the type of alternate number that you want to assign:

- **Add Enterprise Alternate Number**.
- **Add +E.164 Alternate Number**.

Step 4 In the **Number Mask** field, enter the number mask that you want to apply to the directory number.

The **Alternate Number** field displays how the alternate number appears after Cisco Unified Communications Manager applies the number mask.

Step 5 (Optional) If you want to enable local routing for the alternate number, perform the following steps:

a) Check the **Add to Local Route Partition** check box.

b) From the **Route Partition** drop-down list, choose a route partition that is assigned to a local calling search space.

Step 6 (Optional) If you want to use a number pattern to set up intercluster routing for this alternate number, click **Save**.

Step 7 (Optional) If you want to set up intercluster routing for this alternate number, check the **Advertise Globally via ILS** check box for this alternate number.

Step 8 (Optional) If you want to assign a PSTN failover number to this alternate number, from the **PSTN failover** drop-down list, assign a number as the PSTN failover.

Step 9 Click **Save**.

What to do next

Set Up Advertised Pattern for Alternate Numbers, on page 190.

Set Up Advertised Pattern for Alternate Numbers

Use advertised patterns to summarize a range of Enterprise alternate numbers or E.164 alternate numbers. You can advertise the pattern to the ILS network to enable intercluster calling to numbers that match the pattern.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Global Dial Plan Replication** > **Advertised Patterns**.

Step 2 From the **Find and List Advertised Patterns** window, do either of the following:

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

Step 3 In the **Pattern** field, enter the number pattern. For example, 54XXX summarizes a range of numbers between 54000 - 54999.

Step 4 In the **Pattern Type** field, select the pattern type: **Enterprise Number Pattern** or **E.164 Number Pattern**.

Step 5 From the radio buttons, select whether you want to apply a PSTN Failover.

- **Don't use PSTN Failover**
- **Use Pattern as PSTN Failover**
- **Apply Strip Digits and Prepend Digits to Pattern and Use for PSTN Failover**—If you choose this option, enter the digits in the **PSTN Failover Strip Digits** and **PSTN Failover Prepend Digits** fields.

Step 6 Click **Save**.

Set Up PSTN Failover

Perform the following procedure to assign a PSTN failover number for directory URIs or alternate numbers and advertise that PSTN failover number to the ILS network. Remote clusters can use the PSTN failover number for calls to learned directory URIs or learned alternate numbers.

Before you begin

Set Up Advertised Pattern for Alternate Numbers, on page 190.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Directory Number**.

Step 2 From the **Find and List Directory Numbers** window, find and select the directory number that is associated to the directory URI or alternate number for which you want to assign a PSTN failover number.
The appears.

Step 3 (Optional) If the alternate number that you want to use as the PSTN failover does not exist, in the **Directory Number Configuration** window, choose one of the following options depending on the type of alternate number that you want to assign:

- **Add Enterprise Alternate Number**.
- **Add +E.164 Alternate Number**.

Step 4 In the **PSTN Failover** drop-down list, choose the alternate number that you want to use as the PSTN failover.

Step 5 Click **Save**.

Cisco Unified Communications Manager associates that PSTN failover number to that directory number. Global Dial Plan Replication advertises that number to the ILS network as the PSTN failover number for all the directory URIs and alternate numbers that are associated to that directory number.

What to do next

Assign Partitions for Learned Numbers and Patterns, on page 191.

Assign Partitions for Learned Numbers and Patterns

You must assign learned numbers and learned patterns to a partition. You can define your own partitions or use the predefined default partitions. Unified Communications Manager is installed with the following predefined partitions for learned alternate numbers and number patterns:

- Global Learned Enterprise Numbers.
- Global Learned E.164 Numbers.
- Global Learned Enterprise Patterns.
- Global Learned E.164 Patterns.

Note You cannot assign a learned number or learned pattern to a NULL partition.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Global Dial Plan Replication** > **Partitions for Learned Numbers and Patterns**.

Step 2 Configure the fields in the **Partitions for Learned Numbers and Patterns** window. For more information on the fields and their configuration options, see the system Online Help.

Step 3 Click **Save**.

Note The route partition must also exist in the calling search space that is used by the calling party in order for calls to be placed to numbers in the partition.

Block a Learned Pattern

Complete this optional task if you want to set up a blocking rule that prevents the local cluster from routing calls to specific enterprise alternate numbers, +E.164 alternate numbers, or number patterns that were learned through the ILS.

Before routing a call to a learned number or learned pattern, ILS checks to see if a local blocking rule matches the dial string. If the blocking rule matches, Unified Communications Manager does not route the call.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Global Dial Plan Replication** > **Block Learned Numbers and Patterns**.

Step 2 Perform one of the following tasks:

- Click **Find** and select an existing blocking rule to edit.
- Click **Add New** to create a new blocking rule.

Step 3 In the **Pattern** field, enter the pattern or number that you want to block. For example, 206XXXXXXX can be used to block calls to 2065551212.

Step 4 If you want to block calls based on the dial string prefix, enter the **Prefix**.

Step 5 If you want to block calls from being sent to a specific cluster, enter the **Cluster ID** of the cluster.

Step 6 From the **Pattern Type** drop-down list, select how you want to apply the blocking rule:

- **Any**—Choose this option if the blocking rule applies to both enterprise number patterns and +E.164 patterns.
- **Enterprise Pattern**—Choose this option if the blocking rule applies to enterprise number patterns only.
- **+E.164 Pattern**—Choose this option if the blocking rule applies to +E.164 number patterns only.

Step 7 Click **Save**.

Set Database Limits for Learned Data

Set a database limit to determine the number of learned objects that Unified Communications Manager can write to the local database.

Procedure

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

Step 2 Choose the **Server** where you want to configure the parameter.

Step 3 From the **Service** drop-down list, choose **Cisco Intercluster Lookup Service (Active)**. If the service does not appear as active, ensure that the service is activated in Cisco Unified Serviceability.

Step 4 Under **Clusterwide Parameters (ILS)** section, set an upper limit for the **ILS Max Number of Learned Objects in Database** service parameter.

Step 5 Click **Save**.

Note This service parameter determines the maximum number of entries that Unified Communications Manager can write to the database for data that is learned through ILS. The default value of the service parameter is 100,000 while the maximum value of the service parameter is 1,000,00

If you reduce the service parameter to a value that is lower than the current number of ILS-learned entries that are saved in the database, Unified Communications Manager does not write additional ILS learned objects to the database. However, the existing database entries remain.

Import Global Dial Plan Data

Use this procedure if you are interoperating with a Cisco TelePresence Video Communications Server, a third-party call control system, or another system that is not running ILS. You can import a catalog of directory URIs, +E.164 patterns and PSTN failover rules from the other system into a hub cluster in the ILS network. ILS replicates the catalog throughout the ILS network so that the clusters can place calls to the other system.

Before you begin

Export your dial plan catalogs from the other system to a CSV file.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Global Dial Plan RepIication** > **Imported Global Dial Plan Catalog**.

Step 2 From the **Find and List Imported Global Dial Plan Catalogs** window, perform one of the following tasks:

- Click **Find** and select an existing catalog from the resulting list.
- Click **Add New** to add a new catalog.

Step 3 From the **Imported Global Dial Plan Catalog Settings** window, in the **Name** field, enter a unique name to identify the catalog that you want to import.

Step 4 (Optional) In the **Description** field, enter a description of the catalog.

Step 5 In the **Route String** field, create a route string for the system from which you are importing the catalog.

Note Route strings can be up to 250 alphanumeric characters long and can include dots and dashes.

Step 6 Click **Save**.

Step 7 From Cisco Unified CM Administration, choose **Bulk Administration** > **Upload/Download Files**.

- Click **Add New**.
- Click **Browse** and select the CSV file for the catalog that you want to import.

Note Ensure that the CSV file that you use for the import is compatible with the version of Cisco Unified Communications Manager. For example, a CSV file that is compatible to import into Version 9.0(1) is not compatible with Version 10.0(1).

Step 8 In the **Select the Target** drop-down list, select **Imported Directory URIs and Patterns**.

Step 9 In the **Select Transaction Type** drop-down list, select **Insert Imported Directory URIs and Patterns**.

Step 10 Click **Save**.

Step 11 From Cisco Unified CM Administration, choose **Bulk Administration** > **Directory URIs and Patterns** > **Insert Imported Directory URIs and Patterns**.

Step 12 In the **File Name** drop-down list, choose the CSV file that contains the catalog that you want to import.

Step 13 In the **Imported Directory URI Catalog** drop-down list, choose the catalog that you named in the **Imported Global Dial Plan Catalog** window.

Step 14 In the **Job Description** text box, enter a name for the job that you are about to run.

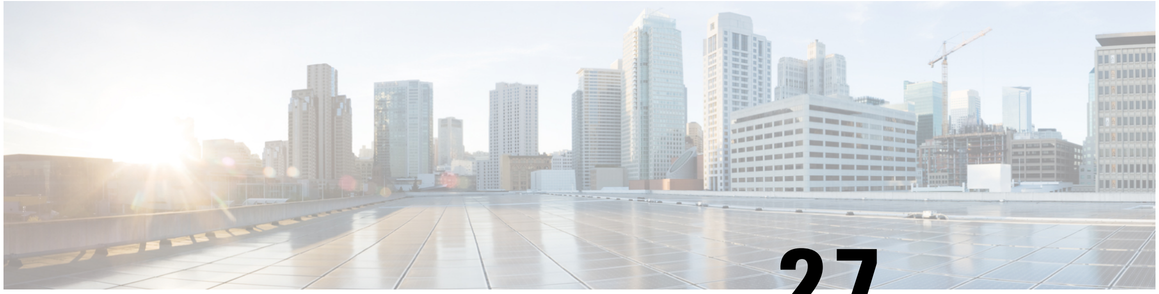
Step 15 Perform one of the following steps:

- If you want to run the job now, select the **Run Immediately** option, and click **Submit**.
- If you want to schedule the job to run at a specified time, select the **Run Later** radio button and click **Submit**.

Note If you choose the **Run Later** option, you must use the Bulk Administration Job Scheduler to schedule when the job runs.

Cisco Unified Communications Manager saves all imported +E.164 patterns to the Global Learned +E.164 Patterns partition.

Note You can also export all locally configured directory URIs, +E.164 number patterns, and their associated PSTN failover rules to a CSV file that you can import into the other call control system. Refer to the menus at **Bulk Administration** > **Directory URIs and Patterns** > **Export Local Directory URIs and Patterns** for details.



CHAPTER 27

Configure URI Dialing

URI Dialing Overview

Unified Communications Manager supports dialing using directory URIs for call addressing. A directory URI is a uniform resource identifier, a string of characters that can be used to identify a directory number. Directory URIs look like email addresses and follow the username@host format where the host portion is an IPv4 address or a fully qualified domain name. If that directory number is assigned to a phone, Unified Communications Manager can route calls to that phone using the directory URI. URI dialing is available for SIP and SCCP endpoints that support directory URIs.

Directory URI Format

Directory URIs are alphanumeric strings that consist of a user and a host address separated by the @ symbol.

Cisco Unified Communications Manager supports the following formats for directory URIs:

- user@domain (for example, joe@cisco.com)
- user@ip_address (for example, joe@10.10.10.1)

The system supports the following formats in the user portion of a directory URI (the portion before the @ symbol):

- Accepted characters are a-z, A-Z, 0-9, !, $, %, &, *, _, +, ~, -, =, , ?, , ‘, ,, ., /, (and) .
- The user portion has a maximum length of 47 characters.
- Cisco Unified Communications Manager automatically applies percent encoding to the following characters when the directory URI is saved in the database:

  # % ^ ` { } | \ : ” < > [ ] \ ‘ and spaces.

Note The user portion of a directory URI is case sensitive by default. You can edit the user portion to be case insensitive by editing the **URI Lookup Policy** enterprise parameter.

When you apply percent encoding, the digit length of the directory URI increases. For example, if you input joe smith#@cisco.com (20 characters) as a directory URI, Unified Communications Managerstores the directory URI in the database as joe%20smith%23@cisco.com (24 characters). Due to database restrictions, the **Directory URI** field has a maximum length of 254 characters.

Cisco Unified Communications Manager supports the following formats in the host portion of a directory URI (the portion after the @ symbol):

- Supports IPv4 addresses or fully qualified domain names.
- Accepted characters are alphanumeric characters, hyphens (-), and dots (.).
- The host portion cannot start or end with a hyphen (-).
- The host portion cannot have two dots in a row.
- The host portion has a minimum length of two characters.
- The host portion is not case sensitive.

Note Within **Cisco Unified Communications Manager Administration**, when you use Bulk Administration to import a CSV file that contains directory URIs with embedded double quotes and commas, you must enclose the entire directory URI in double quotes (").

Call Forward to URI

- Call-forwarding to URIs won't be possible from physical phones.
- Call-forward to a URI can only be configured through applications if that URI is already in the Unified Communications Manager database. If the URI is not in the database, then the application will error out "Call Forward Setting Failed /n Failed to forward calls to: New Number" while trying to configure call-forward.
- Call-forward can be configured for any URI, whether the URI exists in the database or not through the Unified Communications Manager Administration page.
- You can configure call-forwards on the **Cisco Unified Communications Self Care Portal** > **End User** Page to any URI, regardless of whether it exists in the database. The 'Percent Encoding' must be used when entering these characters **# % ^ ` { } | \ : ? < > [ ] \ ‘** . For example, **%3A** is used for mentioning **:** and **%20** is used for mentioning space.
- You must provide "**mobile%3A%2012345@cisco.com**" under the Call-Forward section of the **Cisco Unified Communications Self Care Portal** > **End User** page, if you need to forward calls to the URI "mobile: 12345@cisco.com".

URI Dialing Prerequisites

Before you configure the URI dialing, you must set up an ILS network and enable Global Dial Plan Replication in the ILS network. Refer the following sections to complete this task:

- Global Dial Plan Replication Task Flow, on page 188
- ILS Configuration Task Flow, on page 174

URI Dialing Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Assign directory URIs to the local cluster in the network: • Assign Directory URI to Users, on page 198 • Associate Directory URI with Directory Numbers, on page 198	Provision end users into your system and assign directory URI to those end users. Also, configure a directory number and associate a directory URI with that directory number. **Note** For both end user configuration and director number configuration, you can also use Bul Administration to import end users, director URIs, directory numbers, and phones into Ci Unified Communications Manager. For mor information, see the *Bulk Administration Gu for Cisco Unified Communications Manage* http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanag products-maintenance-guides-list.html.
Step 2	Assign Default Directory URI Partition, on page 199	Assign the default directory URI partition to an existing partition that is located in a calling search space.
Step 3	Configure SIP Profiles for URI Dialing, on page 199	Configure the SIP profiles to configure intercluster URI dialing in your network.
Step 4	Configure SIP Trunks for URI Dialing, on page 200	Configure whether Cisco Unified Communications Manager inserts a directory number, a directory URI, or a blended address for outgoing SIP messages.
Step 5	Configure SIP Route Patterns, on page 201	Configure SIP route patterns to route intercluster directory URI calls.
Step 6	Repeat step 1 to step 5 for all the clusters in your ILS network.	Perform this step if you have multiple clusters in your ILS network.

	Command or Action	Purpose
Step 7	Import Directory URI Catalogs, on page 201	(Optional) If you want to place directory URI calls to a Cisco TelePresence Video Communications Server, or a third-party call control system, import directory URI catalogs from a CSV file for the other system into any hub cluster in the ILS network.

Assign Directory URI to Users

Perform the following steps to assign a directory URI to an end user.

Procedure

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

Step 2 In the **Find and List Users** window, specify the search criteria and click **Find**.

Step 3 Choose a user from the resulting list. The **End User Configuration** window appears.

Step 4 In the **Directory URI** field, enter a directory URI that you want to associate to this end user. A directory URI looks like an email address and follows the user@host format.

Note If you enter a directory URI and also enter a directory number in the **Primary Extension** field, this directory URI automatically becomes the primary directory URI that is associated to that directory number.

Step 5 Click **Save**.

Associate Directory URI with Directory Numbers

Perform the following procedure to associate a directory URI with a directory number. If that directory number is assigned to a phone, Cisco Unified Communications Manager allows you to dial that phone using the directory URI.

Before you begin

Assign Directory URI to Users, on page 198

Procedure

Step 1 In Cisco Unified CM Administration, choose **Device** > **Phone**. The **Find and List Phones** window appears.

Step 2 Specify the filter criteria and click **Find**.

Step 3 Click on the device for which you want to associate the directory number. The **Phone Configuration** window appears.

Step 4 In the **Association** pane:

- Click on an existing directory number.
- Click on **Add a new DN** if no directory numbers are configured.

Step 5 In the **Directory Number Configuration** window, enter the directory URI address in the **URI** text box.

Step 6 From the **Partition** drop-down list, choose the partition to which the directory URI belongs.

Ensure that the directory URI that you enter is unique within the partition that you choose. If you do not want to restrict access to the URI, choose **None** for the partition.

Step 7 Click **Save**.

What to do next

Assign Default Directory URI Partition, on page 199

Assign Default Directory URI Partition

Perform the following procedure to assign a default directory URI partition.

Before you begin

Associate Directory URI with Directory Numbers, on page 198

Procedure

Step 1 In Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**. The **Enterprise Parameters Configuration** window appears.

Step 2 For the **Directory URI Alias Partition** in the **End User Parameters** area, choose an existing partition that is in an existing calling search space.

Step 3 Click **Save**.

What to do next

Configure SIP Profiles for URI Dialing, on page 199

Configure SIP Profiles for URI Dialing

Before you begin

Assign Default Directory URI Partition, on page 199

Procedure

Step 1 In Cisco Unified CM Administration, choose **Device** > **Device Settings** > **SIP Profile**. The **Find and List SIP Profiles** window appears.

Step 2 Enter the appropriate search criteria and click **Find**. A list of existing SIP profiles appear.

Step 3 Select the SIP profile that you want to view. The **SIP Profile Configuration** window appears.

Step 4 From the **Dial String Interpretation** drop-down list, choose one of the following options:

- **Always treat all dial strings as URI addresses**—Select this option to treat the address of incoming calls as URI addresses.
- **Phone number consists of characters 0–9, A–D, *, and + (others treated as URI addresses)**—Select this option to treat the incoming call as a directory number if all the characters in the user portion of the SIP identity header fall within this range. If the user portion of the address uses any characters that do not fall within this range, the address is treated as a URI.
- **Phone number consists of characters 0-9, *, and + (others treated as URI addresses**—Select this option to treat the incoming call as a directory number if all the characters in the user portion of the SIP identity header fall within this range. If the user portion of the address uses any characters that do not fall within this range, the address is treated as a URI.

Step 5 Check the **Use Fully Qualified Domain Name in SIP Requests** check box for all the SIP profiles in your network.

Step 6 Click **Apply Config**.

What to do next

Configure SIP Trunks for URI Dialing, on page 200

Configure SIP Trunks for URI Dialing

If you are deploying URI dialing, configure the contact header addressing policy for the SIP trunks in your network. Cisco Unified Communications Manager can insert a directory number, directory URI, or a blended address that includes both the directory number and directory URI in the SIP identity headers for outgoing SIP messages.

Procedure

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

Step 2 Click **Find** and select an existing SIP trunk.

Step 3 In the **Outbound Calls** area, select one of the following from the **Calling and Connected Party Info Format** drop-down list:

- **Deliver DN only in connected party**—In outgoing SIP messages, Unified Communications Manager inserts the calling party's directory number in the SIP contact header information. This is the default setting.
- **Deliver URI only in connected party, if available**—In outgoing SIP messages, Unified Communications Manager inserts the sending party's directory URI in the SIP contact header. If a directory URI is not available, Unified Communications Manager inserts the directory number instead.
- **Deliver URI and DN in connected party, if available**—In outgoing SIP messages, Unified Communications Manager inserts a blended address that includes the calling party's directory URI and directory number in the SIP contact headers. If a directory URI is not available, Unified Communications Manager includes the directory number only.

Step 4 Click **Save**.

Configure SIP Route Patterns

You must configure SIP route patterns to route intercluster directory URI calls.

Follow these steps to configure SIP route patterns.

Before you begin

Configure SIP Trunks for URI Dialing, on page 200

Procedure

Step 1 In Cisco Unified CM Administration, choose **Call Routing** > **SIP Route Pattern**.

Step 2 Choose one of the following options:

- To add a new SIP route pattern, click the **Add New** button.
- To modify the settings for an existing SIP route pattern, enter the search criteria, click **Find**, and choose a SIP route pattern from the resulting list.

Step 3 Configure the fields in the **SIP Route Pattern Configuration** window. See the online help for more information about the fields and their configuration options.

Step 4 Click **Save**.

What to do next

(Optional) Import Directory URI Catalogs, on page 201

Import Directory URI Catalogs

Cisco Unified Communications Manager allows you to import global dial plan data from a CSV file into any hub cluster in an ILS network and ILS replicates the imported global dial plan data throughout the ILS network allowing you to interoperate Cisco Unified Communications Manager with a Cisco TelePresence Video Communications Server or a third-party call control system.

(Optional) To import directory URI catalogs, follow this procedure:

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Global Dial Plan RepIication** > **Imported Global Dial Plan Catalog**.

Step 2 From the **Find and List Imported Global Dial Plan Catalogs** window, perform one of the following tasks:

- Click **Find** and select an existing catalog from the resulting list.
- Click **Add New** to add a new catalog.

Step 3 From the **Imported Global Dial Plan Catalog Settings** window, in the **Name** field, enter a unique name to identify the catalog that you want to import.

Step 4 (Optional) In the **Description** field, enter a description of the catalog.

Step 5 In the **Route String** field, create a route string for the system from which you are importing the catalog.

Note Route strings can be up to 250 alphanumeric characters long and can include dots and dashes.

Step 6 Click **Save**.

Step 7 From Cisco Unified CM Administration, choose **Bulk Administration** > **Upload/Download Files**.

- Click **Add New**.
- Click **Browse** and select the CSV file for the catalog that you want to import.

Note Ensure that the CSV file that you use for the import is compatible with the version of Cisco Unified Communications Manager. For example, a CSV file that is compatible to import into Version 9.0(1) is not compatible with Version 10.0(1).

Step 8 In the **Select the Target** drop-down list, select **Imported Directory URIs and Patterns**.

Step 9 In the **Select Transaction Type** drop-down list, select **Insert Imported Directory URIs and Patterns**.

Step 10 Click **Save**.

Step 11 From Cisco Unified CM Administration, choose **Bulk Administration** > **Directory URIs and Patterns** > **Insert Imported Directory URIs and Patterns**.

Step 12 In the **File Name** drop-down list, choose the CSV file that contains the catalog that you want to import.

Step 13 In the **Imported Directory URI Catalog** drop-down list, choose the catalog that you named in the **Imported Global Dial Plan Catalog** window.

Step 14 In the **Job Description** text box, enter a name for the job that you are about to run.

Step 15 Perform one of the following steps:

- If you want to run the job now, select the **Run Immediately** option, and click **Submit**.
- If you want to schedule the job to run at a specified time, select the **Run Later** radio button and click **Submit**.

Note If you choose the **Run Later** option, you must use the Bulk Administration Job Scheduler to schedule when the job runs.

Cisco Unified Communications Manager saves all imported +E.164 patterns to the Global Learned +E.164 Patterns partition.

PART IV

Configure Call Admission Control

CHAPTER 28

Call Admission Control Overview

About Call Admission Control

Use call admission control (CAC) to regulate voice quality over a WAN link.

Voice quality can degrade when too many active calls exist on a link and the amount of bandwidth is oversubscribed. Call admission control regulates voice quality by limiting the number of calls that can be active at the same time on a particular link. Call admission control does not guarantee a particular level of audio quality on the link, but it does allow you to regulate the amount of bandwidth that active calls on the link consume.

Call admission control operates by rejecting a call for bandwidth and policy reasons. When a call is rejected due to call admission control, the phone of the called party does not ring, and the caller receives a busy tone. The caller also receives a message on their phone, such as “Not enough bandwidth.” If you have enabled automated alternate routing (AAR), call admission control automatically diverts calls to alternate public switched telephone network (PSTN) routes when WAN bandwidth is not available.

Call Admission Control Configuration

Choose from one of the following task flows to implement call admission control (CAC).

Task Flow	Description
Enhanced Locations Call Adminssion Control Task Flow	Use enhanced locations CAC in distributed deployments, where multiple clusters manage devices in the same physical sites using the same WAN uplinks. Enhanced locations CAC lets you regulate voice quality by limiting the amount of bandwidth that is available for calls over links between the locations. It also allows you to control call admissions for immersive video calls, such as TelePresence, separately from other video calls.
RSVP Configuration Task Flow	Use RSVP to implement call admission control in complex, multi-tiered topologies that include IP telephony and videoconferencing applications. RSVP is also able to handle dynamic changes to bandwidth.

CHAPTER 29

Configure Enhanced Locations Call Admission Control

Enhanced Locations Call Admission Control Overview

Enhanced locations call admission control (CAC) provides control over WAN bandwidth in complex WAN topologies as well as distributed deployments, where multiple clusters manage devices in the same physical sites using the same uplinks. Enhanced locations CAC also allows you to control call admissions for immersive video calls, such as TelePresence separately from other video calls.

You can effectively share locations between clusters by enabling the clusters to communicate with one another to reserve, release, and adjust allocated bandwidth for the same locations across clusters.[1]

Network Modeling

To define how your system handles media, you structure your network model around the concepts of locations and links.

A location represents a local area network (LAN). It could contain endpoints or simply serve as a transit location between links for wide area network (WAN) network modeling.

Links interconnect locations and are used to define bandwidth available between locations. Links represent the WAN link.

Weights are measurements of bandwidth pathways. These are used on links to provide a cost to the effective path. Weights are provided when there is more than one path between any two locations.

Your system calculates shortest paths (least cost) from all locations to all locations and builds effective paths. These have the least overall weight and are the most efficient pathways.

[1] Locations Media Resource Audio Bit Rate Policy service parameter determines the bit rate value to deduct from the audio bandwidth pools within and between the locations of the parties for an audio-only call when a media resource such as a transcoder is inserted into the media path and for more complex scenarios. This service parameter does not have any impact if there is no media in one of the call legs. In such cases, location bandwidth manager deducts the maximum hop bandwidth that is configured for the source destination from the available bandwidth of that location.

Your system tracks bandwidth across any link that the network model indicates from originating location to terminating location.

Location Bandwidth Manager

The location bandwidth manager (LBM) service computes the effective path from source location to destination location. It provides useful functions behind the scenes, such as handling bandwidth requests from Unified Communications Manager call control and replicating bandwidth information within the cluster and between clusters. You can find the configured and realtime information this function provides in Serviceability Administration.

Locations Media Resource Audio Bit Rate Policy service parameter determines the bit rate value to deduct from the audio bandwidth pools within and between the locations of the parties for an audio-only call when a Media Resource such as a transcoder is inserted into the media path and for more complex scenarios. This service parameter does not have any impact if there is no media in one of the call legs. In such cases, location bandwidth manager deducts the maximum hop bandwidth configured for the source destination from the available bandwidth of that location.

Note Do not change the Location Bandwidth Manager bandwidth or link configurations during production hours as that could unnecessarily spike CPU utilization on the server.

Intercluster Enhanced Locations Call Admission Control

The intercluster function extends enhanced locations CAC network modeling across multiple clusters. Each cluster manages its own network topology. They then propogate their topologies to other clusters that are configured In the LBM intercluster replication network.

A shared location is a location that is configured with the same name on clusters participating in a the LBM replication network.

This type of location serves the following purposes:

- Enables clusters to share their respective configured topologies with one another
- Lets multiple clusters perform CAC on the same locations

Enhanced Locations Call Admission Control Prerequisites

- Unified Communications Manager and location bandwidth manager (LBM) manage bandwidth for all types of devices, including IP phones, gateways, and H.323 and SIP trunk destinations. However, intercluster enhanced locations CAC requires SIP intercluster trunks that are assigned to the system shadow location, which is a special location that has no links to other locations and no bandwidth allocations. All other types of devices are supported only when assigned to ordinary (fixed) locations.
- Unified Communications Manager and LBM do not manage bandwidth for media resources. For cases in which media resources change the bandwidth requirement for a call, you can change a global parameter setting that determines whether the minimum or maximum bandwidth is reserved.

Enhanced Locations Call Admission Control Task Flow

Procedure

	Command or Action	Purpose
Step 1	Activate the LBM Service, on page 210	Verify whether the Cisco Location Bandwidth Manager service is activated. For a new system install, you must manually enable the service on the desired nodes. For enhanced locations CAC to work properly, one instance of this service must run on each cluster.
Step 2	Create an LBM Group, on page 210	If LBM is not running on the same node, configure an LBM group and assign the LBM group to the server. The LBM group lets you optimize network delay and performance. Each server must communicate with an LBM service to determine the available bandwidth for each call and to deduct bandwidth for the duration of each call.
Step 3	Configure Locations and Location Links, on page 211	Configure locations to implement call admission control in a centralized call-processing system. A location represents a local area network (LAN), and can contain endpoints or simply serve as a transit location between links for wide area network (WAN) network modeling. Locations provide bandwidth accounting within a location as well as in or out of a location. Links provide bandwidth accounting between locations and interconnect locations.
Step 4	(Optional) Assign Intra-Location Bandwidth, on page 211	Assign intra-location bandwidth to the location, if you do not want to use the default of unlimited bandwidth. By default, when you create a new location, a link from the newly added location to the Hub_None is added as well, with unlimited audio bandwidth, 384 kbps video bandwidth and 384 kbps immersive video bandwidth. You can adjust this allotment to match your network model.
Step 5	Establish External Communication, on page 212	Configure the LBM hub group to allow the LBM servers acting as hubs to find LBM servers in remote clusters. This step establishes external communication with those clusters. An LBM service becomes a hub when an LBM hub group is assigned to it. Any LBM servers that are assigned an LBM hub group establish

	Command or Action	Purpose
		communication with all other LBM servers that are assigned the same or an overlapping LBM hub group.
Step 6	Configure the SIP Intercluster Trunk for Enhanced Location Call Admission, on page 212	Assign a SIP intercluster trunk (ICT) to the shadow location to establish proper intercluster operation. SIP trunks that are linked to devices with a specific location, such as SIP gateways, can be assigned to ordinary locations. A shadow location is a special location that contains no links to other locations and no bandwidth allocations.
Step 7	(Optional) Deduct Audio Bandwidth from Audio Pool for Video Calls, on page 213	Use this procedure if you want to split the audio and video bandwidth deductions into separate pools for video calls. By default, the system deducts the bandwidth requirement for both the audio stream and video stream from the video pool for video calls.

Activate the LBM Service

Verify whether the Cisco Location Bandwidth Manager service is activated. For a new system install, you must manually enable the service on the desired nodes. For enhanced locations CAC to work properly, one instance of this service must run on each cluster.

Procedure

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

Step 2 From the **Server** drop-down list, choose a server, and then click **Go**.

Step 3 If needed, check the **Cisco Location Bandwidth Manager** check box.

Step 4 Click **Save**.

Create an LBM Group

If LBM is not running on the same node, configure an LBM group and assign the LBM group to the server. The LBM group lets you optimize network delay and performance. Each server must communicate with an LBM service to determine the available bandwidth for each call and to deduct bandwidth for the duration of each call.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Location Info** > **Location Bandwidth Manager Group**.

Step 2 Perform one of the following tasks:

- Click **Find** and then choose an existing LBM group from the resulting list to modify the settings for an existing LBM group.
- Click **Add New** ro add a new LBM group.

Step 3 Configure the fields on the **Location Bandwidth Manager Group Configuration** window. For more information on the fields and their configuration options, see the system Online Help.

Step 4 Click **Save**.

Configure Locations and Location Links

Configure locations to implement call admission control in a centralized call-processing system. A location represents a local area network (LAN), and can contain endpoints or simply serve as a transit location between links for wide area network (WAN) network modeling. Locations provide bandwidth accounting within a location as well as in or out of a location. Links provide bandwidth accounting between locations and interconnect locations.

Procedure

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

Step 2 Perform one of the following tasks:

- Click **Find** and then choose an existing location from the resulting list, to modify the settings for an existing location.
- Click **Add New** to add a new location.

Step 3 Configure the fields on the **Location Configuration** window. For more information on the fields and their configuration options, see the system Online Help.

Step 4 Click **Save**.

Assign Intra-Location Bandwidth

Assign intra-location bandwidth to the location, if you do not want to use the default of unlimited bandwidth. By default, when you create a new location, a link from the newly added location to the Hub_None is added as well, with unlimited audio bandwidth, 384 kbps video bandwidth and 384 kbps immersive video bandwidth. You can adjust this allotment to match your network model.

Tip If the audio quality is poor or choppy, lower the bandwidth setting. For example, for ISDN use multiples of 56 kbps or 64 kbps.

Procedure

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

Step 2 Enter search criteria, click **Find**, and then choose a location from the resulting list.

Step 3 Click **Show Advanced** to show the intra-location bandwidth fields.

Step 4 If required, choose the **kbps** radio button for **Audio Bandwidth**, and then enter a bandwidth value in the text box.

Step 5 If required, choose the **kbps** radio button for **Video Bandwidth**, and then enter a bandwidth value in the text box.

Step 6 If required, choose the **kbps** radio button for **Immersive Video Bandwidth**, and then enter a bandwidth value in the text box.

Step 7 Click **Save**.

Establish External Communication

Configure the LBM hub group to allow the LBM servers acting as hubs to find LBM servers in remote clusters. This step establishes external communication with those clusters. An LBM service becomes a hub when an LBM hub group is assigned to it. Any LBM servers that are assigned an LBM hub group establish communication with all other LBM servers that are assigned the same or an overlapping LBM hub group.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Location Info** > **Location Bandwidth Manager (LBM) Intercluster Replication Group**.

Step 2 Perform one of the following tasks:

- Click **Find** to modify the settings for an LBM intercluster replication group, and choose an existing LBM intercluster replication group from the resulting list.
- Click **Add New** to add a new LBM intercluster replication group.

Step 3 Configure the fields on the **Location Bandwidth Manager Intercluster Replication Group Configuration** window. For more information on the fields and their configuration options, see the system Online Help.

Step 4 Click **Save**.

Configure the SIP Intercluster Trunk for Enhanced Location Call Admission

Assign a SIP intercluster trunk (ICT) to the shadow location to establish proper intercluster operation. SIP trunks that are linked to devices with a specific location, such as SIP gateways, can be assigned to ordinary locations. A shadow location is a special location that contains no links to other locations and no bandwidth allocations.

Before you begin

You need to have a configured SIP intercluster trunk. See SIP Trunk Configuration Task Flow, on page 99 for more information.

Procedure

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

Step 2 Enter search criteria, click **Find**, and then choose an existing SIP intercluster trunk from the resulting list.

Step 3 From the **Location** drop-down list, choose **Shadow**.

Step 4 Click **Save**.

Deduct Audio Bandwidth from Audio Pool for Video Calls

Use this procedure if you want to split the audio and video bandwidth deductions into separate pools for video calls. By default, the system deducts the bandwidth requirement for both the audio stream and video stream from the video pool for video calls.

Note When you enable this feature, CAC includes the bandwidth required for the IP/UDP network overhead in the audio bandwidth deduction. This audio bandwidth deduction equates to the audio bit rate plus the IP/UDP network overhead bandwidth requirement. The video bandwidth deduction is the video bit rate only.

Procedure

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

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

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

Step 4 From the **Clusterwide Parameters (Call Admission Control)** area, set the value of the **Deduct Audio Bandwidth Portion from Audio Pool for a Video Call** service parameter to **True**.

Note When you configure the **Deduct Audio Bandwidth Portion from Audio Pool for a Video Call** service parameter to **True**, the video and immersive video parameters are considered as media level and not as session level. Hence, for a video call, you can allocate audio and video bandwidths from audio and video pools respectively for each region and location. The video and immersive video bandwidth limits apply only to the video media stream; not to the combination of the audio and video media streams.

Step 5 Click **Save**.

Enhanced Locations Call Admission Control Interactions and Restrictions

Enhanced Locations Call Admission Control Interactions

Table 18: Enhanced Locations Call Admission Control Interactions

Feature	Interaction
Bandwidth	If there is a conflict in bandwidth capacity or weight assignment on the common links or locations, the local cluster uses the minimum of the assigned values.
Device support	Your system and LBM manage bandwidth for all types of devices, including IP phones, gateways, and H.323 and SIP trunk destinations. However, intercluster enhanced locations CAC requires SIP ICTs assigned to the system shadow location. All other types of devices are supported only when assigned to ordinary (fixed) locations.

Enhanced Locations Call Admission Control Restrictions

Table 19: Enhanced Locations Call Admission Control Restrictions

Restriction	Description
Bandwidth Reservation Path	During network failure conditions, the bandwidth reservation path calculated by Unified Communications Manager might not accurately reflect network conditions. There is no satisfactory way to allow for this scenario in the model.
Bandwidth and Video Capabilities	If video capabilities are enabled, then bandwidth for audio will be allocated from video.
Synchronization	The model created by the system is not perfectly synchronized at all times. Use conservative bandwidth allocations to accommodate this restriction.

CHAPTER 30

Configure Resource Reservation Protocol

RSVP Call Admission Control Overview

Resource Reservation Protocol (RSVP) is a resource-reservation, transport-level protocol for reserving resources in IP networks. You can use RSVP as an alternative to enhanced-locations call admission control (CAC). RSVP reserves resources for specific sessions. A session is a flow that has a particular destination address, destination port, and a protocol identifier (TCP or UDP).

RSVP Call Admission Control Prerequisites

You must use IPv4 addressing. RSVP does not support IPv6 addressing.

RSVP Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure Clusterwide Default RSVP Policy, on page 216	Configure the RSVP policy for all nodes in the cluster.
Step 2	Configure Location-pair RSVP Policy, on page 217	Optional. You can configure the RSVP policy for a specific location pair if you want the location pair to use a different policy than the rest of the cluster.
Step 3	Configure RSVP Retry, on page 218	Configure the frequency and number of RSVP retries.
Step 4	Configure Midcall RSVP Error Handling, on page 218	Configure how the system responds when RSVP fails during a call.

	Command or Action	Purpose
Step 5	Configure MLPP-to-RSVP Priority Mapping, on page 219	Optional. If you use multilevel precedence and preemption (MLPP), map the caller MLPP precedence level to an RSVP priority.
Step 6	Configure RSVP agents.	Perform this IOS procedure on your gateway device. See the documentation for device for information about how to configure an RSVP agent.
Step 7	Configure the Application ID, on page 220	When you configure the RSVP application ID, the system adds an identifier to both the voice and video traffic so that the Cisco RSVP Agent can set a separate bandwidth limit on either type of traffic, based on the identifier it receives.
Step 8	Configure DSCP Marking, on page 220	Configure DSCP marking so that if the RSVP reservation fails, the system can instruct the RSVP agent or endpoint devices to change media Differentiated Services Control Point (DSCP) marking to best effort. Otherwise, an excess of EF-marked media packets can degrade quality of service (QoS) even for flows that have a reservation.

Configure Clusterwide Default RSVP Policy

Configure the RSVP policy for all nodes in the cluster.

Procedure

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

Step 2 In the **Service Parameter Configuration** window, choose a server and choose the Cisco CallManager service.

Step 3 In the **Clusterwide Parameters (System - RSVP)** section, configure the Default Interlocation RSVP Policy service parameter.

You can set this service parameter to the following values:

- No Reservation-No RSVP reservations 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 for audio 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 audio stream succeeds but a reservation for the video stream does not succeed.

What to do next

Choose one of the following options:

- If you want a location pair to use a different policy than the rest of the cluster, Configure Location-pair RSVP Policy, on page 217.
- If you are using the same RSVP policy for all nodes in the cluster, Configure RSVP Retry, on page 218.

Configure Location-pair RSVP Policy

You can configure the RSVP policy for a specific location pair if you want the location pair to use a different policy than the rest of the cluster. When you use this procedure, the RSVP policy that you configure for the location pair overrides the policy that you configured for the cluster.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose the **System** > **Location**.

Step 2 Find one location of the location pair and select this location.

Step 3 To modify the RSVP policy between the selected location and another location, select the other location in the location pair.

Step 4 In the **RSVP Setting** drop-down list, choose an RSVP policy for this location pair.

You can set this field to the following values:

- **Use System Default**–The RSVP policy for the location pair matches the cluster-wide RSVP policy.
- **No Reservation**–No RSVP reservations get made between any two locations.
- **Video Desired (Optional)** –A call can proceed as a best-effort, audio-only call if failure to obtain reservations for both audio and video streams occurs. The RSVP agent continues to attempt RSVP reservation for audio and informs Cisco Unified Communications Manager if reservation succeeds. The system 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.
- **Video Desired**–A video call can proceed as an audio-only call if a reservation for the audio stream succeeds but the reservation for the video stream does not succeed.

What to do next

Configure RSVP Retry, on page 218

Configure RSVP Retry

Use this procedure to configure the frequency and number of RSVP retries.

Before you begin

- Configure Clusterwide Default RSVP Policy, on page 216
- Optional. Configure Location-pair RSVP Policy, on page 217

Procedure

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

Step 2 In the Service Parameter Configuration window, choose a server and choose the Cisco CallManager service.

Step 3 In the Clusterwide Parameters (System - RSVP) section, configure the specified service parameters.

You can set these service parameters to the following values:

- RSVP Retry Timer-Specify the RSVP retry timer value in seconds. If you set this parameter to 0, you disable RSVP retry on the system.
- Mandatory RSVP Midcall Retry Counter-Specify the midcall RSVP retry counter when the RSVP policy specifies Mandatory and midcall error handling option is set to “call fails following retry counter exceeds.” The default value specifies 1 time. If you set the service parameter to -1, retry continues indefinitely until either the reservation succeeds or the call gets torn down.

What to do next

Configure Midcall RSVP Error Handling, on page 218

Configure Midcall RSVP Error Handling

Use this procedure to configure midcall RSVP error handling.

Before you begin

Configure RSVP Retry, on page 218

Procedure

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

Step 2 In the Service Parameter Configuration window, choose a server and choose the Cisco CallManager service.

Step 3 In the Clusterwide Parameters (System - RSVP) section, configure the specified service parameter.

You can set the Mandatory RSVP mid call error handle option service parameter to the following values:

- Call becomes best effort-If RSVP fails during a call, the call becomes a best-effort call. If retry is enabled, RSVP retry attempts begin simultaneously.
- Call fails following retry counter exceeded-If RSVP fails during a call, the call fails after N retries of RSVP, where the Mandatory RSVP Mid-call Retry Counter service parameter specifies N.

What to do next

Configure RSVP agents on your gateway device. See the documentation for device for information about how to configure an RSVP agent. After you have configure RSVP agents on your gateway, return to Cisco Unified Communications Manager Administration and choose one of the following options:

- Optional. Configure MLPP-to-RSVP Priority Mapping, on page 219 if you are using multilevel precedence and preemption in your network.
- Configure the Application ID, on page 220

Configure MLPP-to-RSVP Priority Mapping

Optional. Use the following clusterwide (System - RSVP) service parameters to configure the mapping from a caller MLPP precedence level to RSVP priority:

- MLPP EXECUTIVE OVERRIDE To RSVP Priority Mapping
- MLPP FLASH OVERRIDE To RSVP Priority Mapping
- MLPP FLASH To RSVP Priority Mapping
- MLPP IMMEDIATE To RSVP Priority Mapping
- MLPP PL PRIORITY To RSVP Priority Mapping
- MLPP PL ROUTINE To RSVP Priority Mapping

To locate and configure these service parameters, follow these steps:

Procedure

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

Step 2 In the Service Parameter Configuration window, choose a server and choose the Cisco CallManager service.

Step 3 In the Clusterwide Parameters (System - RSVP) section, configure the specified service parameters.

These service parameters function as follows:

- Cisco Unified Communications Manager maps the caller precedence level to RSVP priority when initiating an RSVP reservation based on the following configuration: the higher the service parameter value, the higher the priority.
- The IOS router preempts the call based on RSVP priority.
- The RSVP agent must notify Cisco Unified Communications Manager about the reason for an RSVP reservation failure, including the cause for preemption.

- Cisco Unified Communications Manager uses the existing MLPP mechanism to notify the preempted calling and called parties about the preemption.

What to do next

Configure RSVP agents on your gateway device. See the documentation for device for information about how to configure an RSVP agent. After you have configure RSVP agents on your gateway, return to Cisco Unified Communications Manager Administration and Configure the Application ID, on page 220.

Configure the Application ID

When you configure the RSVP application ID, the system adds an identifier to both the voice and video traffic so that the Cisco RSVP Agent can set a separate bandwidth limit on either type of traffic, based on the identifier it receives.

Before you begin this procedure, configure RSVP agents on your gateway device. See the documentation for device for information about how to configure an RSVP agent.

Before you begin

To deploy the RSVP application ID in the network, you must use a minimum version of Cisco IOS Release 12.4(6)T or higher on the Cisco RSVP Agent router.

Procedure

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

Step 2 In the **Service Parameter Configuration** window, choose a server and choose the Cisco CallManager service.

Step 3 In the **Clusterwide Parameters (System - RSVP)** section, configure the RSVP Audio Application ID service parameter.

(Default = AudioStream)

Step 4 In the **Clusterwide Parameters (System - RSVP)** section, configure the RSVP Video Application ID

(Default = VideoStream)

What to do next

Configure DSCP Marking, on page 220

Configure DSCP Marking

If the RSVP reservation fails, the system instructs the RSVP agent or endpoint devices (in case a failure to allocate an RSVP agent occurs) to change media Differentiated Services Control Point (DSCP) marking to best effort. Otherwise, an excess of EF-marked media packets can degrade quality of service (QoS) even for flows that have a reservation.

Before you begin

Configure the Application ID, on page 220

Procedure

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

Step 2 In the **Service Parameter Configuration** window, choose a server and choose the Cisco CallManager service.

Step 3 In the **Clusterwide Parameters (System - QoS)** section, configure the **DSCP for Audio Calls When RSVP Fails** service parameter.

Step 4 In the **Clusterwide Parameters (System - QoS)** section, configure the **DSCP for Video Calls When RSVP Fails** service parameter.

PART V

Configure End Users

CHAPTER 31

End User Configuration Overview

About End User Configuration

The chapters in this part describe how to provision and configure end users for your system.

End users are the main consumers of Cisco Unified Communications Manager features. End users can be assigned with phones and directory numbers thereby allowing your end users to make calls and communicate with other users in the system as well as placing calls to external networks such as the PSTN.

For provisioning large numbers of end users at once, Cisco Unified Communications Manager provides the following features:

- LDAP Directory Integration—You can synchronize Cisco Unified Communications Manager with an external LDAP directory thereby allowing you to import end user data from the LDAP directory.
- Bulk Administration Tool—You can use the Bulk Administration Tool to import and configure a large number of end users, and associated user data, from a CSV file in a single operation.

After your end users are provisioned, you can configure user settings such as user profiles that allow your users to provision their own phones, in addition to phone services and credential policies.

End User Configuration

Complete the following task flows to configure end users for your system.

Procedure

	Command or Action	Purpose
Step 1	User Access Configuration Task Flow, on page 231	Plan the roles and access control groups for your end users. Decide whether the system-defined roles and access control groups have the access privileges that your deployment requires or if you need to create new roles and new access control groups.

	Command or Action	Purpose
Step 2	Credential Policy Configuration Task Flow, on page 248	Configure credential policies for your end users.
Step 3	User Profile Configuration Task Flow, on page 252	Configure user profiles for groups of users who meet the same access and functionality requirements. The user profile consists of common phone and phone line settings that can allow you to quickly configure new phones and phone lines for users who use this user profile. You can also enable self-provisioning for users who use this profile.
Step 4	Service Profile Configuration Task Flow, on page 256	Configure a service profile with settings for Unified Communications (UC) services. You can apply the service profile to groups of users who have the same services requirements. The service profile allows you to configure UC services for any new phones provisioned for users who use this service profile.
Step 5	Configure a Feature Group Template, on page 266	Optional. Configure a feature group template to your end users. A feature group template contains a set of common feature configurations as well as an assigned user profile and service profile. For LDAP synchronized users you can assign the feature group template during the LDAP sync thereby assigning a user profile, service profile, line and device templates, and self-provisioning capability to the user.
Step 6	LDAP Synchronization Configuration Task Flow, on page 269	If your deployment includes a company LDAP directory, you can import your end users directly from the LDAP directory into the Cisco Unified Communications Manager database.
Step 7	LDAP Synchronization Configuration Task Flow, on page 269	If you are not importing end users from an LDAP directory, you can use the Bulk Administration Tool to import the end user list, and end user configurations, from a CSV file into the Cisco Unified Communications Manager database. For details on how to use the Bulk Administration Guide to perform bulk transactions to the database, see the *Bulk Administration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

	Command or Action	Purpose
Step 8	Manual End User Configuration Task Flow, on page 280	Optional. Add new users to the database manually.

CHAPTER 32

Configure User Access

User Access Overview

Manage user access to Cisco Unified Communications Manager by configuring the following items:

- Access Control Groups
- Roles
- User Rank

Roles Overview

When you provision end users, you must decide on what roles you want to assign to your users. You can assign roles to an end user, application user, or to an access control group. You can assign multiple roles to a single user.

Each role contains a set of privileges that are attached to a specific resource or application. For example, the Standard CCM End Users role provides users who are assigned that role with access to the Cisco Unified Communications Self Care Portal. You can also assign roles that provide access to resources such as Cisco Unified Communications Manager Administration, Cisco CDR Analysis and Reporting, the Dialed Number Analyzer, and the CTI interface. For most resources with graphical user interfaces, such as a specific configuration window, the privileges that are attached to the role allow the user to view or update data in that window, or in a group of related windows.

Configuring and Assigning Roles

You must decide whether you want to assign standard roles to your users, or create custom roles:

- Standard roles—Standard roles are predefined, default roles that come installed in Cisco Unified Communications Manager. You cannot edit the privileges or modify the role in any way.
- Custom roles—Custom roles are roles that you create. You can create custom roles when there are no standard roles that contain the privileges that you want to assign to your users. For example, if you want

to assign a standard role, but want to modify one of the privileges, you can copy the privileges of the standard role into a custom role and then edit the privileges in that custom role.

Privilege Types

Each role contains a set of privileges that are attached to a specific resource. There are two types of privileges that you can assign to a resource:

- Read—Read privilege gives the user the ability to view the settings for that resource, but the user cannot make any configuration updates. For example, the privilege may allow the user to view the settings on a particular configuration window, but the configuration window for that application will not display update buttons or icons.
- Update—Update privileges give the user the ability to modify the settings for that resource. For example, the privileges may allow the user to make updates in a specific configuration window.

End User and Administrator Roles

The Standard CCM End Users role provides end users with access to the Cisco Unified Communications Self Care Portal. For additional privileges, such as CTI access, you must assign additional roles, such as the Standard CTI Enabled role.

The Standard CCM Admin Users role is the base role for all administration tasks and serves as the authentication role. This role provides users with administrative access to the Cisco Unified Communications Manager Administration user interface. Cisco Unified Communications Manager Administration defines this role as the role that is necessary to log in to Cisco Unified Communications Manager Administration.

Related Topics

Standard Roles and Access Control Groups, on page 237

Access Control Group Overview

You can use access control groups along with roles to quickly assign network access permissions to a group of users with similar access requirements.

An access control group is a list of end users and application users. You can assign end users or application users who share similar access needs to an access control group that contains the roles and permissions that they need. For an end user or application user to be assigned to an access control group, the user must meet the minimum rank requirement for that access control group. For example, an end user with a User Rank of 4 can be assigned only to access control groups with minimum rank requirements between 4 and 10.

The system includes a set of predefined standard access control groups. Each standard access control group has a set of roles assigned by default. When you assign a user to that access control group, those roles are also assigned to that end user.

You cannot edit the roles that are assigned to standard access control groups. However, you can create customized access control groups and assign the roles that you choose to your customized access control groups.

Related Topics

Standard Roles and Access Control Groups, on page 237

User Rank Overview

The User Rank hierarchy provides a set of controls over which access control groups an administrator can assign to an end user or application user.

When provisioning end users or application users, administrators can assign a user rank for the user. Administrators can also assign a user rank requirement for each access control group. When adding users to access conttrol groups, administrators can assign users only to the groups where the user's User Rank meets the group's rank requirement. For example, an administrator can assign a user whom has a User Rank of 3 to access control groups that have a User Rank requirement between 3 and 10. However, an administrator cannot assign that user to an access control group that has a User Rank requirement of 1 or 2.

Administrators can create their own user rank hierarchy within the **User Rank Configuration** window and can use that hierarchy when provisioning users and access control groups. Note that if you don't configure a user rank hierarchy, or if you simply don't specify the User Rank setting when provisioning users or access conrol groups, all users and access control groups are assigned the default User Rank of 1 (the highest rank possible).

User Access Prerequisites

Before you provision end users:

- Standard Roles and Access Control Groups, on page 237—Review the list of predefined roles and access control groups. Determine if you will need to configure customized roles and groups.
- Plan which user ranks you will assign to your users and groups.

User Access Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure User Rank Hierarchy, on page 232	Set up the user rank hierarchy for your system.
Step 2	If you need to create a new role, use one of the following methods: • Create a Custom Role, on page 232 • Copy an Existing Role, on page 233	Use the 'Create' procedure if you want to create and configure a new role from scratch. Use the 'Copy' procedure if the new role has similar privileges to an existing role. You can copy the privileges from the existing role into a new role, and then make edits to the privileges in the new role.
Step 3	If you need to create new access control groups, use one of the following methods: • Create Access Control Groups, on page 234 • Copy Access Control Group, on page 234	Use the 'Create' procedure to create a new access control group from scratch. Use the 'Copy' procedure if the new access control group has similar settings to an existing access control group. You can copy the settings from the existing access control group into a new group and then edit the settings.

	Command or Action	Purpose
Step 4	Assign Roles to Access Control Group, on page 235	If you created a new access control group, assign roles to your access control group.
Step 5	Configure Overlapping Privilege Policy, on page 236	Configure an enterprise policy to cover overlapping access privileges. This covers the situation where end users or application users are assigned to multiple access control groups or roles, each with conflicting privilege settings.

Related Topics

Standard Roles and Access Control Groups, on page 237

Configure User Rank Hierarchy

Use this procedure to create a custom user rank hierarchy.

Note If you don't configure a user rank hierarchy, all users and access control groups get assigned a user rank of 1 (the highest possible rank) by default.

Procedure

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

Step 2 Click **Add New**.

Step 3 From the **User Rank** drop-down menu, select a rank setting between 1–10. The highest rank is 1.

Step 4 Enter a **Rank Name** and **Description**.

Step 5 Click **Save**.

Step 6 Repeat this procedure to add additional user ranks.
You can assign the user rank to users and access control groups to control which groups a user can be assigned to.

Create a Custom Role

Create a custom role when there is no system-defined role with the privilege settings that you require.

Tip If the privileges in the new role that you want to create are similar to that of an existing role, follow the procedure Copy an Existing Role, on page 233 to copy the existing privileges into a new role that you can edit.

Procedure

Step 1 In Cisco Unified CM Administration, click **User Management** > **User Settings** > **Role**.

Step 2 Do either of the following:

- To create a new role, click **Add New**. Choose the **Application** with which this role associates, and click **Next**.
- To copy settings from an existing role, click **Find** and open the existing role. Click **Copy** and enter a name for the new role. Click **OK**.

Step 3 Enter a **Name** and **Description** for the role.

Step 4 For each resource, check the boxes that apply:

- Check the **Read** check box if you want users to be able to view settings for the resource.
- Check the **Update** check box if you want users to be able to edit setttings for the resource.
- Leave both check boxes unchecked to provide no access to the resource.

Step 5 Click **Grant access to all** or **Deny access to all** button to grant or remove privileges to all resources that display on a 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 to the resources that are listed on those pages.

Step 6 Click **Save**.

What to do next

Create Access Control Groups, on page 234

Copy an Existing Role

The **Copy** command allows you to create new roles that are based on the settings of existing roles. Cisco Unified Communications Manager does not allow you to edit standard roles, but you can use the **Copy** command to create a new role with the identical resources and privileges as the standard role. You can then edit the privileges in the new role that you created.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, click **User Management** > **User Settings** > **Role**.

Step 2 Click **Find** and select the role whose resources and privileges you want to copy.

Step 3 Click **Copy**.

Step 4 Enter the name of the new role and click **OK**.
The **Role Configuration** window displays the settings of the new role. The privileges for the new role are the same as the privileges for the role you copied.

Step 5 For any of the resources in the new role, edit the privileges as follows:

- Check the **Read** check box to allow users to view the resource.
- Check the **Update** check box to allow users to edit the resource.
- To restrict access to the resource, leave both check boxes unchecked.

Step 6 Click **Save**.

What to do next

Create a new access control group using one of the following methods:

- Create Access Control Groups, on page 234
- Copy Access Control Group, on page 234

Related Topics

Standard Roles and Access Control Groups, on page 237

Create Access Control Groups

Use this procedure is you need to create a new access control group. You may need to create a new access control group if the system-defined access control groups do not meet your deployment needs.

Before you begin

If you need to create new roles, perform one of the following procedures:

- Create a Custom Role, on page 232
- Copy an Existing Role, on page 233

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Access Control Groups.**

Step 2 Click **Add New**.

Step 3 Enter a **Name** for the access control group.

Step 4 From the **Available for Users with User Rank as** drop-down, select the minimum User Rank for a user to be assigned to this group. The default user rank is 1.

Step 5 Click **Save**.

What to do next

Assign Roles to Access Control Group, on page 235

Copy Access Control Group

Create a custom access control group by copying the settings from an existing access control group. When you copy an existing access control group, the system copies all the settings, including any assigned roles and users, to the new access control group. However, unlike default access control groups, you can make edits to the roles assigned to a custom access control group.

Before you begin

If you need to create a new role, perform either of the following steps:

- Create a Custom Role, on page 232
- Copy an Existing Role, on page 233

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Access Control Groups**.

Step 2 Click **Find** and select the access control group whose settings you want to copy.

Step 3 Click **Copy**.

Step 4 Enter a name for the new access control group and click **OK**.

Step 5 From the **Available for Users with User Rank as** drop-down, select the minimum User Rank for a user to be assigned to this group.

Step 6 Click **Save**.

What to do next

Assign Roles to Access Control Group, on page 235

Related Topics

Standard Roles and Access Control Groups, on page 237
Assign LDAP Synchronized Users to an Access Control Group, on page 277
Assign End Users to an Access Control Group, on page 281

Assign Roles to Access Control Group

For any new access control groups that you create, assign roles to the access control group. If you copied the access control group from an existing group, you may also need to delete a role.

Note You cannot edit the role assignments for any of the standard access control groups that are are configured by default.

Before you begin

Perform either of the following tasks to create a new access control group:

- Create Access Control Groups, on page 234
- Copy Access Control Group, on page 234

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Access Control Group**.

Step 2 Click **Find** and select an access control group.

Step 3 From the **Related Links** drop-down list box, select **Assign Role to Access Control Group** and click **Go**.

Step 4 If you need to assign a role:

a) Click **Assign Role to Group**.
b) In the **Find and List Roles** window, check the roles that you want to assign to the group.
c) Click **Add Selected**.

Step 5 If you need to delete a role:

a) In the **Role** list box, highlight the role that you want to delete.
b) Click **Delete Role Assignment**.

Step 6 Click **Save**.

What to do next

Configure Overlapping Privilege Policy, on page 236

Configure Overlapping Privilege Policy

Configure how Cisco Unified Communications Manager handles overlapping user privileges in access control group assignments. This is to cover situations where an end user is assigned to multiple access control groups, each with conflicting roles and access privileges.

Before you begin

Assign Roles to Access Control Group, on page 235

Procedure

Step 1 In Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

Step 2 Under **User Management Parameters**, configure one of the following values for the **Effective Access Privileges For Overlapping User Groups and Roles** as follows:

- **Maximum**—The effective privilege represents the maximum of the privileges of all the overlapping access control groups. This is the default option.
- **Minimum**—The effective privilege represents the minimum of the privileges of all the overlapping access control groups.

Step 3 Click **Save**.

Standard Roles and Access Control Groups

The following table summarizes the standard roles and access control groups that come preconfigured on Cisco Unified Communications Manager. The privileges for a standard role are configured by default. In addition, the access control groups that are associated with a standard role are also configured by default.

For both standard roles and the associated access control group, you cannot edit any of the privileges, or the role assignments.

Table 20: Standard Roles, Privileges, and Access Control Groups

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard AXL API Access	Allows access to the AXL database API	Standard CCM Super Users
Standard AXL API Users	Grants login rights to execute AXL APIs.	
Standard AXL Read Only API Access	Allows you to execute AXL read only APIs (list APIs, get APIs, executeSQLQuery API) by default.	
Standard Admin Rep Tool Admin	Allows you to view and configure Cisco Unified Communications Manager CDR Analysis and Reporting (CAR).	Standard CAR Admin Users, Standard CCM Super Users
Standard Audit Log Administration	Allows you to perform the following tasks for the audit logging feature : • View and configure audit logging in the Audit Log Configuration window in Cisco Unified Serviceability • View and configure trace in Cisco Unified Serviceability and collect traces for the audit log feature in the Real-Time Monitoring Tool • View and start/stop the Cisco Audit Event service in Cisco Unified Serviceability • View and update the associated alert in the RTMT	Standard Audit Users

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard CCM Admin Users	Grants log-in rights to Cisco Unified Communications Manager Administration.	Standard CCM Admin Users, Standard CCM Gateway Administration, Standard CCM Phone Administration, Standard CCM Read Only, Standard CCM Server Monitoring, Standard CCM Super Users, Standard CCM Server Maintenance, Standard Packet Sniffer Users
Standard CCM End Users	Grant an end user log-in rights to the Cisco Unified Communications Self Care Portal	Standard CCM End Users
Standard CCM Feature Management	Allows you to perform the following tasks in Cisco Unified Communications Manager Administration: • View, delete, and insert the following items by using the Bulk Administration Tool: • Client matter codes and forced authorization codes • Call pickup groups • View and configure the following items in Cisco Unified Communications Manager Administration: • Client matter codes and forced authorization codes • Call park • Call pickup • Meet-Me numbers/patterns • Message Waiting • Cisco Unified IP Phone Services • Voice mail pilots, voice mail port wizard, voice mail ports, and voice mail profiles	Standard CCM Server Maintenance

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard CCM Gateway Management	Allows you to perform the following tasks in Cisco Unified Communications Manager Administration: • View and configure gateway templates in the Bulk Administration Tool • View and configure gatekeepers, gateways, and trunks	Standard CCM Gateway Administration
Standard CCM Phone Management	Allows you to perform the following tasks in Cisco Unified Communications Manager Administration: • View and export phones in the Bulk Administration Tool • View and insert user device profiles in the Bulk Administration Tool • View and configure the following items in Cisco Unified Communications Manager Administration: • BLF speed dials • CTI route points • Default device profiles or default profiles • Directory numbers and line appearances • Firmware load information • Phone button templates or softkey templates • Phones • Reorder phone button information for a particular phone by clicking the Modify Button Items button in the Phone Configuration window	Standard CCM Phone Administration

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard CCM Route Plan Management	Allows you to perform the following tasks in Cisco Unified Communications Manager Administration: • View and configure application dial rules • View and configure calling search spaces and partitions • View and configure dial rules, including dial rule patterns • View and configure hunt lists, hunt pilots, and line groups • View and configure route filters, route groups, route hunt list, route lists, route patterns, and route plan report • View and configure time period and time schedule • View and configure translation patterns	
Standard CCM Service Management	Allows you to perform the following tasks in Cisco Unified Communications Manager Administration: • View and configure the following items: • Annunciators, conference bridges, and transcoders • audio sources and MOH servers • Media resource groups and media resource group lists • Media termination point • Cisco Unified Communications Manager Assistant wizard • View and configure the Delete Managers, Delete Managers/Assistants, and Insert Managers/Assistants windows in the Bulk Administration Tool	Standard CCM Server Maintenance

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard CCM System Management	Allows you to perform the following tasks in Cisco Unified Communications Manager Administration: • View and configure the following items: • Automate Alternate Routing (AAR) groups • Cisco Unified Communications Managers (Cisco Unified CMs) and Cisco Unified Communications Manager groups • Date and time groups • Device defaults • Device pools • Enterprise parameters • Enterprise phone configuration • Locations • Network Time Protocol (NTP) servers • Plug-ins • Security profiles for phones that run Skinny Call Control Protocol (SCCP) or Session Initiation Protocol (SIP); security profiles for SIP trunks • Survivable Remote Site Telephony (SRST) references • Servers • View and configure the Job Scheduler windows in the Bulk Administration Tool	Standard CCM Server Maintenance
Standard CCM User Privilege Management	Allows you to view and configure application users in Cisco Unified Communications Manager Administration.	
Standard CCMADMIN Administration	Allows you access to all aspects of the CCMAdmin system	
Standard CCMADMIN Administration	Allows you to view and configure all items in Cisco Unified Communications Manager Administration and the Bulk Administration Tool.	Standard CCM Super Users

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard CCMADMIN Administration	Allows you to view and configure information in the Dialed Number Analyzer.	
Standard CCMADMIN Read Only	Allows read access to all CCMAdmin resources	
Standard CCMADMIN Read Only	Allows you to view configurations in Cisco Unified Communications Manager Administration and the Bulk Administration Tool.	Standard CCM Gateway Administration, Standard CCM Phone Administration, Standard CCM Read Only, Standard CCM Server Maintenance, Standard CCM Server Monitoring
Standard CCMADMIN Read Only	Allows you to analyze routing configurations in the Dialed Number Analyzer.	
Standard CCMUSER Administration	Allows access to the Cisco Unified Communications Self Care Portal.	Standard CCM End Users
Standard CTI Allow Call Monitoring	Allows CTI applications/devices to monitor calls	Standard CTI Allow Call Monitoring
Standard CTI Allow Call Park Monitoring	Allows CTI applications/devices to use call park. **Important** The maximum number of opened lines and park lines must not exceed 65,000. If the total exceeds 65,000, remove the Standard CTI Allow Call Park Monitoring role from the application user or reduce the number of park lines that are configured.	Standard CTI Allow Call Park Monitoring
Standard CTI Allow Call Recording	Allows CTI applications/devices to record calls	Standard CTI Allow Call Recording
Standard CTI Allow Calling Number Modification	Allows CTI applications to transform calling party numbers during a call	Standard CTI Allow Calling Number Modification
Standard CTI Allow Control of All Devices	Allows control of all CTI-controllable devices	Standard CTI Allow Control of All Devices
Standard CTI Allow Control of Phones Supporting Connected Xfer and conf	Allows control of all CTI devices that supported connected transfer and conferencing	Standard CTI Allow Control of Phones supporting Connected Xfer and conf

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard CTI Allow Control of Phones Supporting Rollover Mode	Allows control of all CTI devices that supported Rollover mode	Standard CTI Allow Control of Phones supporting Rollover Mode
Standard CTI Allow Reception of SRTP Key Material	Allows CTI applications to access and distribute SRTP key material	Standard CTI Allow Reception of SRTP Key Material
Standard CTI Enabled	Enables CTI application control	Standard CTI Enabled
Standard CTI Secure Connection	Enables a secure CTI connection to Cisco Unified Communications Manager	Standard CTI Secure Connection
Standard CUReporting	Allows application users to generate reports from various sources	
Standard CUReporting	Allows you to view, download, generate, and upload reports in Cisco Unified Reporting	Standard CCM Administration Users, Standard CCM Super Users
Standard EM Authentication Proxy Rights	Manages Cisco Extension Mobility (EM) authentication rights for applications; required for all application users that interact with Cisco Extension Mobility (for example, Cisco Unified Communications Manager Assistant and Cisco Web Dialer)	Standard CCM Super Users, Standard EM Authentication Proxy Rights
Standard Packet Sniffing	Allows you to access Cisco Unified Communications Manager Administration to enable packet sniffing (capturing).	Standard Packet Sniffer Users
Standard RealtimeAndTraceCollection	Allows an you to access Cisco Unified Serviceability and the Real-Time Monitoring Tool view and use the following items: • Simple Object Access Protocol (SOAP) Serviceability AXL APIs • SOAP Call Record APIs • SOAP Diagnostic Portal (Analysis Manager) Database Service • configure trace for the audit log feature • configure Real-Time Monitoring Tool, including collecting traces	Standard RealtimeAndTraceCollection

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard SERVICEABILITY	Allows you to view and configure the following windows in Cisco Unified Serviceability or the Real-Time Monitoring Tool: • Alarm Configuration and Alarm Definitions (Cisco Unified Serviceability) • Audit Trace (marked as read/view only) • SNMP-related windows (Cisco Unified Serviceability) • Trace Configuration and Troubleshooting of Trace Configuration (Cisco Unified Serviceability) • Log Partition Monitoring • Alert Configuration (RTMT), Profile Configuration (RTMT), and Trace Collection (RTMT) Allows you to view and use the SOAP Serviceability AXL APIs, the SOAP Call Record APIs, and the SOAP Diagnostic Portal (Analysis Manager) Database Service. For the SOAP Call Record API, the RTMT Analysis Manager Call Record permission is controlled through this resource. For the SOAP Diagnostic Portal Database Service, the RTMT Analysis Manager Hosting Database access controlled thorough this resource.	Standard CCM Server Monitoring, Standard CCM Super Users
Standard SERVICEABILITY Administration	A serviceability administrator can access the Plugin window in Cisco Unified Communications Manager Administration and download plugins from this window.	
Standard SERVICEABILITY Administration	Allows you to administer all aspects of serviceability for the Dialed Number Analyzer.	
Standard SERVICEABILITY Administration	Allows you to view and configure all windows in Cisco Unified Serviceability and Real-Time Monitoring Tool. (Audit Trace supports viewing only.) Allows you to view and use all SOAP Serviceability AXL APIs.	

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard SERVICEABILITY Read Only	Allows you to view all serviceability-related data for components in the Dialed Number Analyzer.	Standard CCM Read Only
Standard SERVICEABILITY Read Only	Allows you to view configuration in Cisco Unified Serviceability and Real-Time Monitoring Tool. (excluding audit configuration window, which is represented by the Standard Audit Log Administration role) Allows an you to view all SOAP Serviceability AXL APIs, the SOAP Call Record APIs, and the SOAP Diagnostic Portal (Analysis Manager) Database Service.	
Standard System Service Management	Allows you to view, activate, start, and stop services in Cisco Unified Serviceability.	
Standard SSO Config Admin	Allows you to administer all aspects of SAML SSO configuration	
Standard Confidential Access Level Users	Allows you to access all the Confidential Access Level Pages	Standard Cisco Call Manager Administration
Standard CCMADMIN Administration	Allows you to administer all aspects of CCMAdmin system	Standard Cisco Unified CM IM and Presence Administration
Standard CCMADMIN Read Only	Allows read access to all CCMAdmin resources	Standard Cisco Unified CM IM and Presence Administration
Standard CUReporting	Allows application users to generate reports from various sources	Standard Cisco Unified CM IM and Presence Reporting

CHAPTER 33

Configure Credential Policy

Credential Policy Overview

Credential policies control the authentication process for resources in Cisco Unified Communications Manager. A credential policy defines password requirements and account lockout details such as failed login attempts, expiration periods and lockout durations for end user passwords, end user PINs, and application user passwords. Credential policies can be assigned broadly to all accounts of a specific credential types, such as all end user PINs, or they can be customized for a specific application user, or end user.

Credential Types

In Credential Policy Configuration you can configure a new credential policy and then apply that new policy as the default credential policy for each of the following three credential types:

- End User PINs
- End User Passwords
- Application User Passwords

You can also apply the credential policy to a specific end user PIN, end user password, or application user password.

Credential Policies with LDAP Authentication Enabled

If your system is configured for LDAP Authentications with the corporate directory:

- With LDAP Autthentication enabled, credential policies do not apply to end user passwords.
- Credential policies do apply to end user PINs and application user passwords, irrespective of whether LDAP Authentication is enabled. These password types use local authentication.

Note Credential policies do not apply to operating system users or CLI users. These administrators use standard password verification procedures that the operating system supports.

Trivial Passwords

The system can be configured to check for trivial passwords and PINs. A trivial password is a credential that can be easily hacked, such as a password that be guessed easily such as using ABCD as your password or 123456 as your PIN.

Non-trivial passwords meet the following requirements:

- Must contain three of the following four characteristics: uppercase character, lowercase character, number, or 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 are not allowed.

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, 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.

Credential Policy Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure a Credential Policy, on page 249	Configure credential policies for end users and application users.
Step 2	Configure Default Credentials for a Credential Policy, on page 249	Apply the configured credential policy as the default credential policy for any of three credential types: end user passwords, and application users. The default credential policy will be applied by default to that credential type for newly provisioned users.

Related Topics

Apply Credential Policy to End User, on page 281

Configure a Credential Policy

Configure a credential policy that you can apply as the default credential policy for all credentials that match a specific credential type such as end user PINs or end user passwords.

Note Ensure that the **Inactive Days Allowed** parameter under the Credential Policy Settings is set to 0 for CTI application users. Else, the application users unexpectedly become inactive and the CTI applications may fail to connect to Unified CM after restart.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Credential Policy**.

Step 2 Perform one of the following steps:

- Click **Find** and select an existing credential policy.
- Click **Add New** to create a new credential policy.

Step 3 Complete the fields in the **Credential Policy Configuration** window. See the online help for more information about the fields and their configuration settings.

Step 4 Click **Save**.

What to do next

Configure Default Credentials for a Credential Policy, on page 249

Configure Default Credentials for a Credential Policy

Perform these steps to configure the default credentials for your credential policy. You can assign default credentials to assign a temporary password that a user must change upon their next login.

Before you begin

Configure a Credential Policy, on page 249

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Credential Policy Default**.

Step 2 From the **Credential Policy** drop-down list box, choose the credential policy for this group.

Step 3 Enter the password in both the **Change Credential** and **Confirm Credential** configuration windows.

Step 4 Check the **User Cannot Change** check box if you do not want your users to be able to change this credential.

Step 5 Check the **User Must Change at Next Login** check box if you want to use this credential as a temporary credential that an end user must change the next time that they login.

Note Please note that, if you check this box, your users are unable to change PIN using Personal Directory service.

Step 6 If you do not want the credential to expire, check the **Does Not Expire** check box.

Step 7 Click **Save**.

What to do next

If you want to apply a credential policy to a specific end user or PIN:

- Apply Credential Policy to End User, on page 281

CHAPTER 34

Configure User Profiles

User Profile Overview

User profiles contain common directory number and device settings. You can configure different user profiles that contain the most common directory number settings and device settings that your users require and then assign each user profile to the users that require those settings. You can configure different user profiles for different groups of users in your company, according to the phone line and phone setting requirements for each set of users.

For those end users who are enabled for self-provisioning, the phone and phone line settings from the user profile get applied to any new phones that the user provisions. If the user is not enabled for self-provisioning, the user profile settings can be applied to any new phones that the administrator provisions on behalf of the end user.

User profiles use settings from the following phone and phone line templates to build a profile for the end user:

- Universal Line Template—a collection of common phone line settings that are typically assigned to a directory number. Universal line templates allow you to quickly configure phone lines for new directory numbers that get assigned to an end user.
- Universal Device Template—a collection of common device settings that are typically assigned to a phone or other device. Universal device templates allow you to quickly configure new phones that get assigned to an end user.

User Profile Prerequisites

Before configuring your user profiles, make sure to plan how you are going to provision phones for your deployment. Decide whether you are going to use self-provisioning to allow end users to provision their own phones.

User Profile Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure a Universal Line Template, on page 252	Configure universal line templates with common settings that are typically applied to a directory number.
Step 2	Configure a Universal Device Template, on page 253	Configure universal device templates with common settings that are typically applied to phones and other devices.
Step 3	Configure a User Profile, on page 253	Assign the universal line and universal device templates to a user profile.

Configure a Universal Line Template

Universal Line Templates make it easy to apply common settings to newly assigned directory numbers. Configure different templates to meet the needs of different groups of users.

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **Universal Line Template**.

Step 2 Click **Add New**.

Step 3 Configure the fields in the **Universal Line Template Configuration** window. See the online help for more information about the fields and their configuration options.

Step 4 If you are deploying Global Dial Plan Replication with alternate numbers expand the **Enterprise Alternate Number** and **+E.164 Alternate Number** sections and do the following:

a) Click the **Add Enterprise Alternate Number** button and/or **Add +E.164 Alternate Number** button.

b) Add the **Number Mask** that you want to use to assign to your alternate numbers. For example, a 4-digit extension might use 5XXXX as an enterprise number mask and 1972555XXXX as an +E.164 alternate number mask.

c) Assign the partition where you want to assign alternate numbers.

d) If you want to advertise this number via ILS, check the **Advertise Globally via ILS** check box. Note that if you are using advertised patterns to summarize a range of alternate numbers, you may not need to advertise individual alternate numbers.

e) Expand the **PSTN Failover** section and choose the **Enterprise Number** or **+E.164 Alternate Number** as the PSTN failover to use if normal call routing fails.

Step 5 Click **Save**.

Configure a Universal Device Template

Universal device templates make it easy to apply configuration settings to newly provisioned devices. The provisioned device uses the settings of the universal device template. You can configure different device templates to meet the needs of different groups of users. You can also assign the profiles that you've configured to this template.

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **Universal Device Template**.

Step 2 Click **Add New**.

Step 3 Enter the following mandatory fields:

a) Enter a **Device Description** for the template.
b) Select a **Device Pool** type from the drop-down list.
c) Select a **Device Security Profile** from the drop-down list.
d) Select a **SIP Profile** from the drop-down list.
e) Select a **Phone Button Template** from the drop-down list.

Step 4 Complete the remaining fields in the **Universal Device Template Configuration** window. For field descriptions, see the online help.

Step 5 Under **Phone Settings**, complete the following optional fields:

a) If you configured a **Common Phone Profile**, assign the profile.
b) If you configured a **Common Device Configuration**, assign the configuration.
c) If you configured a **Feature Control Policy**, assign the policy.

Step 6 Click **Save**.

Configure a User Profile

Assign universal line and universal device template to users through the User Profile. Configure multiple user profiles for different groups of users. You can also enable self-provisioning for users who use this service profile.

Procedure

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

Step 2 Click **Add New**.

Step 3 Enter a **Name** and **Description** for the user profile.

Step 4 Assign a **Universal Device Template** to apply to users' **Desk Phones**, **Mobile and Desktop Devices**, and **Remote Destination/Device Profiles**.

Step 5 Assign a **Universal Line Template** to apply to the phone lines for users in this user profile.

Step 6 If you want the users in this user profile to be able to use the self-provisioning feature to provision their own phones, do the following:

a) Check the **Allow End User to Provision their own phones** check box.

b) In the **Limit Provisioning once End User has this many phones** field, enter a maximum number of phones the user is allowed to provision. The maximum is 20.

Step 7 If you want Cisco Jabber users who are associated with this user profile, to be able to use the Mobile and Remote Access feature, check the **Enable Mobile and Remote Access** check box.

Note

- By default, this check box is selected. When you uncheck this check box, the **Client Policies** section is disabled, and No Service client policy option is selected by default.
- This setting is mandatory only for Cisco Jabber users whom are using OAuth Refresh Logins. Non-Jabber users do not need this setting to be able to use Mobile and Remote Access. Mobile and Remote Access feature is applicable only for the Jabber Mobile and Remote Access users and not to any other endpoints or clients.

Step 8 Assign the Jabber policicies for this user profile. From the **Desktop Client Policy**, and **Mobile Client Policy** drop-down list, choose one of the following options:

- No Service—This policy disables access to all Cisco Jabber services.
- IM & Presence only—This policy enables only instant messaging and presence capabilities.
- IM & Presence, Voice and Video calls—This policy enables instant messaging, presence, voicemail, and conferencing capabilities for all users with audio or video devices. This is the default option.

Note Jabber desktop client includes Cisco Jabber for Windows users and Cisco Jabber for Mac users. Jabber mobile client includes Cisco Jabber for iPad and iPhone users and Cisco Jabber for Android users.

Step 9 Click **Save**.

CHAPTER 35

Configure Service Profile

Service Profile Overview

A Service Profile allows you to create a profile that comprises common Unified Communications (UC) Services settings. You can then apply the service profile to an end user in order to assign the UC services configuration settings in the Service Profile to that end user. You can configure different service profiles for different groups of users in your company so that each group of users has the appropriate services configured for their job.

A Service Profile comprises configuration settings for the following UC services:

- Voicemail
- Mailstore
- Conferencing
- Directory
- IM and Presence
- CTI
- Video conferencing services

Applying Service Profiles to End Users

You can use the following methods to apply a service profile to an end user:

- For LDAP Synchronized Users—If you have imported end users from an LDAP directory, you can assign the service profile to a feature group template and then apply that feature group template to your end users
- For Active Local Users (i.e. non-LDAP users)—In End User Configuration, you can assign a service profile for an individual end user. You can also use the Bulk Administration Tool to assign a service profiles for many end users at once. For details, see the *Bulk Administration Guide for Cisco Unified Communications Manager*.

Service Profile Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure any of the following Unified Communications (UC) services that you want to assign to this service profile: • Add Voicemail Service, on page 256 • Add Mailstore Service, on page 257 • Add Conferencing Service, on page 258 • Add Directory Service, on page 258 • Add IM and Presence Service, on page 259 • Add CTI Service, on page 260 • Add Video Conference Scheduling Service, on page 261	Configure the UC services settings that you want to set up for your service profiles.
Step 2	Configure a Service Profile, on page 262	Configure the user's service profile to point to the UC services that you want to apply to this service profile.

Add Voicemail Service

Add a voicemail service to your system. You can add multiple voicemail services and then select which service you want to add to your service profiles.

Procedure

Step 1 From Cisco Unified CM Administration choose **User Management** > **User Settings** > **UC Service**.

Step 2 Click **Add New**.

Step 3 From the **UC Service Type** drop-down list box, choose **Voicemail**.

Step 4 From the **Product Type** drop-down list box, choose **Unity** or **Unity Connection**.

Step 5 Enter a **Name** for the voicemail service.

Step 6 Enter a **Description** that helps you distinguish between services.

Step 7 In the **Hostname/IP Address** field, enter the hostname, IP address, or fully qualified domain name of the server that hosts the voicemail service.

Step 8 In the **Port** field, enter a port to connect to the voicemail service. The default port is 443.

Step 9 In the **Protocol** field, enter the protocol that will be used to route voicemail messages. The available options are **HTTP** and **HTTPS**.

Note Cisco recommends that you use HTTPS as the voicemail transport protocol for Cisco Unity and Cisco Unity Connection servers. Only change to HTTP if your network configuration does not support HTTPS.

Step 10 Click **Save**.

What to do next

Add Mailstore Service, on page 257

Add Mailstore Service

Add a mailstore service to your system. Cisco Jabber clients use the mailstore service for visual voicemail functionality.

Note Cisco Unity creates subscriber mailboxes for message storage on the Microsoft Exchange server.

Cisco Unity Connection usually provides a mailstore service, and hosts the mailstore service on the same server.

Before you begin

Add Voicemail Service, on page 256

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **User Settings** > **UC Service**.

Step 2 Click **Add New**.

Step 3 From the **UC Service Type** drop-down list box, choose **Mailstore**.

Step 4 Enter a **Name** for the mailstore service.

Step 5 Enter a **Description** for the mailstore service.

Step 6 In the **Hostname/IP Address** field, enter the hostname, IP address, or fully qualified domain name for the server that hosts the mailstore service.

Step 7 In the **Port** field, specify a port between 1–65535 that matches the available port on the mailstore service. number between 1 - 65535. The default mailstore port is 143.

Note For secure voice messaging with Cisco Unity connection, use 7993.

Step 8 In the **Protocol** field, enter the protocol that will be used to route voicemail messages: TCP (default), TLS, UDP, or SSL.

Note For secure messaging with Cisco Unity Connection, use TLS.

Step 9 Click **Save**.

What to do next

Add Conferencing Service, on page 258

Add Conferencing Service

Add a conferencing service to your system.

Before you begin

Add Mailstore Service, on page 257

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **User Settings** > **UC Service**.

Step 2 Click **Add New**.

Step 3 From the **UC Service Type** drop-down list box, choose **Conferencing**.

Step 4 From the **Product Type** drop-down list box, choose the product that you want to use for conferencing:

- MeetingPlace Classic
- MettingPlace Express
- Webex

Step 5 Enter a **Name** for the conferencing service.

Step 6 Enter a **Description** for the conferencing service.

Step 7 In the **Hostname/IP Address** field, enter the hostname, IP address, or fully qualified domain name of the server that hosts the conferencing service.

Step 8 In the **Port** field, enter a port value that matches the available port on the conferencing service. The recommended values are:

- 80 (default setting)—Use this port for HTTP
- 443—Use this port for HTTPS

Step 9 From the **Protocol** drop-down list box, choose the Protocol to use when endpoints contact this service:

- TCP (default setting)
- UDP
- SSL
- TLS

Note For secure messaging with Cisco Unity Connection, use TLS.

Step 10 Click **Save**.

What to do next

Add Directory Service, on page 258

Add Directory Service

Add a directory service to your system if you want to point Cisco Unified Communications Manager towards an external LDAP directory for directory lookups.

Before you begin

Add Conferencing Service, on page 258

Procedure

Step 1 From Cisco Unified CM Administration, choose **USer Management** > **User Settings** > **UC Service**.

Step 2 Click **Add New**.

Step 3 From the **UC Service Type** drop-down list box, choose **Directory**.

Step 4 From the **Product Type** field, choose either of the following:

- Directory—Choose this option if you want your clients to use UDS to connect to the Cisco Unified Communications Manager database for directory lookups.
- Enhanced Directory—Choose this option if you want your clients to connect to an external LDAP directory for directory lookups.

Step 5 Enter a **Name** for the directory service.

Step 6 Enter a **Description** for the directory service.

Step 7 In the **Hostname/IP Address** field, enter the hostname, IP address, or fully qualified domain name of the server that hosts the directory service that you want your clients to use for directory lookups.

Note If you are using an external LDAP directory for directory lookups, enter the hostname, IP address, or fully qualified domain name of the LDAP directory.

Step 8 In the **Port** field, enter a port number that matches the available port on the directory service. The default port value is 389. In addition, ports 636, 3628, 3629 can connect to an external LDAP directory.

Step 9 In the **Protocol** field, enter the protocol that will be used to route communications between the directory service and endpoints. The available options are:

- TCP (default setting)
- UDP
- TLS

Step 10 Click **Save**.

What to do next

Add IM and Presence Service, on page 259

Add IM and Presence Service

Add an IM and Presence service to your system.

Before you begin

Add Directory Service, on page 258

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **User Settings** > **UC Service**.

Step 2 Click **Add New**.

Step 3 From the **UC Service Type** drop-down list box, choose IM and Presence.

Step 4 From the **Product Type** drop-down list box, choose one of the following options:

- Unified CM (IM and Presence)
- WeEx (IM and Presence)

Step 5 Enter a **Name** for the IM and Presence service.

Step 6 Enter a **Description** for the IM and Presence service.

Step 7 In the **Hostname/IP Address** field, enter the hostname, IP address, or DNS SRV for the server that hosts the IM and Presence service.

Tip Cisco recommends DNS SRV to help the client find the correct IM and Presence service for the user.

Step 8 Click **Save**.

What to do next

Add CTI Service, on page 260

Add CTI Service

Add a CTI service to your system.

Before you begin

Add IM and Presence Service, on page 259

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **User Settings** > **UC Service**.

Step 2 Click **Add New**.

Step 3 From the **UC Service Type** drop-down list box, choose **CTI**.

Step 4 Enter a **Name** for the CTI service.

Step 5 Enter a **Description** for the CTI service.

Step 6 In the **Hostname/IP Address** field, enter the hostname, IP address, or fully qualified domain name for the server that hosts the CTI service.

Step 7 In the **Port** field, enter the port number of the CTI service. The default port is 2748.

Step 8 Click **Save**.

What to do next

Add Video Conference Scheduling Service, on page 261

Add Video Conference Scheduling Service

Add a video conference scheduling service that provides a portal to the TelePresence Management System for video conference scheduling.

Before you begin

Add CTI Service, on page 260

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **User Settings** > **UC Service**.

Step 2 Click **Add New**.

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

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

Step 5 In the **IP Address/Hostname** field, enter the hostname, IP address, or fully qualified domain name of the server that hosts the video conferencing scheduling service.

Step 6 In the **Port** field, enter a port number that matches the available port on the video conference scheduling service. The available ports are:

- 80 (default) or 8080—use these ports for HTTP
- 443 or 8443—use these ports for HTTPS

Step 7 From the **Protocol** drop-down list box, choose one of the following protocols for communications with the video conference scheduling service:

- HTTP
- HTTPS

Step 8 In the **Portal URL** field, enter a URL that points to the TelePresence Management System.

Step 9 Click **Save**.

What to do next

Configure a Service Profile, on page 262

Configure UC Services

Use this procedure to configure the UC service connections that your users will use. You can configure connections for the following UC services:

- Voicemail
- Mailstore

- Conferencing
- Directory
- IM and Presence Service
- CTI
- Video Conferencing Scheduling Portal
- Jabber Client Configuration (jabber-config.xml)

Note The fields may vary depending on which UC service you configure.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management > User Settings > UC Services**.

Step 2 Click **Add New**.

Step 3 From the UC Service Type drop-down, select the UC service that you want to configure and click **Next**.

Step 4 Select the **Product Type**.

Step 5 Enter a **Name** for the service.

Step 6 Enter the **Hostname or IP address** for the server where the service is homed.

Step 7 Complete the **Port** and **Protocol** information.

Step 8 Configure the remaining fields. For help with the fields and their settings, refer to the online help. The field options vary depending on which UC service you are deploying.

Step 9 Click **Save**.

Step 10 Repeat this procedure until you have provisioned all the UC services that you need.

Note If you want the service to be located on multiple servers, configure different UC service connections that point to different servers. For example, with the IM and Presence Service Centralized Deployment, it is recommended to configure multiple IM and Presence UC services that point to different IM and Presence nodes. After you have configured all your UC connections, you can add them to a Service Profile.

Configure a Service Profile

Configure a Service Profile that include the UC Services that you want to assign to end users who use the profile.

Before you begin

You must set up your Unified Communications (UC) services before you can add them to a service profile.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Service Profile**.

Step 2 Click **Add New**.

Step 3 Enter a **Name** for the chosen Service Profile Configuration.

Step 4 Enter a **Description** for the chosen Service Profile Configuration.

Step 5 For each UC service that you want to be a part of this profile, assign the **Primary**, **Secondary**, and **Tertiary** connections for that service.

Step 6 Complete the remaining fields in the **Service Profile Configuration** window. For detailed field descriptions, see the online help.

Step 7 Click **Save**.

CHAPTER 36

Configure Feature Group Template

Feature Group Template Overview

Feature group templates help you deploy your end users with configured phones and phone lines. Feature group templates allow you to assign common phone, phone line, and service settings to all users who are assigned that feature group template. If you have also enabled self-provisioning for your end users, the feature group template allows your users to quickly provision and set up their phones with the desired phone, phone line and services settings.

The feature group template configuration includes the following profiles that you can assign to the feature group template:

- User Profile—contains a set of common phone and phone line settings. You must configure the user profile with a universal line template, which assigns the common phone line settings, and a universal device template, which assigns the common phone settings. These templates assist users who are set up for self-provisioning to configure their own phones.
- Service Profile—contains a group of common settings for Unified Communications services such as conferencing and directory services.

When you configure a feature group template to include a user profile and service profile and then assign that feature group template to an end user, the user profile and service profile settings propagate through to any new phones that the end user provisions.

If you are deploying the IM and Presence Service, you can use the feature group template to enable LDAP-synchronized users with instant messaging and presence capability.

Feature Group Template Prerequisites

Before you configure a feature group template, configure a user profile and service profile for your end users.

- User Profile Configuration Task Flow, on page 252
- Service Profile Configuration Task Flow, on page 256

Configure a Feature Group Template

Feature group templates aid in your system deployment by helping you to quickly configure phones, lines, and features for your provisioned users. If you are syncing users from a company LDAP directory, configure a feature group template with the User Profile and Service Profile that you want users synced from the directory to use. You can also enable the IM and Presence Service for synced users through this template.

Procedure

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

Step 2 Click **Add New**.

Step 3 Enter a **Name** and **Description** for the Feature Group Template.

Step 4 Check the **Home Cluster** check box if you want to use the local cluster as the home cluster for all users whom use this template.

Step 5 Check the **Enable User for Unified CM IM and Presence** check box to allow users whom use this template to exchange instant messaging and presence information.

Step 6 From the drop-down list, select a **Services Profile** and **User Profile**.

Step 7 Complete the remaining fields in the **Feature Group Template Configuration** window. Refer to the online help for field descriptions.

Step 8 Click **Save**.

What to do next

Associate the feature group template with an LDAP directory sync to apply the settings from the template to synchronized end users.

CHAPTER 37

Import Users From LDAP Directory

LDAP Synchronization Overview

Lightweight Directory Access Protocol (LDAP) synchronization helps you to provision and configure end users for your system. During LDAP synchronization, the system imports a list of users and associated user data from an external LDAP directory into the Unified Communications Manager database. You can also configure your end users while the import occurs.

Note Unified Communications Manager supports LDAPS (LDAP with SSL) but does not support LDAP with StartTLS. Ensure that you upload the LDAP server certificate to Unified Communications Manager as a Tomcat-Trust.

See the *Compatibility Matrix for Cisco Unified Communications Manager and the IM and Presence Service* for information on the supported LDAP directories.

LDAP synchronization advertises the following functionalities:

- **Importing End Users**—You can use LDAP synchronization during the initial system setup to import your user list from a company LDAP directory into the Unified Communications Manager database. If you've preconfigured items such as feature group templates, user profiles, service profiles, universal device and line templates, you can apply configurations to your users, and assign configured directory numbers and directory URIs during the sync process. The LDAP synchronization process imports the list of users and user-specific data and applies the configuration templates that you've set up.

  Note You cannot make edits to an LDAP synchronization once the initial synchronization has occurred already.

- **Scheduled Updates**—You can configure Unified Communications Manager to synchronize with multiple LDAP directories at scheduled intervals to ensure that the database is updated regularly and user data is up-to-date.

- **Authenticate End Users**—You can configure your system to authenticate end user passwords against the LDAP directory rather than the Cisco Unified Communications Manager database. LDAP authentication provides companies with the ability to assign a single password to end users for all company applications. This functionality does not apply to PINs or application user passwords.
- **Directory Server User Search for Cisco Mobile and Remote Access Clients and Endpoints**—You can search a corporate directory server even when operating outside the enterprise firewall. When this feature is enabled, the User Data Service (UDS) acts as a proxy and sends the user search request to the corporate directory instead of sending it to the Unified Communications Manager database.

LDAP Authentication for End Users

LDAP synchronization allows you to configure your system to authenticate end user passwords against the LDAP directory rather than the Cisco Unified Communications Manager database. LDAP authentication provides companies with the ability to assign a single password to end users for all company applications. This functionality does not apply to PINs or application user passwords.

Directory Server User Search for Cisco Mobile and Remote Access Clients and Endpoints

In previous releases, when a user with a Cisco mobile and remote access client (for example, Cisco Jabber) or endpoint (for example, Cisco DX 80 phone) performed a user search while outside the enterprise firewall, results were based on those user accounts that are saved in the Cisco Unified Communications Manager database. The database contains user accounts which are either configured locally or synchronized from the corporate directory.

With this release, Cisco mobile and remote access clients and endpoints can now search a corporate directory server even when operating outside the enterprise firewall. When this feature is enabled, the User Data Service (UDS) acts as a proxy and sends the user search request to the corporate directory instead of sending it to the Cisco Unified Communications Manager database.

Use this feature to achieve the following results:

- Deliver the same user search results regardless of geographic location—Mobile and remote access clients and endpoints can perform user searches by using the corporate directory; even when they are connected outside the enterprise firewall.
- Reduce the number of user accounts that are configured in the Cisco Unified Communications Manager database—Mobile clients can now search users in the corporate directory. In the previous releases, user search results were based on the users that are configured in the database. Now, administrators no longer need to configure or synchronize user accounts to the database solely for user searches. Administrators need to configure only those user accounts that are served by a cluster. Reducing the total number of user accounts in the database shortens software upgrade time frames while improving overall database performance.

To configure this feature, you must enable the **Enable user search to Enterprise Directory Server** option in the **LDAP Search Configuration** window, and configure the LDAP directory server details. For details, see the Configure Enterprise Directory User Search, on page 273 procedure.

LDAP Synchronization Prerequisites

Prerequisite Tasks

Before you import end users from an LDAP directory, complete the following tasks:

- Configure User Access. Decide which access control groups you want to assign to your users. For many deployments, the default groups are sufficient. If you need to customize your roles and groups, refer to the 'Manage User Access' chapter of the Administration Guide.
- Configure Default credentials for a credential policy that is applied by default to newly provisioned users.
- If you are syncing users from an LDAP directory, make sure that you have a Feature Group Template set up that includes the User Profiles, Service Profiles, and Universal Line and Device Template settings that you want to assign to your users phones and phone extensions.

Note For users whose data you want to synchronize to your system, ensure that their email ID fields on the Active Directory server are unique entries or left blank.

LDAP Synchronization Configuration Task Flow

Use the following tasks to pull a user list from the external LDAP directory and import it into the Unified Communications Manager database.

Note If you have already synced the LDAP directory once, you can still sync new items from your external LDAP directory, but you cannot add new configurations in Unified Communications Manager to the LDAP directory sync. In this case, you can use the Bulk Administration Tool and menus such as Update Users or Insert Users. Refer to the *Bulk Administration Guide for Cisco Unified Communications Manager*.

Procedure

	Command or Action	Purpose
Step 1	Activate the Cisco DirSync Service, on page 270	Log in to Cisco Unified Serviceability and activate the Cisco DirSync service.
Step 2	Enable LDAP Directory Synchronization, on page 270	Enable LDAP directory synchronization in Unified Communications Manager.
Step 3	Create an LDAP Filter, on page 271	**Optional**. Create an LDAP filter if you want Unified Communications Manager to synchronize only a subset of users from your corporate LDAP directory.

	Command or Action	Purpose
Step 4	Configure LDAP Directory Sync, on page 271	Configure settings for the LDAP directory sync such as field settings, LDAP server locations, synchronization schedules, and assignments for access control groups, feature group templates, and primary extensions.
Step 5	Configure Enterprise Directory User Search, on page 273	**Optional**. Configure the system for enterprise directory server user searches. Follow this procedure to configure phones and clients in your system to perform user searches against an enterprise directory server instead of the database.
Step 6	Configure LDAP Authentication, on page 275	**Optional**. If you want to use the LDAP directory for end user password authentication, configure LDAP authentication settings.
Step 7	Customize LDAP Agreement Service Parameters, on page 275	**Optional**. Configure the optional LDAP Synchronization service parameters. For most deployments, the default values are sufficient.

Activate the Cisco DirSync Service

Perform this procedure to activate the Cisco DirSync Service in Cisco Unified Serviceability. You must activate this service if you want to synchronize end user settings from a corporate LDAP directory.

Procedure

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

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

Step 3 Under **Directory Services**, click the **Cisco DirSync** radio button.

Step 4 Click **Save**.

Enable LDAP Directory Synchronization

Perform this procedure if you want to configure Unified Communications Manager to synchronize end user settings from a corporate LDAP directory.

Note If you have already synced the LDAP directory once, you can still sync new users from your external LDAP directory, but you cannot add new configurations in Unified Communications Manager to the LDAP directory sync. You also cannot add edits to underlying configuration items such as the feature group template or user profile. If you have already completed one LDAP sync, and want to add users with different settings, you can use Bulk Administration menus such as Update Users or Insert Users.

Procedure

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

Step 2 If you want Unified Communications Manager to import users from your LDAP directory, check the **Enable Synchronizing from LDAP Server** check box.

Step 3 From the **LDAP Server Type** drop-down list, choose the type of LDAP directory server that your company uses.

Step 4 From the **LDAP Attribute for User ID** drop-down list, choose the attribute from your corporate LDAP directory that you want Unified Communications Manager to synchronize with for the **User ID** field in the **End User Configuration** window.

Step 5 Click **Save**.

Create an LDAP Filter

You can create an LDAP filter to limit your LDAP synchronization to a subset of users from your LDAP directory. When you apply the LDAP filter to your LDAP directory, Unified Communications Manager imports only those users from the LDAP directory who match the filter.

Note Any LDAP filter that you configure must comply with the LDAP search filter standards that are specified in RFC4515.

Procedure

Step 1 In Cisco Unified CM Administration, choose **System** > **LDAP** > **LDAP Filter**.

Step 2 Click **Add New** to create a new LDAP filter.

Step 3 In the **Filter Name** text box, enter a name for your LDAP filter.

Step 4 In the **Filter** text box, enter a filter. The filter can contain a maximum of 1024 UTF-8 characters and must be enclosed in parentheses ().

Step 5 Click **Save**.

Configure LDAP Directory Sync

Use this procedure to configure Unified Communications Manager to synchronize with an LDAP directory. LDAP directory synchronization allows you to import end user data from an external LDAP directory into the Unified Communications Manager database such that it displays in End User Configuration window. If you have setup feature group templates with universal line and device templates, you can assign settings to newly provisioned users and their extensions automatically.

Tip If you are assigning access control groups or feature group templates, you can use an LDAP filter to limit the import to the group of users with the same configuration requirements.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **LDAP** > **LDAP Directory**.

Step 2 Perform one of the following steps:

- Click **Find** and select an existing LDAP directory.
- Click **Add New** to create a new LDAP directory.

Step 3 In the **LDAP Directory Configuration** window, enter the following:

a) In the **LDAP Configuration Name** field, assign a unique name to the LDAP directory.
b) In the **LDAP Manager Distinguished Name** field, enter a user ID with access to the LDAP directory server.
c) Enter and confirm the password details.
d) In the **LDAP User Search Space** field, enter the search space details.
e) In the **LDAP Custom Filter for Users Synchronize** field, select either **Users Only** or **Users and Groups**.
f) (Optional). If you want to limit the import to only a subset of users who meet a specific profile, from the **LDAP Custom Filter for Groups** drop-down list, select an LDAP filter.

Step 4 In the **LDAP Directory Synchronization Schedule** fields, create a schedule that Unified Communications Manager uses to synchronize data with the external LDAP directory.

Step 5 Complete the **Standard User Fields to be Synchronized** section. For each End User field, choose an LDAP attribute. The synchronization process assigns the value of the LDAP attribute to the end user field in Unified Communications Manager.

Step 6 If you are deploying URI dialing, make sure to assign the LDAP attribute that will be used for the user's primary directory URI address.

Step 7 In the **Custom User Fields To Be Synchronized** section, enter custom user field name with the required LDAP attribute.

Step 8 To assign the imported end users to an access control group that is common to all the imported end users, do the following

a) Click **Add to Access Control Group**.
b) In the pop-up window, click the corresponding check box for each access control group that you want to assign to the imported end users.
c) Click **Add Selected**.

Step 9 If you want to assign a feature group template, select the template from the **Feature Group Template** drop-down list.

Note The end users are synced with the assigned **Feature Group Template** only for the first time when the users are not present. If an existing **Feature Group Template** is modified and a full sync is performed for the associated LDAP, the modifications will not get updated.

Step 10 If you want to assign a primary extension by applying a mask to imported telephone numbers, do the following:

a) Check the **Apply mask to synced telephone numbers to create a new line for inserted users** check box.

b) Enter a **Mask**. For example, a mask of 11XX creates a primary extension of 1145 if the imported telephone number is 8889945.

Step 11 If you want to assign primary extensions from a pool of directory numbers, do the following:

a) Check the **Assign new line from the pool list if one was not created based on a synced LDAP telephone number** check box.

b) In the **DN Pool Start** and **DN Pool End** text boxes, enter the range of directory numbers from which to select primary extensions.

Step 12 In the **LDAP Server Information** section, enter the hostname or IP address of the LDAP server.

Step 13 If you want to use TLS to create a secure connection to the LDAP server, check the **Use TLS** check box.

Step 14 Click **Save**.

Step 15 To complete an LDAP sync, click **Perform Full Sync Now**. Otherwise, you can wait for the scheduled sync.

Note When users are deleted in LDAP, they will automatically be removed from Unified Communications Manager after 24 hours. Also, if the deleted user is configured as a mobility user for any of the following devices, these inactive devices will also be automatically deleted:

- Remote Destination Profile
- Remote Destination Profile Template
- Mobile Smart Client
- CTI Remote Device
- Spark Remote Device
- Nokia S60
- Cisco Dual Mode for iPhone
- IMS-integrated Mobile (Basic)
- Carrier-integrated Mobile
- Cisco Dual Mode for Android

Configure Enterprise Directory User Search

Use this procedure to configure phones and clients in your system to perform user searches against an enterprise directory server instead of the database.

Before you begin

- Ensure that the primary, secondary, and tertiary servers, which you choose for LDAP user search, are network reachable to the Unified Communications Manager subscriber nodes.
- From **System** > **LDAP** > **LDAP System**, configure the type of LDAP server from the **LDAP Server Type** drop-down list in the **LDAP System Configuration** window.

Procedure

Step 1 In Cisco Unified CM Administration, choose **System** > **LDAP** > **LDAP Search**.

Step 2 To enable user searches to be performed using an enterprise LDAP directory server, check the **Enable user search to Enterprise Directory Server** check box.

Step 3 Configure the fields in the **LDAP Search Configuration** window. See the online help for more information about the fields and their configuration options.

Step 4 Click **Save**.

LDAP Attributes for UDS Search of Directory Server

The following table lists the LDAP attributes that UDS users search request uses when the **Enable user search to Enterprise Directory Server** option is enabled. For these types of directory requests, UDS acts as a proxy and relays the search request to the corporate directory server.

Note UDS users response tag may be mapped to one of the LDAP attributes. The mapping of the attributes is determined by the option you select from the **LDAP Server Type** drop-down list. Access this drop-down list from **System** > **LDAP** > **LDAP System Configuration** window.

UDS Users Response Tag	LDAP Attribute
userName	• samAccountName • uid
firstName	givenName
lastName	sn
middleName	• initials • middleName
nickName	nickName
displayName	displayName
phoneNumber	• telephonenumber • ipPhone
homeNumber	homephone
mobileNumber	mobile
email	mail

UDS Users Response Tag	LDAP Attribute
directoryUri	• msRTCSIP-primaryuseraddress • mail
department	• department • departmentNumber
manager	manager
title	title
pager	pager

Configure LDAP Authentication

Perform this procedure if you want to enable LDAP authentication so that end user passwords are authenticated against the password that is assigned in the company LDAP directory. This configuration applies to end user passwords only and does not apply to end user PINs or application user passwords.

Procedure

Step 1 In Cisco Unified CM Administration, choose **System** > **LDAP** > **LDAP Authentication**.

Step 2 Check the **Use LDAP Authentication for End Users** check box to use your LDAP directory for user authentication.

Step 3 In the **LDAP Manager Distinguished Name** field, enter the user ID of the LDAP Manager who has access rights to the LDAP directory.

Step 4 In the **Confirm Password** field, enter the password for the LDAP manager.

Note Ensure that you renter the LDAP password when you are upgrading your Unified Communications Manager from Release 11.5(1)SU2 to Release 14SU3 and above.

Step 5 In the **LDAP User Search Base** field, enter the search criteria.

Step 6 In the **LDAP Server Information** section, enter the hostname or IP address of the LDAP server.

Step 7 If you want to use TLS to create a secure connection to the LDAP server, check the **Use TLS** check box.

Step 8 Click **Save**.

What to do next

Customize LDAP Agreement Service Parameters, on page 275

Customize LDAP Agreement Service Parameters

Perform this procedure to configure the optional service parameters that customize the system-level settings for LDAP agreements. If you do not configure these service parameters, Unified Communications Manager applies the default settings for LDAP directory integration. For parameter descriptions, click the parameter name in the user interface.

You can use service parameters to customize the below settings:

- **Maximum Number of Agreements**—Default value is 20.
- **Maximum Number of Hosts**—Default value is 3.
- **Retry Delay On Host Failure (secs)**—Default value for host failure is 5.
- **Retry Delay On HotList failure (mins)**—Default value for hostlist failure is 10.
- **LDAP Connection Timeouts (secs)**—Default value is 5.
- **Delayed Sync Start time (mins)**—Default value is 5.
- **User Customer Map Audit Time**

Procedure

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

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

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

Step 4 Configure values for the Cisco DirSync service parameters.

Step 5 Click **Save**.

LDAP Directory Service Parameters

Service Parameter	Description
Maximum Number Of Agreements	The maximum number of LDAP directories that you can configure. The default setting is 20.
Maximum Number Of Hosts	The maximum number of LDAP hostnames that you can configure for failover purposes. The default value is 3.
Retry Delay On Host Failure (secs)	After a host failure, the number of seconds that Cisco Unified Communications Manager delays before it retries the connection to the first LDAP server (hostname). The default value is 5.
Retry Delay On HostList Failure (mins)	After a hostlist failure, the number of minutes that Cisco Unified Communications Manager delays before it retries every configured LDAP server (hostnames). The default is 10.
LDAP Connection Timeout (secs)	The number of seconds that Cisco Unified Communications Manager allows for establishing the LDAP connection. The LDAP service provider aborts the connection attempt if a connection cannot be established in the specified amount of time. The default is 5.

Service Parameter	Description
Delayed Sync Start time (mins)	The number of minutes that Cisco Unified Communications Manager delays in starting the directory synchronization process after the Cisco DirSync service starts. The default is 5.

Convert LDAP Synchronized User to Local User

When you synchronize your LDAP directory with Cisco Unified Communications Manager, for LDAP-synchronized end users, you cannot edit any of the fields within the **End User Configuration** window unless you convert the LDAP-synchronized user to a local user.

To edit to an LDAP-synchronized field in the **End User Configuration** window, convert the user to a local user. However, if you perform this conversion, the end user will not be updated when Cisco Unified Communications Manager synchronizes with the LDAP directory.

Procedure

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

Step 2 Click **Find** and select the end user.

Step 3 Click the **Convert to Local User** button.

Step 4 Make your updates in the **End User Configuration** window.

Step 5 Click **Save**.

Assign LDAP Synchronized Users to an Access Control Group

Perform this procedure to assign LDAP synchronized users to an access control group.

Before you begin

Cisco Unified Communications Manager must be configured to synchronize end users with an external LDAP directory.

Procedure

Step 1 In Cisco Unified CM Administration, choose **System** > **LDAP** > **LDAP Directory**.

Step 2 Click **Find** and select a configured LDAP Directory.

Step 3 Click the **Add to Access Control Group** button.

Step 4 Select the access control groups that you want to apply to the end users in this LDAP directory.

Step 5 Click **Add Selected**.

Step 6 Click **Save**

Step 7 Click **Perform Full Sync**.
Cisco Unified Communications Manager syncs with the external LDAP directory and synchronized users get inserted into the correct access control group.

Note The synchronized users get inserted into the selected access group only when you add an access control group for the first time. Any subsequent group that you add to LDAP will not be applied to the synchronized users after performing a full sync.

CHAPTER 38

Configure End Users Manually

Manual End User Provision Overview

If you are not importing end users from an LDAP directory, you can use either of the following methods to add your end users to the Unified Communications Manager database:

- Import using Bulk Administration Tool
- Manually add new users

Manual End User Provisioning Prerequisites

Before importing your end users, plan and configure the roles, access aontrol groups, and credential policies for your end users.

- User Access Configuration Task Flow, on page 231
- Credential Policy Configuration Task Flow, on page 248

Import End Users using Bulk Administration

Using the Bulk Administration Tool, you can perform bulk transactions to the Cisco Unified Communications Manager database, including importing and updating large numbers of end users, phones, and ports, in a single process. The Bulk Administration Tool allows you to import the end user list, and end user configurations, from a CSV file into the database.

For details on how to use the Bulk Administration Tool to import end users, see the *Bulk Administration Guide for Cisco Unified Communications Manager*.

Manual End User Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Add a New End User, on page 280	Add a new end user to the database manually.
Step 2	Assign End Users to an Access Control Group, on page 281	Assign any local end users that you provision to an access control group with the required role permissions. Local users include any manually provisioned end users and any end users whom you import using the Bulk Administration Tool. Local users have a User Status of 'Active Local User' in **End User Configuration**.
Step 3	Apply Credential Policy to End User, on page 281	(Optional). Confirm if the default credential policy can be applied to this end user. If not, apply a credential policy to the end user PIN or password.
Step 4	Assign Feature Group Template to Local End Users, on page 282	Assign a feature group template for the end user. When you assign the feature group template, the system assigns to the end user the user profile, service profile, universal line and device templates, and self-provisioning settings that are associated to that feature group template.

Add a New End User

Use this procedure to add a new end user to the Unified Communications Manager database manually.

Procedure

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

Step 2 Click **Add New**.

Step 3 Enter the **User ID** and **Last name**.

Step 4 Choose the **User Rank** from the drop-down list.

Step 5 Complete the fields in the **End User Configuration** window. For field descriptions, see the online help.

Step 6 Click **Save**.

What to do next

Assign End Users to an Access Control Group, on page 281

Assign End Users to an Access Control Group

Use this procedure to assign provisioned users to an access control group. For LDAP Synchronized users that were assigned to an access control group during the LDAP sync, you can also use this procedure to assign additional access control groups. This may be useful if your LDAP sync configuration included a common access control group, but you require that some users be assigned to additional access control groups based on their role.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Access Control Group**.

Step 2 Click **Find** and select an access control group.

Step 3 Click **Add End Users to Group**.

Step 4 In the **Find and List Users** window, select the end users whom you want to add to the group.

Step 5 Click **Add Selected**.

Step 6 Click **Save**.

Apply Credential Policy to End User

Apply a configured credential policy to a specific end user password or end user PIN. You may need to do this if you need to make an update from the default credential policy.

Note You can also apply a credential policy to an application user password. For details, see the *Administration Guide for Cisco Unified Communications Manager*.

Procedure

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

Step 2 Click **Find** and select the end user.

Step 3 Click the **Edit Credential** button that corresponds to the password or PIN, depending on the credential to which you want to apply the credential policy.

Step 4 From the **Authentication Rule** drop-down list, choose the credential policy that you want to apply.

Step 5 Complete any additional fields in the **Credential Configuration** window. For help with the fields and their settings, see the online help.

Step 6 Click **Save**.

Assign Feature Group Template to Local End Users

Assign a feature group template to a local end user. A local end user is an end user who has been either added to the database manually, or imported using the Bulk Administration Tool. Local end users are not synchronized with an external LDAP directory.

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **Quick User/Phone Add**.

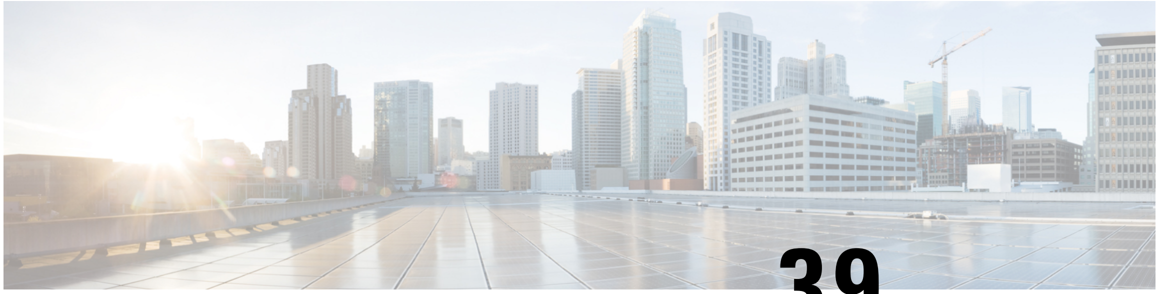
Step 2 Click **Find** and select an end user.

Step 3 From the **Feature Group Template** drop-down list, select the feature group template that you have configured for this end user.

Step 4 Click **Save**.

PART VI

Configure Endpoint Devices



CHAPTER 39

Endpoint Devices Overview

About Endpoint Device Configuration

The chapters in this part provide information about how to configure endpoint devices, and how to associate users with endpoints.

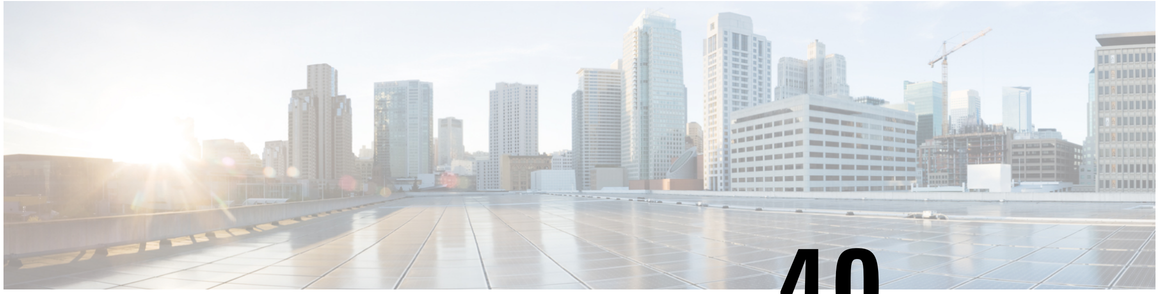
Endpoint Device Configuration

Complete the following task flows to configure end users for your system.

Procedure

	Command or Action	Purpose
Step 1	Configure Analog Telephone Adaptor, on page 298	Configure an analog telephone adapter that acts as an interface between analog telephones and IP-based telephony networks.
Step 2	Software-Based Endpoint Configuration, on page 335	Configure software-based endpoints such as CTI ports, H.323 clients, and Cisco IP Communicator.
Step 3	Cisco IP Phones Configuration Task Flow, on page 345	Configure Cisco IP Phones to function on your network.
Step 4	Diagnostics and Reporting Configuration Task Flow, on page 371	Use call diagnostics and the Quality Reporting Tool (QRT) to ensure call quality on Cisco IP Phones.
Step 5	Third-Party SIP Endpoints Configuration Task Flow, on page 383	Configure third-party SIP endpoints.

	Command or Action	Purpose
Step 6	Configure Device Profiles and Templates Task Flow, on page 390	Configure the profiles and templates that define the services, features, and directory numbers that associate with a particular device.
Step 7	Users and Devices Configuration Task Flow, on page 401	Associate devices with end users and application users.



CHAPTER 40

Configure Mobile and Remote Access

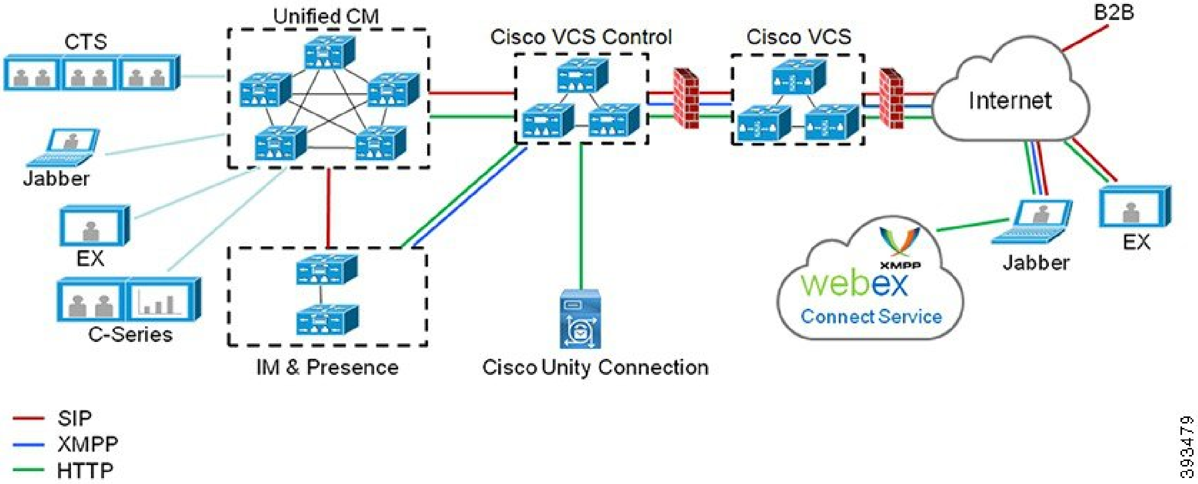
Mobile and Remote Access Overview

Unified Communications Manager Mobile and Remote Access is a core part of the Cisco Collaboration Edge Architecture. It allows endpoints such as Cisco Jabber to have their registration, call control, provisioning, messaging, and presence services that are provided by Unified Communications Manager when the endpoint is not within the enterprise network. Cisco Expressway connects the mobile endpoint to the on-premises network, providing secure firewall traversal and line-side support for Unified CM registrations.

The overall solution provides:

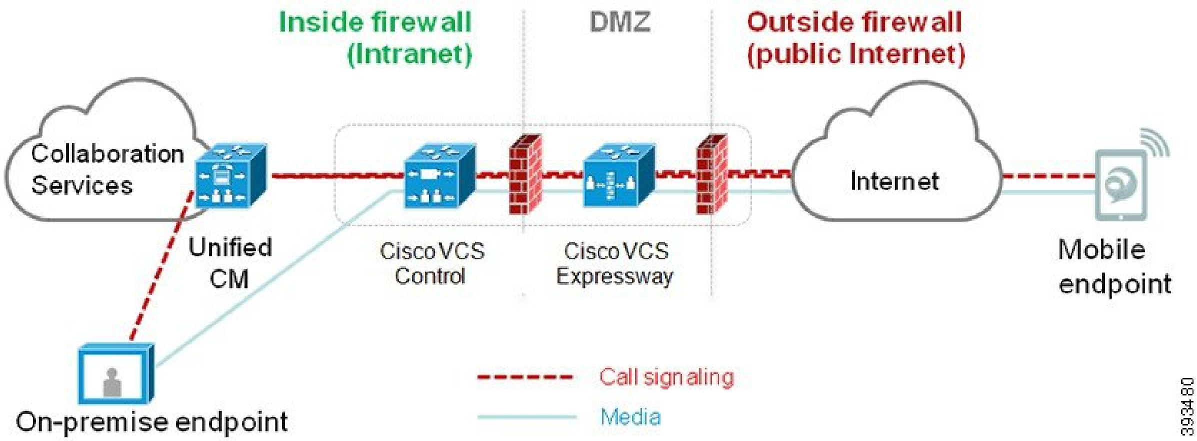
- Off-premises access: a consistent experience outside the network for Jabber and EX/MX/SX Series clients
- Security: secure business-to-business communications
- Cloud services: enterprise grade flexibility and scalable solutions providing rich Webex integration and Service Provider offerings
- Gateway and interoperability services: media and signaling normalization, and support for non-standard endpoints

Figure 3: Unified Communications: Mobile and Remote Access



Third-party SIP or H.323 devices can register to the Expressway-C and, if necessary, interoperate with Unified CM-registered devices over a SIP trunk.

Figure 4: Typical Call Flow: Signaling and Media Paths



- Unified CM provides call control for both mobile and on-premises endpoints.
- Signaling traverses the Expressway solution between the mobile endpoint and Unified CM.
- Media traverses the Expressway solution and is relayed between endpoints directly; all media is encrypted between the Expressway-C and the mobile endpoint.

Configuring Mobile and Remote Access

To enable Cisco Jabber users with Mobile and Remote Access functionality, set up an Mobile and Remote Access User Policy within the **User Profile Configuration** window of Unified Communications Manager. The Mobile and Remote Access User Policy is not required for non-Jabber endpoints.

In addition, you must configure Cisco Expressway with Mobile and Remote Access. For details, see Mobile and Remote Access via Cisco Expressway Deployment Guide .

Mobile and Remote Access Prerequisites

Cisco Unified Communications Manager Requirements

The following requirements apply:

- If you are deploying multiple Unified Communications Manager clusters, set up an ILS network.
- Mobile and Remote Access requires that you set up NTP servers for your deployment. Make sure that you have NTP servers deployed for your network and Phone NTP References for SIPendpoints.

DNS Requirements

For the internal connection to Cisco Expressway, configure the following locally resolvable DNS SRV that points to Unified Communications Manager:

```
_cisco-uds._tcp<domain>
```

You must create internal DNS records, for both forward and reverse lookups, for all Unified Communications nodes used with Mobile and Remote Access. This allows Expressway-C to find the nodes when IP addresses or hostnames are used instead of FQDNs. Make sure that the SRV record is not resolvable outside of the local network.

Cisco Expressway Requirements

This feature requires you to integrate Unified Communications Manager with Cisco Expressway. For Cisco Expressway configuration details for Mobile and Remote Access, refer to the Mobile and Remote Access Through Cisco Expressway Deployment Guide.

The minimum Expressway release for Mobile and Remote Access Access Policy support with Cisco Jabber is X8.10.

Certificate Prerequisites

You must exchange certificates between Unified Communications Manager, the IM and Presence Service, and Cisco Expressway-C. Cisco recommends that you use CA-signed certificates with the same CA for each system. In this case:

- Install the CA root certificate chain on each system (for Unified Communications Manager and the IM and Presence Service Service install the certificate chain to the tomcat-trust store).
- For Unified Communications Manager, issue a CSR to request CA-signed tomcat (for AXL and UDS traffic) and Cisco CallManager (for SIP) certificates.
- For the IM and Presence Service Service, issue a CSR to request CA-signed tomcat certificates.

Note If you use different CAs, you must install each CA's root certificate chain on Unified Communications Manager, IM and Presence Service Service, and Expressway-C.

Note You can also use self-signed certificates for both Unified Communications Manager and the IM and Presence Service Service. In this case, you must upload onto Expressway-C the tomcat and Cisco CallManager certificates for Unified Communications Manager and a tomcat certificate for the IM and Presence Service Service.

Mobile and Remote Access Configuration Task Flow

Complete these tasks in Cisco Unified Communications Manager if you want to deploy Mobile and Remote Access endpoints.

Procedure

	Command or Action	Purpose
Step 1	Activate Cisco AXL Web Service, on page 290	Make sure that the Cisco AXL Web Service is activated on the publisher node.
Step 2	Configure Maximum Session BitRate for Video, on page 291	Optional. Configure Region-specific settings for your MRA endpoints. For example, if you expect MRA endpoints to use video, you may want to increase the **Maximum Session Bit Rate for Video Calls** setting as the default setting of 384 kbps may be too low for some video endpoints.
Step 3	Configure a Device Pool for Mobile and Remote Access, on page 291	Assign your Date/Time Group and Region configuration to the device pool that your MRA endpoints will use.
Step 4	Configure Phone Security Profile for Mobile and Remote Access, on page 293	Use this procedure to set up a phone security profile to be used by MRA endpoints.
Step 5	Configure MRA Access Policy for Cisco Jabber Users, on page 293	Cisco Jabber only. Set up an MRA Access Policy for Cisco Jabber users. Cisco Jabber users must be enabled with MRA access within their user profiles in order to use the MRA feature.
Step 6	Configure Users for MRA, on page 295	For Cisco Jabber users, the User Policy that you set up must be applied to their End User Configurations.
Step 7	Configure Endpoints for MRA , on page 295	Configure and provision endpoints that will use the MRA feature.

Activate Cisco AXL Web Service

Make sure that the Cisco AXL Web Service is activated on the publisher node.

Procedure

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

Step 2 From the **Server** drop-down list, select the publisher node and click **Go**.

Step 3 Under **Database and Admin Services**, confirm that the **Cisco AXL Web Service** is **Activated**.

Step 4 If the service is not activated, check the corresponding check box and click **Save** to activate the service.

Configure Maximum Session BitRate for Video

Configure Region settings for your Mobile and Remote Access endpoints. The default settings may be sufficient in many cases, but if you expect Mobile and Remote Access endpoints to use video, you may want to increase the **Maximum Session Bit Rate for Video Calls** within your Region Configuration. The default setting of 384 kbps may be too low for some video endpoints, such as the DX series.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Region Information** > **Region**.

Step 2 Perform any one of the following:

- Click **Find** and select the region to edit the bit rates within an existing region.
- Click **Add New** to create a new region.

Step 3 In the **Modify Relationship to other Regions** area, configure a new setting for the **Maximum Session Bit Rate for Video Calls**. For example, 6000 kbps.

Step 4 Configure any other fields in the **Region Configuration** window. For more information on the fields and their configuration options, see Online Help..

Step 5 Click **Save**.

Configure a Device Pool for Mobile and Remote Access

When you created a new region, assign your region to the device pool that your Mobile and Remote Access endpoints use.

Procedure

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

Step 2 Do either of the following:

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

Step 3 Enter a **Device Pool Name**.

Step 4 Select a redundant **Cisco Unified Communications Manager Group**.

Step 5 Assign the **Date/Time Group** that you set up. This group includes the Phone NTP references that you set up for Mobile and Remote Access endpoints.

Step 6 From the **Region** drop-down list, select the region that you configured for Mobile and Remote Access.

Step 7 Complete the remaining fields in the **Device Pool Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 8 Click **Save**.

Configure ICE

Use this procedure if you want to deploy ICE to handle call setup for Mobile and Remote Access calls. ICE is an optional deployment that uses STUN and TURN services to analyze the available media paths for an Mobile and Remote Access call and to select the best path. ICE adds potentially to the call setup time, but increases the reliability of Mobile and Remote Access calls.

Before you begin

Decide how you are going to deploy ICE. You can configure ICE for groups of phones via the Common Phone Profile Configuration, to individual Cisco Jabber desktop devices, or through system-wide defaults that apply to all phones.

As a fallback mechanism, ICE can use a TURN server to relay media. Make sure that you have deployed a TURN server.

Procedure

Step 1 From Cisco Unified CM Administration:

- Choose **System** > **Enterprise Phone** to configure system defaults for ICE.
- Choose **Device** > **Device Settings** > **Common Phone Profile** to configure ICE for groups of endpoints and select the profile you want to edit.
- Choose **Device** > **Phone** to configure ICE for an individual Cisco Jabber desktop endpoint and select the endpoint that you want to edit.

Step 2 Scroll down to the **Interactive Connectivity Establishment (ICE)** section.

Step 3 Set the **ICE** drop-down list to **Enabled**.

Step 4 Set the **Default Candidate Type**:

- **Host**—A candidate obtained by selecting the IP address on the host device. This is the default.
- **Server Reflexive**—An IP address and port candidate obtained by sending a STUN request. In many cases, this may represent the public IP address of the NAT.
- **Relayed**—An IP address and port candidate obtained from a TURN server. The IP address and port are resident on the TURN server such that media is relayed through the TURN server.

Step 5 From the **Server Reflexive Address** drop-down list, select whether you want to enable STUN-like services by setting this field to **Enabled** or **Disabled**. You must set this field to enabled if you configured Server Relexive as the Default Candidate.

Step 6 Enter the IP address or hostname for the Primary and Secondary TURN Servers.

Step 7 Set the **TURN Server Transport Type** to **Auto (default setting)**, **UDP**, **TCP**, or **TLS**.

Step 8 Enter the **Username** and **Password** of the TURN Server.

Step 9 Click **Save**.

Note If you configured ICE for a Common Phone Profile, you must associate phones to that Common Phone Profile for phones to be able to use the profile. You can apply the profile to a phone through the **Phone Configuration** window.

Configure Phone Security Profile for Mobile and Remote Access

Use this procedure to set up a phone security profile to be used by Mobile and Remote Access endpoints.

Procedure

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

Step 2 Click **Add New**.

Step 3 From the **Phone Security Profile Type** drop-down list, select your device type. For example, you could select **Cisco Unified Client Service Framework** for a Jabber application.

Step 4 Click **Next**.

Step 5 Enter a **Name** for the profile. For Mobile and Remote Access, the name must be in FQDN format and must include the enterprise domain.

Step 6 From the **Device Security Mode** drop-down list, select **Encrypted**.

Note This field must be set to **Encrypted**. Otherwise, Expressway rejects communications.

Step 7 Set the **Transport Type** to **TLS**.

Step 8 Leave the **TFTP Encrypted Config** check box unchecked for the following phones as Mobile and Remote Access will not work for these phones with this option enabled: DX Series, IP Phone 7800, or IP Phone 8811, 8841, 8845, 8861 and 8865

Step 9 Complete the remaining fields in the **Phone Security Profile Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 10 Click **Save**.

Note You must apply this profile to the Phone Configuration for each of your Mobile and Remote Access endpoints.

Configure MRA Access Policy for Cisco Jabber Users

Use this procedure to set up an MRA Access Policy for Cisco Jabber users. Cisco Jabber users must be enabled with MRA access within their user profiles in order to use the MRA feature. The minimum Expressway release for MRA Access Policy support with Cisco Jabber is X8.10.

Note The MRA Access Policy is not required for non-Jabber users.

Note For more details on user profiles, see User Profile Overview, on page 251.

Procedure

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

Step 2 Click **Add New**.

Step 3 Enter a **Name** and **Description** for the user profile.

Step 4 Assign a **Universal Device Template** to apply to users' **Desk Phones**, **Mobile and Desktop Devices**, and **Remote Destination/Device Profiles**.

Step 5 Assign a **Universal Line Template** to apply to the phone lines for users in this user profile.

Step 6 If you want the users in this user profile to be able to use the self-provisioning feature to provision their own phones, do the following:

a) Check the **Allow End User to Provision their own phones** check box.

b) In the **Limit Provisioning once End User has this many phones** field, enter a maximum number of phones the user is allowed to provision. The maximum is 20.

Step 7 If you want Cisco Jabber users who are associated with this user profile, to be able to use the Mobile and Remote Access feature, check the **Enable Mobile and Remote Access** check box.

Note
- By default, this check box is selected. When you uncheck this check box, the **Client Policies** section is disabled, and No Service client policy option is selected by default.
- This setting is mandatory only for Cisco Jabber users whom are using OAuth Refresh Logins. Non-Jabber users do not need this setting to be able to use Mobile and Remote Access. Mobile and Remote Access feature is applicable only for the Jabber Mobile and Remote Access users and not to any other endpoints or clients.

Step 8 Assign the Jabber policies for this user profile. From the **Desktop Client Policy**, and **Mobile Client Policy** drop-down list, choose one of the following options:

- No Service—This policy disables access to all Cisco Jabber services.
- IM & Presence only—This policy enables only instant messaging and presence capabilities.
- IM & Presence, Voice and Video calls—This policy enables instant messaging, presence, voicemail, and conferencing capabilities for all users with audio or video devices. This is the default option.

Note Jabber desktop client includes Cisco Jabber for Windows users and Cisco Jabber for Mac users. Jabber mobile client includes Cisco Jabber for iPad and iPhone users and Cisco Jabber for Android users.

Step 9 Click **Save**.

Configure Users for MRA

For Cisco Jabber users, the MRA access policy that you configured must be associated to your Cisco Jabber users during the LDAP sync. For information on how to provision end users, see the End User Configuration, on page 225.

Configure Endpoints for MRA

Provision and configure endpoints for Mobile and Remote Access:

- For Cisco Jabber clients, refer to Cisco Jabber Configuration Task Flow, on page 459
- For other endpoints, refer to Endpoint Device Configuration, on page 285

Configure Cisco Expressway for Mobile and Remote Access

For details on how to configure Cisco Expressway for Mobile and Remote Access, refer to the Mobile and Remote Access Through Cisco Expressway Deployment Guide.

CHAPTER 41

Configure Analog Telephone Adaptors

Analog Telephone Adaptor Overview

The Cisco Analog Telephone Adaptor (ATA) functions as an analog telephone adapter that interfaces regular analog telephones to IP-based telephony networks. The Cisco ATA converts any regular analog telephone into an Internet telephone. Each adapter supports two voice ports, each with its own telephone number.

Like other IP devices, the Cisco ATA receives its configuration file and list of Unified Communications Managers from the TFTP server. If the TFTP server does not have a configuration file, the Cisco ATA uses the TFTP server name or IP address and port number as the primary Unified Communications Manager name or IP address and port number.

The Cisco ATA:

- Contains a single 10 BaseT RJ-45 port and two RJ-11 FXS standard analog telephone ports
- Supports a number of codecs, including G.711 alaw, G.711 mulaw, and G.723 and G.729a voice codecs
- Converts voice into IP data packets
- Supports redial, speed dial, call forwarding, call waiting, call hold, transfer, conference, voice messaging, message-waiting indication, off-hook ringing, caller-ID, callee-ID, and call waiting caller-ID

The ATA 180 series uses SCCP, while the ATA 190 series uses SIP. For more information, see the ATA documentation:

- ATA 180 Series: https://www.cisco.com/c/en/us/support/unified-communications/ata-180-series-analog-telephone-adaptors/tsd-products-support-series-home.html
- ATA 190 Series: https://www.cisco.com/c/en/us/support/unified-communications/ata-190-series-analog-telephone-adapters/tsd-products-support-series-home.html

Configure Analog Telephone Adaptor

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.
The **Find and List Phones** window appears.

Step 2 Click **Add New**.

Step 3 From the **Phone Type** drop down list, select the Analog Telephone Adaptor model you have and click **Next**.
The **Phone Configuration** window appears.

Step 4 Configure the fields in the **Phone Configuration** window.

See the Related Topics section for more information about the fields and their configuration options.

Step 5 Click **Save**.

Step 6 Click **Apply Config** for your changes to take effect and synchronize the phone.

Analog Telephone Adaptor 186 Configuration Fields

Table 21: Analog Telephony Adaptor 186 Configuration Fields

Field	Description
MAC Address	Enter the Media Access Control (MAC) address that identifies ATA 186. Make sure that the value comprises 12 hexadecimal characters. You can determine the MAC address for ATA 186 in any of these ways: • Look at the MAC label on the back of ATA 186. • Display the web page for ATA 186 and click the **Device Information** hyperlink.
Description	Enter a text description of the ATA 186. This field can contain up to 128 characters. You can use all characters except quotes (“), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).
Device Pool	Choose the device pool to which you want the ATA 186 assigned. The device pool defines sets of common characteristics for devices, such as region, date/time group, and softkey template. To see the Device Pool configuration settings, click the View Details link.
Common Device Configuration	Choose the Common Device Configuration to which you want the ATA 186 assigned. To see the Common Device Configuration settings, click the View Details link.

Field	Description
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.
Common Phone Profile	From the drop-down list, choose a common phone profile from the list of available common phone profiles. To see the Common Phone Profile settings, click the View Details link.
Calling Search Space	From the drop-down list, choose the calling search space or leave the calling search space as the default of <None>.
AAR Calling Search Space	From the drop-down list, choose the appropriate calling search space for the device to use when it performs automated alternate routing (AAR) or leave the calling search space as the default of <None>.
Media Resource Group List	Choose the appropriate Media Resource Group List. A Media Resource Group List comprises a prioritized grouping of media resource groups. If you choose **<None>**, Cisco Unified CM uses the Media Resource Group List that is defined in the device pool.
Location	From the drop-down list, choose the location that is associated with the phones and gateways in the device pool.
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. Cisco Unified CM uses the AAR group that is associated with Device Pool or Line.
User Locale	From the drop-down list, choose the user locale that is associated with the ATA 186. The user locale identifies a set of detailed information to support users, including language and font. If you do not specify a user locale, Cisco Unified CM uses the user locale that is associated with the device pool.
Network Locale	From the drop-down list, choose the network locale that is associated with the ATA 186. The network locale contains a definition of the tones and cadences that the phone in a specific geographic area uses. If you do not specify a network locale, Cisco Unified CM uses the network locale that is associated with the device pool.
Device Mobility Mode	From the drop-down list, 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 a device.
Owner	Select **User** or **Anonymous** (Public/Shared Space, for the owner type.

Field	Description
Owner User ID	From the drop-down list, choose the user ID of the assigned phone user. The user ID gets recorded in the call detail record (CDR) for all calls made from this device. Assigning a user ID to the device also moves the device from “Unassigned Devices” to “Users” in the License Usage Report. **Note** Do not configure this field if you are using extension mobility. Extension mobility does not support device owners.
Phone Load Name	Enter the custom software for ATA 186.
Use Trusted Relay Point	Choose one of the following values: • Off—Choose this value to disable the use of a Trusted Relay Point (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. • 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.
Always Use Prime Line	From the drop-down list, choose one of the following options: • Off—When the phone is idle and receives a call on any line, the phone user answers the call from the line on which the call is received. • On—When the phone is idle (off hook) and receives a call on any line, the primary line gets chosen for the call. Calls on other lines continue to ring, and the phone user must select those other lines to answer these calls. • Default— Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter, which supports the Cisco CallManager service.
Always Use Prime Line for Voice Message	From the drop-down list, choose one of the following options: • Off—If the phone is idle, pressing the Messages button on the phone automatically dials the voice-messaging system from the line that has a voice message. Unified Communications Manager always selects the first line that has a voice message. If no line has a voice message, the primary line gets used when the phone user presses the Messages button. • 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 • Default—Unified Communications Manager uses the configuration from the Always Use Prime Line for Voice Message service parameter, which supports the Cisco CallManager service.

Field	Description
Geolocation	From the drop-down list, 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.
Ignore Presentation Indicators (internal calls only)	Check this check box to configure call display restrictions on a call-by-call basis. When this check box is checked, Unified 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.
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	When the CTI port gets added to a hunt list, the administrator can log the user in or out by checking (and unchecking) this check box. Users use the softkey on the phone to log their phone in or out of the hunt list.
Remote Device	Check this box to allocate a buffer for the 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.
Hot Line Device	Check this check box to make this device a Hotline device. Hotline devices can only connect to other Hotline devices. This feature is an extension of PLAR, which configures a phone to automatically dial one directory number when it goes off-hook. Hotline provides additional restrictions that you can apply to devices that use PLAR. To implement Hotline, you must also create a softkey template without supplementary service softkeys, and apply it to the Hotline device.

Number Presentation Transformation

Table 22: Caller ID for Calls From This Phone

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.

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.

Table 23: Remote Number

Field	Description
Calling Party Transformation CSS	From the drop-down list, choose the calling search space (CSS) that contains the calling party transformation pattern that you want to apply on the remote calling number for calls received on this device.
Use Device Pool Calling Party Transformation CSS	Check this check box to apply the Calling Party Transformation CSS configured at the device pool to which this device belongs to transform the remote calling and remote connected number.

Table 24: Protocol Specific Information

Field	Description
BLF Presence Group	From the drop-down list, choose a Busy Lamp Field (BLF) presence group for the end user. The selected group specifies the destinations that the end user can monitor The default value for BLF Presence Group specifies Standard Presence group, configured with installation. BLF Presence Groups that are configured in Cisco Unified Administration also appear in the drop-down list.
Device Security Profile	Choose the security profile to apply to the device. You must apply a security profile to all devices that are configured in Unified Communications Manager Administration.
SUBSCRIBE Calling Search Space	Supported with the Presence feature, the SUBSCRIBE calling search space determines how Unified Communications Manager routes presence requests that come from the end user. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the end user. From the drop-down list, 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. 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 can configure a calling search space as you do all calling search spaces.
Unattended Port	Check this check box to indicate an unattended port on this device.

Field	Description
RFCC 2833 Disabled	For devices that are running SCCP, check this check box to disable RFC2833 support.

Table 25: Product-Specific Configuration Layout

Field	Description
Model-specific configuration fields that the device manufacturer defines	To view field descriptions and help for product-specific configuration items, click the "?" information icon in the Product Specific Configuration area to display help in a popup dialog box. If you need more information, see the documentation for ATA 186.

Analog Telephone Adaptor 187 Configuration Fields

Table 26: Analog Telephony Adaptor 187 Configuration Fields

Field	Description
MAC Address	Enter the Media Access Control (MAC) address that identifies ATA 187. Make sure that the value comprises 12 hexadecimal characters. You can determine the MAC address for ATA 187 in any of these ways: • Look at the MAC label on the back of ATA 187. • Display the web page for ATA 187 and click the **Device Information** hyperlink.
Description	Enter a text description of the ATA 187. This field can contain up to 128 characters. You can use all characters except quotes ("), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).
Device Pool	Choose the device pool to which you want the ATA 187 assigned. The device pool defines sets of common characteristics for devices, such as region, date/time group, and softkey template. To see the Device Pool configuration settings, click the View Details link.
Common Device Configuration	Choose the Common Device Configuration to which you want the ATA 187 assigned. 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.

Field	Description
Common Phone Profile	From the drop-down list, choose a common phone profile from the list of available common phone profiles. To see the Common Phone Profile settings, click the View Details link.
Calling Search Space	From the drop-down list, choose the calling search space or leave the calling search space as the default of <None>.
AAR Calling Search Space	From the drop-down list, choose the appropriate calling search space for the device to use when it performs automated alternate routing (AAR) or leave the calling search space as the default of <None>.
Media Resource Group List	Choose the appropriate Media Resource Group List. A Media Resource Group List comprises a prioritized grouping of media resource groups. If you choose **<None>**, Cisco Unified CM uses the Media Resource Group List that is defined in the device pool.
User Hold MOH Audio Source	From the drop-down list, choose the audio source to use for music on hold (MOH) when a user initiates a hold action.
Location	From the drop-down list, choose the location that is associated with the phones and gateways in the device pool.
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. If no AAR group is specified, Cisco Unified CM uses the AAR group that is associated with Device Pool or Line.
User Locale	From the drop-down list, choose the user locale that is associated with the CTI Port. The user locale identifies a set of detailed information to support users, including language and font. If you do not specify a user locale, Cisco Unified CM uses the user locale that is associated with the device pool.
Network Locale	From the drop-down list, choose the network locale that is associated with the CTI Port. The network locale contains a definition of the tones and cadences that the phone in a specific geographic area uses. If you do not specify a network locale, Cisco Unified CM uses the network locale that is associated with the device pool.
Built in Bridge	Enable or disable the built-in conference bridge for the barge feature by using the Built In Bridge drop-down list. Choose one of the following: • On • Off • Default
Privacy	For Privacy, choose **On** in the Privacy drop-down list.

Field	Description
Device Mobility Mode	From the drop-down list, 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.
Owner	Select **User** or **Anonymous (Public/Shared Space)** , for the owner type.
Owner User ID	From the drop-down list, choose the user ID of the assigned phone user. The user ID gets recorded in the call detail record (CDR) for all calls made from this device. Assigning a user ID to the device also moves the device from "Unassigned Devices" to "Users" in the License Usage Report. **Note** Do not configure this field if you are using extension mobility. Extension mobility does not support device owners.
Phone Load Name	Enter the custom software for ATA 187.
Use Trusted Relay Point	Choose one of the following values: • **Off**—Choose this value to disable the use of a Trusted Relay Point (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. • **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.
Always Use Prime Line	From the drop-down list, choose one of the following options: • Off—When the phone is idle and receives a call on any line, the phone user answers the call from the line on which the call is received. • On—When the phone is idle (off hook) and receives a call on any line, the primary line gets chosen for the call. Calls on other lines continue to ring, and the phone user must select those other lines to answer these calls. • Default—Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter, which supports the Cisco CallManager service.

Field	Description
Always Use Prime Line for Voice Message	From the drop-down list, choose one of the following options: • Off—If the phone is idle, pressing the Messages button on the phone automatically dials the voice-messaging system from the line that has a voice message. Unified Communications Manager always selects the first line that has a voice message. If no line has a voice message, the primary line gets used when the phone user presses the Messages button. • 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 • Default—Unified Communications Manager uses the configuration from the Always Use Prime Line for Voice Message service parameter, which supports the Cisco CallManager service.
Geolocation	From the drop-down list, 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.
Ignore Presentation Indicators (internal calls only)	Check this check box to configure call display restrictions on a call-by-call basis. When this check box is checked, Unified 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.
Logged into Hunt Group	When the ATA 187 gets added to a hunt list, the administrator can log the user in or out by checking (and unchecking) this check box. Users use the softkey on the phone to log their phone in or out of the hunt list.
Remote Device	Check this box to allocate a buffer for the 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.

Field	Description
Protected Device	Check this check box to designate a phone as protected, which enables the phone to play a 2-second tone to notify the user when a call is encrypted and both phones are configured as protected devices. The tone plays for both parties when the call is answered. The tone does not play unless both phones are protected and the call occurs over encrypted media. Checking this check box represents only one of several configuration requirements for the secure indication tone to play. For a detailed description of the secure indication tone feature and the configuration requirements, see the *Feature Configuration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html. If you check this check box and the system determines that the call is not encrypted, the phone plays nonsecure indication tone to alert the user that the call is not protected.

Number Presentation Transformation

Table 27: Caller ID for Calls From This Phone

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.
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.

Table 28: Remote Number

Field	Description
Calling Party Transformation CSS	From the drop-down list, choose the calling search space (CSS) that contains the calling party transformation pattern that you want to apply on the remote calling number for calls received on this device.
Use Device Pool Calling Party Transformation CSS	Check this check box to apply the Calling Party Transformation CSS configured at the device pool to which this device belongs to transform the remote calling and remote connected number.

Table 29: Protocol Specific Information

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: • **None**—This option, which serves as the default setting, indicates that no packet capturing is occurring. After you complete packet capturing, configure this setting. • **Batch Processing Mode**—Cisco Unified CM writes the decrypted or nonencrypted messages to a file, and the system encrypts each file. On a daily basis, the system creates a new file with a new encryption key. Cisco Unified CM, which stores the file for seven days, also stores the keys that encrypt the file in a secure location. Cisco Unified CM stores the file in the PktCap virtual directory. A single file contains the time stamp, source IP address, source IP port, destination IP address, packet protocol, message length, and the message. The TAC debugging tool uses HTTPS, administrator username and password, and the specified day to request a single encrypted file that contains the captured packets. Likewise, the tool requests the key information to decrypt the encrypted file.
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.
BLF Presence Group	From the drop-down list, choose a Busy Lamp Field (BLF) presence group for the end user. The selected group specifies the destinations that the end user can monitor The default value for BLF Presence Group specifies Standard Presence group, configured with installation. BLF Presence Groups that are configured in Cisco Unified Administration also appear in the drop-down list.
SIP Dial Rules	If required, choose the appropriate SIP dial rule. SIP dial rules provide local dial plans for Cisco Unified IP Phones 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, choose the codec to use if a media termination point is required for SIP calls.

Field	Description
Device Security Profile	Choose the security profile to apply to the device. You must apply a security profile to all devices that are configured in Unified Communications Manager Administration.
Rerouting Calling Search Space	From the drop-down list, 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.
SUBSCRIBE Calling Search Space	Supported with the Presence feature, the SUBSCRIBE calling search space determines how Unified Communications Manager routes presence requests that come from the end user. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the end user. From the drop-down list, 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. 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 can configure a calling search space as you do all calling search spaces.
SIP Profile	Choose the default SIP profile or a specific profile that was previously created. SIP profiles provide specific SIP information for the phone such as registration and keepalive timers, media ports, and do not disturb control.
Digest User	Choose an end user that you want to associate with the phone for this setting that is used with digest authentication (SIP security). Ensure that you configured digest credentials for the user that you choose, as specified in the End User Configuration window. After you save the phone configuration and apply the configuration update to the phone, the digest credentials for the user get added to the phone configuration file.

Field	Description
Media Termination Point Required	Use this field to indicate whether a media termination point is used to implement features that ATA 187 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 ATA 187 clients and those ATA 187 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.
Required DTMF Reception	For devices 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.

Table 30: Certification Authority Proxy Function (CAPF) Information

Field	Description
Certificate Operation	From the drop-down list, choose one of the following options: • No Pending Operation—Displays when no certificate operation is occurring (default setting). • Install/Upgrade—Installs a new or upgrades an existing locally significant certificate in the phone. • Delete—Deletes the locally significant certificate that exists in the phone. • Troubleshoot—Retrieves the locally significant certificate (LSC) or the manufacture installed certificate (MIC), so you can view the certificate credentials in the CAPF trace file. If both certificate types exist in the phone, Cisco Unified CM creates two trace files, one for each certificate type. By choosing the Troubleshooting option, you can verify that an LSC or MIC exists in the phone.

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, 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, this field applies. Manually enter a string or generate a string by clicking the **Generate String** button. Ensure that the string contains 4 to 10 digits. To install, upgrade, delete, or troubleshoot a locally significant certificate, the phone user or administrator must enter the authentication string on the phone.

Field	Description
Key Size (Bits)	For this setting that is used for CAPF, choose the key size for the certificate from the drop-down list. 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.

Table 31: Secure Shell User

Field	Description
Secure Shell User	Enter a user ID for the secure shell user. You can enter any alphanumeric or special characters up to 50 characters. Invalid characters include ",%, &, <, >, and \. This field displays when the phone device that you are configuring supports SSH access. Cisco Technical Assistance Center (TAC) uses secure shell for troubleshooting and debugging. Contact TAC for further assistance. See the *Security Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html for this release for information about how to configure encrypted phone configuration files to ensure that Cisco Unified CM does not send SSH credentials to the phone in the clear.
Secure Shell Password	Enter the password for a secure shell user. You can enter any alphanumeric or special characters up to 200 characters. Invalid characters include ",%, &, <, >, and \. Contact TAC for further assistance. See the *Security Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

Table 32: Product-Specific Configuration Layout

Field	Description
Model-specific configuration fields that the device manufacturer defines	To view field descriptions and help for product-specific configuration items, click the "?" information icon in the Product Specific Configuration area to display help in a popup dialog box. If you need more information, see the documentation for ATA 187.

Analog Telephony Adaptor 190 Configuration Fields

Table 33: Analog Telephony Adaptor 190 Configuration Fields

Field	Description
MAC Address	Enter the Media Access Control (MAC) address that identifies ATA 190. Make sure that the value comprises 12 hexadecimal characters. You can determine the MAC address for ATA 190 in any of these ways: • Look at the MAC label on the back of ATA 190. • Display the web page for ATA 190 and click the **Device Information** hyperlink.
Description	Enter a text description of the ATA 190. This field can contain up to 128 characters. You can use all characters except quotes ("), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).
Device Pool	Choose the device pool to which you want the ATA 190 assigned. The device pool defines sets of common characteristics for devices, such as region, date/time group, and softkey template. To see the Device Pool configuration settings, click the View Details link.
Common Device Configuration	Choose the Common Device Configuration to which you want the ATA 190 assigned. 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.
Common Phone Profile	From the drop-down list, choose a common phone profile from the list of available common phone profiles. To see the Common Phone Profile settings, click the View Details link.
Calling Search Space	From the drop-down list, choose the calling search space or leave the calling search space as the default of <None>.

Field	Description
AAR Calling Search Space	From the drop-down list, choose the appropriate calling search space for the device to use when it performs automated alternate routing (AAR) or leave the calling search space as the default of <None>.
Media Resource Group List	Choose the appropriate Media Resource Group List. A Media Resource Group List comprises a prioritized grouping of media resource groups. If you choose **<None>**, Cisco Unified CM uses the Media Resource Group List that is defined in the device pool.
User Hold MOH Audio Source	From the drop-down list, choose the audio source to use for music on hold (MOH) when a user initiates a hold action.
Location	From the drop-down list, choose the location that is associated with the phones and gateways in the device pool.
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. If no AAR group is specified, Cisco Unified CM uses the AAR group that is associated with Device Pool or Line.
User Locale	From the drop-down list, choose the user locale that is associated with the CTI Port. The user locale identifies a set of detailed information to support users, including language and font. If you do not specify a user locale, Cisco Unified CM uses the user locale that is associated with the device pool.
Network Locale	From the drop-down list, choose the network locale that is associated with the CTI Port. The network locale contains a definition of the tones and cadences that the phone in a specific geographic area uses. If you do not specify a network locale, Cisco Unified CM uses the network locale that is associated with the device pool.
Built in Bridge	Enable or disable the built-in conference bridge for the barge feature by using the Built In Bridge drop-down list. Choose one of the following: • On • Off • Default
Privacy	For Privacy, choose **On** in the Privacy drop-down list.
Device Mobility Mode	From the drop-down list, 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.
Owner	Select **User** or **Anonymous (Public/Shared Space)** , for the owner type.

Field	Description
Owner User ID	From the drop-down list, choose the user ID of the assigned phone user. The user ID gets recorded in the call detail record (CDR) for all calls made from this device. Assigning a user ID to the device also moves the device from "Unassigned Devices" to "Users" in the License Usage Report. **Note** Do not configure this field if you are using extension mobility. Extension mobility does not support device owners.
Phone Load Name	Enter the custom software for ATA 190.
Use Trusted Relay Point	Choose one of the following values: • **Off**—Choose this value to disable the use of a Trusted Relay Point (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. • **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.
Always Use Prime Line	From the drop-down list, choose one of the following options: • Off—When the phone is idle and receives a call on any line, the phone user answers the call from the line on which the call is received. • On—When the phone is idle (off hook) and receives a call on any line, the primary line gets chosen for the call. Calls on other lines continue to ring, and the phone user must select those other lines to answer these calls. • Default— Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter, which supports the Cisco CallManager service.
Always Use Prime Line for Voice Message	From the drop-down list, choose one of the following options: • Off—If the phone is idle, pressing the Messages button on the phone automatically dials the voice-messaging system from the line that has a voice message. Unified Communications Manager always selects the first line that has a voice message. If no line has a voice message, the primary line gets used when the phone user presses the Messages button. • 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 • Default— Unified Communications Manager uses the configuration from the Always Use Prime Line for Voice Message service parameter, which supports the Cisco CallManager service.

Field	Description
Geolocation	From the drop-down list, 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.
Ignore Presentation Indicators (internal calls only)	Check this check box to configure call display restrictions on a call-by-call basis. When this check box is checked, Unified 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.
Logged into Hunt Group	When the ATA 190 gets added to a hunt list, the administrator can log the user in or out by checking (and unchecking) this check box. Users use the softkey on the phone to log their phone in or out of the hunt list.
Remote Device	Check this box to allocate a buffer for the 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.
Protected Device	Check this check box to designate a phone as protected, which enables the phone to play a 2-second tone to notify the user when a call is encrypted and both phones are configured as protected devices. The tone plays for both parties when the call is answered. The tone does not play unless both phones are protected and the call occurs over encrypted media. Checking this check box represents only one of several configuration requirements for the secure indication tone to play. For a detailed description of the secure indication tone feature and the configuration requirements, see the *Security Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html. If you check this check box and the system determines that the call is not encrypted, the phone plays nonsecure indication tone to alert the user that the call is not protected.

Number Presentation Transformation

Table 34: Caller ID for Calls From This Phone

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.
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.

Table 35: Remote Number

Field	Description
Calling Party Transformation CSS	From the drop-down list, choose the calling search space (CSS) that contains the calling party transformation pattern that you want to apply on the remote calling number for calls received on this device.
Use Device Pool Calling Party Transformation CSS	Check this check box to apply the Calling Party Transformation CSS configured at the device pool to which this device belongs to transform the remote calling and remote connected number.

Table 36: Protocol Specific Information

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: • **None**—This option, which serves as the default setting, indicates that no packet capturing is occurring. After you complete packet capturing, configure this setting. • **Batch Processing Mode**—Cisco Unified CM writes the decrypted or nonencrypted messages to a file, and the system encrypts each file. On a daily basis, the system creates a new file with a new encryption key. Cisco Unified CM, which stores the file for seven days, also stores the keys that encrypt the file in a secure location. Cisco Unified CM stores the file in the PktCap virtual directory. A single file contains the time stamp, source IP address, source IP port, destination IP address, packet protocol, message length, and the message. The TAC debugging tool uses HTTPS, administrator username and password, and the specified day to request a single encrypted file that contains the captured packets. Likewise, the tool requests the key information to decrypt the encrypted file.

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.
BLF Presence Group	From the drop-down list, choose a Busy Lamp Field (BLF) presence group for the end user. The selected group specifies the destinations that the end user can monitor The default value for BLF Presence Group specifies Standard Presence group, configured with installation. BLF Presence Groups that are configured in Cisco Unified Administration also appear in the drop-down list.
SIP Dial Rules	If required, choose the appropriate SIP dial rule. SIP dial rules provide local dial plans for Cisco Unified IP Phones 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, choose the codec to use if a media termination point is required for SIP calls.
Device Security Profile	Choose the security profile to apply to the device. You must apply a security profile to all devices that are configured in Unified Communications Manager Administration.
Rerouting Calling Search Space	From the drop-down list, 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.

Field	Description
SUBSCRIBE Calling Search Space	Supported with the Presence feature, the SUBSCRIBE calling search space determines how Unified Communications Manager routes presence requests that come from the end user. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the end user. From the drop-down list, 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. 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 can configure a calling search space as you do all calling search spaces.
SIP Profile	Choose the default SIP profile or a specific profile that was previously created. SIP profiles provide specific SIP information for the phone such as registration and keepalive timers, media ports, and do not disturb control.
Digest User	Choose an end user that you want to associate with the phone for this setting that is used with digest authentication (SIP security). Ensure that you configured digest credentials for the user that you choose, as specified in the End User Configuration window. After you save the phone configuration and apply the configuration update to the phone, the digest credentials for the user get added to the phone configuration file. For more information on digest authentication, see the *Security Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html .
Media Termination Point Required	Use this field to indicate whether a media termination point is used to implement features that ATA 190 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 ATA 190 clients and those ATA 190 devices that do not support the H.245 empty capabilities set or if you want media streaming to terminate through a single source. If you check this check box to require an MTP and this device becomes the endpoint of a video call, the call will be audio only.
Unattended Port	Check this check box to indicate an unattended port on this device.

Field	Description
Required DTMF Reception	For devices 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.

Table 37: Certification Authority Proxy Function (CAPF) Information

Field	Description
Certificate Operation	From the drop-down list, choose one of the following options: • No Pending Operation—Displays when no certificate operation is occurring (default setting). • Install/Upgrade—Installs a new or upgrades an existing locally significant certificate in the phone. • Delete—Deletes the locally significant certificate that exists in the phone. • Troubleshoot—Retrieves the locally significant certificate (LSC) or the manufacture installed certificate (MIC), so you can view the certificate credentials in the CAPF trace file. If both certificate types exist in the phone, Cisco Unified CM creates two trace files, one for each certificate type. By choosing the Troubleshooting option, you can verify that an LSC or MIC exists in the phone. For more information on CAPF operations, see the *Security Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

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, 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, this field applies. Manually enter a string or generate a string by clicking the **Generate String** button. Ensure that the string contains 4 to 10 digits. To install, upgrade, delete, or troubleshoot a locally significant certificate, the phone user or administrator must enter the authentication string on the phone.

Field	Description
Key Size (Bits)	For this setting that is used for CAPF, choose the key size for the certificate from the drop-down list. 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.

Table 38: Secure Shell User

Field	Description
Secure Shell User	Enter a user ID for the secure shell user. You can enter any alphanumeric or special characters up to 50 characters. Invalid characters include ",%, &, <, >, and \. This field displays when the phone device that you are configuring supports SSH access. Cisco Technical Assistance Center (TAC) uses secure shell for troubleshooting and debugging. Contact TAC for further assistance. See the *Security Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html for this release for information about how to configure encrypted phone configuration files to ensure that Cisco Unified CM does not send SSH credentials to the phone in the clear.

Field	Description
Secure Shell Password	Enter the password for a secure shell user. You can enter any alphanumeric or special characters up to 127 characters. Invalid characters include ",%, &, <, >, and \. Contact TAC for further assistance. See the *Security Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html for this release for information about how to configure encrypted phone configuration files to ensure that Cisco Unified CM does not send SSH passwords to the phone in the clear.

Table 39: Product-Specific Configuration Layout

Field	Description
Model-specific configuration fields that the device manufacturer defines	To view field descriptions and help for product-specific configuration items, click the "?" information icon in the Product Specific Configuration area to display help in a popup dialog box. If you need more information, see the documentation for ATA 190.

Analog Telephony Adaptor 191 Configuration Fields

Table 40: Analog Telephony Adaptor 191 Configuration Fields

Field	Description
MAC Address	Enter the Media Access Control (MAC) address that identifies ATA 191. Make sure that the value comprises 12 hexadecimal characters. You can determine the MAC address for ATA 191 in any of these ways: • Look at the MAC label on the back of ATA 191. • Display the web page for ATA 191 and click the **Device Information** hyperlink.
Description	Enter a text description of the ATA 191. This field can contain up to 128 characters. You can use all characters except quotes ("), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).
Device Pool	Choose the device pool to which you want the ATA 191 assigned. The device pool defines sets of common characteristics for devices, such as region, date/time group, and softkey template. To see the Device Pool configuration settings, click the View Details link.

Field	Description
Common Device Configuration	Choose the Common Device Configuration to which you want the ATA 191 assigned. 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.
Common Phone Profile	From the drop-down list, choose a common phone profile from the list of available common phone profiles. To see the Common Phone Profile settings, click the View Details link.
Calling Search Space	From the drop-down list, choose the calling search space or leave the calling search space as the default of <None>.
AAR Calling Search Space	From the drop-down list, choose the appropriate calling search space for the device to use when it performs automated alternate routing (AAR) or leave the calling search space as the default of <None>.
Media Resource Group List	Choose the appropriate Media Resource Group List. A Media Resource Group List comprises a prioritized grouping of media resource groups. If you choose **<None>**, Cisco Unified CM uses the Media Resource Group List that is defined in the device pool.
User Hold MOH Audio Source	From the drop-down list, choose the audio source to use for music on hold (MOH) when a user initiates a hold action.
Location	From the drop-down list, choose the location that is associated with the phones and gateways in the device pool.
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. If no AAR group is specified, Cisco Unified CM uses the AAR group that is associated with Device Pool or Line.
User Locale	From the drop-down list, choose the user locale that is associated with the CTI Port. The user locale identifies a set of detailed information to support users, including language and font. If you do not specify a user locale, Cisco Unified CM uses the user locale that is associated with the device pool.
Network Locale	From the drop-down list, choose the network locale that is associated with the CTI Port. The network locale contains a definition of the tones and cadences that the phone in a specific geographic area uses. If you do not specify a network locale, Cisco Unified CM uses the network locale that is associated with the device pool.

Field	Description
Built in Bridge	Enable or disable the built-in conference bridge for the barge feature by using the Built In Bridge drop-down list. Choose one of the following: • On • Off • Default
Privacy	For Privacy, choose **On** in the Privacy drop-down list.
Device Mobility Mode	From the drop-down list, 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.
Owner	Select **User** or **Anonymous (Public/Shared Space)** , for the owner type.
Owner User ID	From the drop-down list, choose the user ID of the assigned phone user. The user ID gets recorded in the call detail record (CDR) for all calls made from this device. Assigning a user ID to the device also moves the device from “Unassigned Devices” to “Users” in the License Usage Report. **Note** Do not configure this field if you are using extension mobility. Extension mobility does not support device owners.
Phone Load Name	Enter the custom software for ATA 191.
Use Trusted Relay Point	Choose one of the following values: • **Off**—Choose this value to disable the use of a Trusted Relay Point (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. • **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.
Always Use Prime Line	From the drop-down list, choose one of the following options: • Off—When the phone is idle and receives a call on any line, the phone user answers the call from the line on which the call is received. • On—When the phone is idle (off hook) and receives a call on any line, the primary line gets chosen for the call. Calls on other lines continue to ring, and the phone user must select those other lines to answer these calls. • Default—Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter, which supports the Cisco CallManager service.

Field	Description
Always Use Prime Line for Voice Message	From the drop-down list, choose one of the following options: • 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. • 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 • 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.
Geolocation	From the drop-down list, 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.
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.
Logged into Hunt Group	When the ATA 191 gets added to a hunt list, the administrator can log the user in or out by checking (and unchecking) this check box. Users use the softkey on the phone to log their phone in or out of the hunt list.
Remote Device	Check this box to allocate a buffer for the 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.

Field	Description
Protected Device	Check this check box to designate a phone as protected, which enables the phone to play a 2-second tone to notify the user when a call is encrypted and both phones are configured as protected devices. The tone plays for both parties when the call is answered. The tone does not play unless both phones are protected and the call occurs over encrypted media. Checking this check box represents only one of several configuration requirements for the secure indication tone to play. For a detailed description of the secure indication tone feature and the configuration requirements, see the *Security Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html. If you check this check box and the system determines that the call is not encrypted, the phone plays nonsecure indication tone to alert the user that the call is not protected.

Number Presentation Transformation

Table 41: Caller ID for Calls From This Phone

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.
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.

Table 42: Remote Number

Field	Description
Calling Party Transformation CSS	From the drop-down list, choose the calling search space (CSS) that contains the calling party transformation pattern that you want to apply on the remote calling number for calls received on this device.
Use Device Pool Calling Party Transformation CSS	Check this check box to apply the Calling Party Transformation CSS configured at the device pool to which this device belongs to transform the remote calling and remote connected number.

Table 43: Protocol Specific Information

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: • **None**—This option, which serves as the default setting, indicates that no packet capturing is occurring. After you complete packet capturing, configure this setting. • **Batch Processing Mode**—Cisco Unified CM writes the decrypted or nonencrypted messages to a file, and the system encrypts each file. On a daily basis, the system creates a new file with a new encryption key. Cisco Unified CM, which stores the file for seven days, also stores the keys that encrypt the file in a secure location. Cisco Unified CM stores the file in the PktCap virtual directory. A single file contains the time stamp, source IP address, source IP port, destination IP address, packet protocol, message length, and the message. The TAC debugging tool uses HTTPS, administrator username and password, and the specified day to request a single encrypted file that contains the captured packets. Likewise, the tool requests the key information to decrypt the encrypted file.
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.
BLF Presence Group	From the drop-down list, choose a Busy Lamp Field (BLF) presence group for the end user. The selected group specifies the destinations that the end user can monitor The default value for BLF Presence Group specifies Standard Presence group, configured with installation. BLF Presence Groups that are configured in Cisco Unified Administration also appear in the drop-down list.
SIP Dial Rules	If required, choose the appropriate SIP dial rule. SIP dial rules provide local dial plans for Cisco Unified IP Phones 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, choose the codec to use if a media termination point is required for SIP calls.

Field	Description
Device Security Profile	Choose the security profile to apply to the device. You must apply a security profile to all devices that are configured in Unified Communications Manager Administration.
Rerouting Calling Search Space	From the drop-down list, 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.
SUBSCRIBE Calling Search Space	Supported with the Presence feature, the SUBSCRIBE calling search space determines how Unified Communications Manager routes presence requests that come from the end user. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the end user. From the drop-down list, 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. 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 can configure a calling search space as you do all calling search spaces.
SIP Profile	Choose the default SIP profile or a specific profile that was previously created. SIP profiles provide specific SIP information for the phone such as registration and keepalive timers, media ports, and do not disturb control.
Digest User	Choose an end user that you want to associate with the phone for this setting that is used with digest authentication (SIP security). Ensure that you configured digest credentials for the user that you choose, as specified in the End User Configuration window. After you save the phone configuration and apply the configuration update to the phone, the digest credentials for the user get added to the phone configuration file. For more information on digest authentication, see the *Security Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html .

Field	Description
Media Termination Point Required	Use this field to indicate whether a media termination point is used to implement features that ATA 191 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 ATA 191 clients and those ATA 191 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.
Required DTMF Reception	For devices 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.

Table 44: Certification Authority Proxy Function (CAPF) Information

Field	Description
Certificate Operation	From the drop-down list, choose one of the following options: • No Pending Operation—Displays when no certificate operation is occurring (default setting). • Install/Upgrade—Installs a new or upgrades an existing locally significant certificate in the phone. • Delete—Deletes the locally significant certificate that exists in the phone. • Troubleshoot—Retrieves the locally significant certificate (LSC) or the manufacture installed certificate (MIC), so you can view the certificate credentials in the CAPF trace file. If both certificate types exist in the phone, Cisco Unified CM creates two trace files, one for each certificate type. By choosing the Troubleshooting option, you can verify that an LSC or MIC exists in the phone. For more information on CAPF operations, see the *Security Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

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, 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, this field applies. Manually enter a string or generate a string by clicking the **Generate String** button. Ensure that the string contains 4 to 10 digits. To install, upgrade, delete, or troubleshoot a locally significant certificate, the phone user or administrator must enter the authentication string on the phone.

Field	Description
Key Size (Bits)	For this setting that is used for CAPF, choose the key size for the certificate from the drop-down list. 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.

Table 45: Secure Shell User

Field	Description
Secure Shell User	Enter a user ID for the secure shell user. You can enter any alphanumeric or special characters up to 50 characters. Invalid characters include ",%, &, <, >, and \. This field displays when the phone device that you are configuring supports SSH access. Cisco Technical Assistance Center (TAC) uses secure shell for troubleshooting and debugging. Contact TAC for further assistance. See the *Security Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html for this release for information about how to configure encrypted phone configuration files to ensure that Cisco Unified CM does not send SSH credentials to the phone in the clear.

Field	Description
Secure Shell Password	Enter the password for a secure shell user. You can enter any alphanumeric or special characters up to 127 characters. Invalid characters include ",%, &, <, >, and \. Contact TAC for further assistance. See the *Security Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html for this release for information about how to configure encrypted phone configuration files to ensure that Cisco Unified CM does not send SSH passwords to the phone in the clear.

Table 46: Product-Specific Configuration Layout

Field	Description
Model-specific configuration fields that the device manufacturer defines	To view field descriptions and help for product-specific configuration items, click the "?" information icon in the Product Specific Configuration area to display help in a popup dialog box. If you need more information, see the documentation for ATA 191.

CHAPTER 42

Configure Software-Based Endpoints

Software-Based Endpoint Configuration

Complete the tasks in this chapter to configure software-based endpoints such as CTI ports, H.323 clients, and Cisco IP Communicator.

Configure CTI Ports

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.
The **Find and List Phones** window appears.

Step 2 Click **Add New**.

Step 3 From the **Phone Type** drop down list, select CTI Port and click **Next**.
The **Phone Configuration** window appears.

Step 4 Configure the fields in the **Phone Configuration** window. See the Related Topics section for more information about the fields and their configuration options.

Step 5 Click **Save**.

CTI Port Settings

Table 47: CTI Port Settings

Field	Description
Device Name	Specifies the name for the CTI Port that is automatically populated based on the Owner User ID. The format of the device name is *CTIRD<OwnerUserID>* by default. This field is editable. The device name can comprise up to 15 characters. Valid characters include letters, numbers, dashes, dots (periods), spaces, and underscores.
Description	Enter a text description of the CTI Port. This field can contain up to 128 characters. You can use all characters except quotes ("), close angle bracket (>), open angle bracket (<), backslash (\\), ampersand (&), and percent sign (%).
Device Pool	Choose the device pool to which you want the CTI Port assigned. The device pool defines sets of common characteristics for devices, such as region, date/time group, and softkey template. To see the Device Pool configuration settings, click the View Details link.
Common Device Configuration	Choose the Common Device Configuration to which you want the CTI Port assigned. To see the Common Device Configuration settings, click the View Details link.
Common Phone Profile	From the drop-down list box, choose a common phone profile from the list of available common phone profiles. To see the Common Phone Profile settings, click the View Details link.
Calling Search Space	From the drop-down list, choose the calling search space or leave the calling search space as the default of <None>.
AAR Calling Search Space	From the drop-down list, choose the appropriate calling search space for the device to use when it performs automated alternate routing (AAR) or leave the calling search space as the default of <None>.

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. If you choose **<None>**, Cisco Unified CM uses the Media Resource Group List that is defined in the device pool.
User Hold MOH Audio Source	From the drop-down list, choose the audio source to use for music on hold (MOH) when a user initiates a hold action.
Network Hold MOH Audio Source	From the drop-down list, choose the audio source to use for MOH when the network initiates a hold action.
Location	From the drop-down list, choose the location that is associated with the phones and gateways in the device pool.
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. If no AAR group is specified, Cisco Unified CM uses the AAR group that is associated with Device Pool or Line.
User Locale	From the drop-down list box, choose the user locale that is associated with the CTI Port. The user locale identifies a set of detailed information to support users, including language and font. If no user locale is specified, Cisco Unified CM uses the user locale that is associated with the device pool.
Network Locale	From the drop-down list box, choose the network locale that is associated with the CTI Port. The network locale contains a definition of the tones and cadences that the phone in a specific geographic area uses. If no network locale is specified, Cisco Unified CM uses the user locale that is associated with the device pool.
Privacy	For Privacy, choose **On** in the Privacy drop-down list box.
Owner	Select **User** or **Anonymous** (Public/Shared Space, for the owner type.

Field	Description
Owner User ID	From the drop-down list box, choose the user ID of the assigned CTI Port user. The user ID gets recorded in the call detail record (CDR) for all calls made from this device. Assigning a user ID to the device also moves the device from “Unassigned Devices” to “Users” in the License Usage Report.
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.
Use Trusted Relay Point	Choose one of the following values: • Off—Choose this value to disable the use of a Trusted Relay Point (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. • 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.
Always Use Prime Line	From the drop-down list box, choose one of the following options: • Off—When the phone is idle and receives a call on any line, the phone user answers the call from the line on which the call is received. • On—When the phone is idle (off hook) and receives a call on any line, the primary line gets chosen for the call. Calls on other lines continue to ring, and the phone user must select those other lines to answer these calls. • Default—Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter, which supports the Cisco CallManager service.

Field	Description
Always Use Prime Line for Voice Message	From the drop-down list box, choose one of the following options: • 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. • 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 • 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.
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.
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.
Logged into Hunt Group	When the CTI port 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.

Field	Description
Remote Device	Check this box to allocate a buffer for the 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.

Number Presentation Transformation

Table 48: Caller ID for Calls From This Phone

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.
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.

Table 49: Remote Number

Field	Description
Calling Party Transformation CSS	From the drop-down list box, choose the calling search space (CSS) that contains the calling party transformation pattern that you want to apply on the remote calling number for calls received on this device.
Use Device Pool Calling Party Transformation CSS	Check this check box to apply the Calling Party Transformation CSS configured at the device pool to which this device belongs to transform the remote calling and remote connected number.

Table 50: Protocol Specific Information

Field	Description
BLF Presence Group	From the drop-down list box, choose a Busy Lamp Field (BLF) presence group for the end user. The selected group specifies the destinations that the end user can monitor The default value for BLF Presence Group specifies Standard Presence group, configured with installation. BLF Presence Groups that are configured in Cisco Unified Administration also appear in the drop-down list box.
Device Security Profile	Choose the security profile to apply to the device. You must apply a security profile to all devices that are configured in Cisco Unified Communications Manager Administration.
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, 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. 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 can configure a calling search space as you do all calling search spaces.
Unattended Port	Check this check box to indicate an unattended port on this device.

Table 51: MLPP and Confidential Access Level Information

Field	Description
MLPP Domain	From the drop-down list, choose an Multilevel Precedence and Preemption (MLPP) domain to associate with this device. If you leave this field blank, this device inherits its MLPP domain from the value that is set for the device pool. If the device pool does not have an MLPP Domain setting, this device inherits its MLPP Domain from the value that is set for the MLPP Domain Identifier enterprise parameter. The default value for MLPP Domain specifies None.
Confidential Access Mode	From the drop-down list box, select one of the following options to set the Confidential Access Level mode: • Fixed—Confidential Access Level value has higher precedence over call completion. • Variable—Call completion has higher precedence over CAL level.
Confidential Access Level	Select the appropriate Confidential Access Level value from the drop-down list box.

Table 52: Do Not Disturb Information

Field	Description
Do Not Disturb	Check this check box to enable Do Not Disturb on the remote device.
DND Option	When you enable DND, Call Reject option specifies that no incoming call information gets presented to the user. Depending on how you configure the DND Incoming Call Alert parameter, the device may play a beep or display a flash notification of the call.

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 the device. 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 device to play a beep tone only. • Flash Only—For an incoming call, this option causes the device to display a flash alert.

Configure an H.323 Client

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.
The **Find and List Phones** window appears.

Step 2 Click **Add New**.

Step 3 From the **Phone Type** drop down list, select H.323 Client and click **Next**.
The **Phone Configuration** window appears.

Step 4 Configure the fields in the **Phone Configuration** window. See the Related Topics section for more information about the fields and their configuration options.

Step 5 Click **Save**.

H.323 Client Settings

Configure Cisco IP Communicator

Cisco IP Communicator is a software-based application that allows users to place and receive phone calls by using their personal computers. It provides the same functionality as a full-featured Cisco Unified IP Phone. Cisco IP Communicator depends upon the Cisco Unified Communications Manager call-processing system to provide telephony features and voice-over-IP capabilities. You administer Cisco IP Communicator as a phone device by using the Cisco Unified Communications Manager Administration Phone Configuration window.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.
The **Find and List Phones** window appears.

Step 2 Click **Add New**.

Step 3 From the **Phone Type** drop down list, select **Cisco IP Communicator** and click **Next**.

Step 4 From the **Select the device protocol** drop-down list, select either **SCCP** or **SIP** and click **Next**.
The **Phone Configuration** window appears.

Step 5 Configure the following mandatory fields in the **Phone Configuration** window.

- **Device Name**—enter a name to identify the Cisco IP Communicator device.
- **Device Pool**——choose the device pool to which you want this phone assigned. The device pool defines sets of common characteristics for devices, such as region, date/time group, and softkey template.
- **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.
- **Owner User ID**—from the drop-down list box, choose the user ID of the assigned phone user.
- **Device Security Profile**——choose the security profile to apply to the device.

You can use default configuration for the remaining fields. See the online help for more information about the fields and their configuration options.

Step 6 Click **Save**.

Step 7 In the **Association** area, click **Line [1] - Add a new DN**.

Step 8 In the **Directory Number** field, enter the directory number that you want to associate with the phone.

Step 9 Click **Save**.

CHAPTER 43

Configure Cisco IP Phones

Cisco IP Phones Overview

Cisco IP Phones are full-featured telephones that provide voice communication over an IP network. To provide this capability, the IP phones interact with several other key Cisco Unified IP Telephony and network components, such as Unified Communications Manager, DNS and DHCP servers, TFTP servers, media resources, Cisco Power over Ethernet (PoE), and others. These IP phones function much like digital business phones that allow you to place and receive phone calls and to access features such as mute, hold, transfer, speed dial, call forward, and more. In addition, because Cisco IP Phones connect to your data network, they offer enhanced IP telephony features, such as access to network information and services and customizable features and services. The phones also support security features that include file authentication, device authentication, signaling encryption, and media encryption.

This chapter describes how to configure a phone to make it operational on your system. To configure features such as Call Park, Call Forward, Busy Lamp Field (BLF), Call Pickup, and Speed Dial, see the *Feature Configuration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html

Cisco IP Phones Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure Phones, on page 347	Perform this task to configure a SIP or an SCCP Phone.
Step 2	Configure EnergyWise, on page 351	To reduce power consumption, configure the phone to power down (sleep) and power up (wake) automatically.

	Command or Action	Purpose
Step 3	Configure a Client Services Framework Device, on page 353	Perform this procedure to configure a Client Services Framework device. A Client Services Framework device can be any of the following: • Cisco Unified Communications Integration for Microsoft Office Communicator • Cisco Unified Communications Integration for Webex Connect • Cisco Unified Personal Communicator (Release 8.0 and later)
Step 4	Configure a CTI Remote Device, on page 355	Perform this procedure to configure a CTI Remote Device. A CTI remote device is a device type that represents off-cluster phones that users can use with Cisco UC applications. The device type is configured with one or more lines (directory numbers) and one or more remote destinations.
Step 5	Configure a Cisco Spark Remote Device, on page 361	Perform this procedure to configure a Cisco Webex remote device. A Cisco Webex remote device represents a Cisco Webex client that users can use with Cisco UC applications. The device type supports multiple active calls to the configured remote destination. A Cisco Spark remote device requires an enhanced license, except in the following scenario: • When the Owner User ID for the Cisco Spark remote device is also assigned an IP Phone or Jabber client, a single enhanced license is used for both devices. • When the Owner User ID for the Cisco Spark remote device is also assigned a TelePresence device, a single TelePresence license is used for both devices. **Caution** The Cisco Spark remote device is supported only for connecting your on-premises environment to Cisco cloud services. Use of this remote device for any other purpose is not supported.
Step 6	Migrate Phone Data, on page 365	Perform this procedure if you are migrating from one phone to another and you do not need to use the old phone anymore.

Configure Phones

Procedure

	Command or Action	Purpose
Step 1	To configure SIP phones, perform the following procedures: • Configure SIP Phone Secure Port, on page 348 • Restart Services, on page 348 • Configure SIP Profile, on page 348 • Configure Phone Security Profile, on page 385 • Configure a Phone, on page 350 • Configure Cisco IP Phone Services, on page 351 • Configure a VPN client.	Perform these procedures if you have phones that use Session Initiation Protocol (SIP). SIP provides the primary interface between the phone and other network components. In addition to SIP, other protocols are used for various functions such as DHCP for IP address assignment, DNS for domain name to address resolution, and TFTP for downloading image and configuration data. For detailed steps about configuring a VPN client, see the *Feature Configuration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.
Step 2	To configure SCCP Phones, perform the following procedures: • Configure Phone Security Profile, on page 385 • Configure a Phone, on page 350 • Configure Cisco IP Phone Services, on page 351 • Configure a VPN client	Perform these procedures if you want to configure Cisco IP Phones that use the Skinny Client Control Protocol (SCCP). SCCP uses Cisco-proprietary messages to communicate between IP devices and Cisco Unified Communications Manager. SCCP easily coexists in a multiple protocol environment. During registration, a Cisco Unified IP Phone receives its line and all other configurations from Cisco Unified Communications Manager. For detailed steps about configuring a VPN client, see the *Feature Configuration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

What to do next

Provide power, verify network connectivity, and configure network settings for the Cisco Unified IP Phone. For more information about configuring network settings, see the *Cisco Unified IP Phone Administration Guide* for your Cisco Unified IP Phone model.

Configure SIP Phone Secure Port

Follow these steps to configure the SIP Phone Secure Port. Cisco Unified Communications Manager uses this port to listen to SIP phones for SIP line registrations over TLS.

Procedure

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

Step 2 In the **Cisco Unified Communications Manager TCP Port Settings for this Server** section, specify a port number in the **SIP Phone Secure Port** field, or leave the field set to default. The default value is 5061.

Step 3 Click **Save**.

Step 4 Click **Apply Config**.

Step 5 Click **Ok**.

Restart Services

Follow these steps to restart Cisco CallManager and Cisco CTL Provider services.

Procedure

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

Step 2 Choose the Cisco Unified Communications Manager server from the **Servers** drop-down list.
In the CM Services area, Cisco CallManager displays in the **Service Name** column.

Step 3 Click the radio button that corresponds to the Cisco CallManager service.

Step 4 Click **Restart**.
The service restarts and displays the message, `Service Successfully Restarted`.

Step 5 Repeat step 3 and step 4 to restart Cisco CTL Provider service.

Configure SIP Profile

Use this procedure to configure SIP profile with SIP settings for your AS-SIP endpoints and for your SIP trunks.

Before you begin

- Configure SIP Phone Secure Port, on page 348
- Restart Services, on page 348

Procedure

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

Step 2 Click **Find**.

Step 3 For the profile that you want to copy, click the file icon in the **Copy** column.

Step 4 Enter the name and description of the new profile.

Step 5 If you have the IPv6 stack configured and you are deploying two stacks, check the **Enable ANAT** check box.

Note This configuration applies whether you have Unity Connection deployed or not.

Step 6 Click **Save**.

What to do next

Configure Phone Security Profile, on page 385

Configure Phone Security Profile

If you want to enable security features like TLS signaling, CAPF, and digest authentication requirements for the endpoints, you must configure a new security profile that you can apply it to the endpoints.

Note By default, if you don't apply a SIP phone security profile to a provisioned device, the device uses a nonsecure profile.

Procedure

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

Step 2 Click **Add New**.

Step 3 From the **Phone Security Profile Type** drop-down list, choose the Universal Device Template to create a profile that you can use when provisioning through the device templates.

Note Optionally, you can also create security profiles for specific device models.

Step 4 Select the protocol.

Step 5 Enter an appropriate name for the profile in the **Name** field.

Step 6 If you want to use TLS signaling to connect to the device, set the **Device Security Mode** to **Authenticated** or **Encrypted** and the Transport Type to **TLS**.

Step 7 (Optional) Check the **Enable OAuth Authentication** check box if you want the phone to use digest authentication.

Step 8 (Optional) Check the **TFTP Encrypted Config** check box if you want to use encrypted TFTP.

Step 9 Complete the remaining fields in the Phone Security Profile Configuration window. For help with the fields and their settings, see the online help.

Step 10 Click **Save**.

Configure a Phone

Perform these steps to manually add the phone to the Cisco Unified Communications Manager database. You do not have to perform these steps if you are using autoregistration. If you opt for autoregistration, Cisco Unified Communications Manager automatically adds the phone and assigns the directory number. For more information about enabling autoregistration, see Configure Autoregistration Task Flow, on page 549.

Before you begin

- Configure Phone NTP References, on page 51
- Configure Phone Security Profile, on page 385
- Add a Date/Time Group, on page 52
- Set Up SIP Dial Rule, on page 169 (when configuring a SIP phone)

Procedure

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

Step 2 Click **Add New**.

Step 3 From the **Phone Type** drop-down list, select the appropriate Cisco IP Phone model.

Step 4 Click **Next**.

Step 5 From the **Select the device protocol** drop-down list, choose one of the following:

- **SCCP**
- **SIP**

Step 6 Click **Next**.

Step 7 Configure the fields in the **Phone Configuration** window. See the online help for more information about the fields and their configuration options.

Note The CAPF settings that are configured in the security profile relate to the Certificate Authority Proxy Function settings that display in the Phone Configuration window. You must configure CAPF settings for certificate operations that involve manufacturer-installed certificates (MICs) or locally significant certificates (LSC). See the Cisco Unified Communications Manager Security Guide for more information about how CAPF settings that you update in the phone configuration window affect security profile CAPF settings.

Step 8 Click **Save**.

Step 9 In the **Association** area, click **Line [1] - Add a new DN**.

Step 10 In the **Directory Number** field, enter the directory number that you want to associate with the phone.

Step 11 Click **Save**.

What to do next

For SIP or SCCP phones:

Configure Cisco IP Phone Services, on page 351

Configure Cisco IP Phone Services

Configure services for Cisco IP Phones if you want to provide phone services such as a company directory, visual voicemail, or weather forecasts to the Cisco IP Phones. Cisco provides certain default IP phone services, which install automatically with Cisco Unified Communications Manager. You can also create customized Cisco IP Phone services for your site. Follow these steps to configure the customized services in Unified Communications Manager.

Before you begin

Configure a Phone, on page 350

Procedure

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

Step 2 Click **Add New**.

Step 3 Configure the fields in the **IP Phone Services Configuration** window. See the online help for more information about the fields and their configuration options.

Step 4 Click **Save**.

What to do next

- Add services to the phones in the database if they are not classified as enterprise subscriptions. You can add services to the phones using Bulk Administration Tool (BAT) or Cisco Unified Communications Self Care Portal. For more information, see *Cisco Unified Communications Manager Bulk Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html and *Cisco Unified Communications Self Care Portal User Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-user-guide-list.html.

- You can assign the services to the phone buttons, if the phone model supports these buttons. For more information about assigning services, see Cisco IP Phone User Guide for your phone model.

- Configure VPN Client (optional).

Configure EnergyWise

Before you begin

- Ensure that your system includes an EnergyWise controller. For example, a Cisco Switch with the EnergyWise feature enabled.

- See the user documentation for your phone model to check whether your phone model supports the EnergyWise feature.

Procedure

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

Step 2 Specify the search criteria and click **Find**.
A list of phones that are configured on the Cisco Unified Communications Manager is displayed.

Step 3 Choose the phone for which you want to configure the EnergyWise feature.

Step 4 Configure the EnergyWise fields in the **Product Specific Configuration Layout** section. See the Related Topics section for more information about the fields and their configuration options.

Step 5 Click **Save**.

EnergyWise Configuration Fields

Table 53: EnergyWise Configuration Fields

Field	Description
Enable Power Save Plus	Select the day for which you want the phone to automatically power off. You can select multiple days by pressing and holding the Control key while clicking on the days for the schedule. By default, no days are selected.
Phone On Time	Enter the time in 24 hour format, where 00:00 is midnight. This value determines when the phone automatically powers on for the days selected in the **Enable Power Save Plus** field. **Note** To wake up the phone before the **Phone On Time**, you must power on the phone from the switch. For more information, see the switch documentation.
Phone Off Time	Enter the time in 24 hour format, where 00:00 is midnight. This value determines when the phone automatically powers down for the days selected in the **Enable Power Save Plus** field. If the **Phone On Time** and the **Phone Off Time** fields contain the same value, the phone does not power down.
Phone Off Idle Timeout	Specify the duration for which the phone must be idle before the phone powers down. You can specify any value from 20 minutes to 1440 minutes. The default value is 60 minutes.

Field	Description
Enable Audible Alert	Check this check box to instruct the phone to play an audible alert 10 minutes, 7 minutes, 4 minutes, and 30 seconds before the time specified in the **Phone Off Time** field. This check box applies only if the **Enable Power Save Plus** list box has one or more days selected.
EnergyWise Domain	Specify the EnergyWise domain that the phone is in. The maximum length allowed is 127 characters.
EnergyWise Secret	Specify the security secret password that is used to communicate with the endpoints in the EnergyWise domain. The maximum length allowed is 127 characters
Allow EnergyWise Overrides	Check this check box to disable Power Save Plus. If you check this check box, the EnergyWise domain controller policy overrides the **Power On Time** and **Power Off Time** values. **Note** Leaving the **Allow EnergyWise Overrides** check box checked with no days selected in the Enable Power Save Plus field does not disable Power Save Plus.

Configure a Client Services Framework Device

Perform this procedure to configure a Client Services Framework device. A Client Services Framework device can be any of the following:

- Cisco Unified Communications Integration for Microsoft Office Communicator
- Cisco Unified Communications Integration for Webex Connect
- Cisco Unified Personal Communicator (Release 8.0 and later)

Procedure

	Command or Action	Purpose
Step 1	Add a Client Services Framework Device, on page 354	Add a device that uses the Client Services Framework.
Step 2	Associate Device with End User, on page 355	Associate an end user account to the Client Services Framework device.

Add a Client Services Framework Device

Procedure

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

Step 2 Click **Add New**.

Step 3 From the **Phone Type** drop-down list, choose **Cisco Unified Client Services Framework**.

Step 4 Click **Next**.

Step 5 Configure the fields in the **Phone Configuration** window. See the Related Topics section for more information about the fields and their configuration options.

Step 6 Click **Save**.

Step 7 In the **Association** area, click **Line [1] - Add a new DN**.

Step 8 In the **Directory Number** field, enter the directory number that you want to associate with the client services framework device.

Step 9 Click **Save**.

Client Services Framework Device Configuration Fields

Table 54: Client Services Framework Device Configuration Fields

Field	Description
Device Name	Enter a name to identify the Client Services Framework device. The name can include up to 15 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). **Note** When you configure the device name for the Cisco Unified Personal Communicator, make sure that the name starts with UPC.
Description	Enter a brief description for the device. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
Device Pool	Choose the device pool to which you want this device assigned.
Phone Button Template	Choose **Standard Client Services Framework**.
Owner User ID	Choose the user ID of the assigned Client Services Framework device user. The user ID is recorded in the call detail record (CDR) for all calls made from this device.

Field	Description
Device Security Profile	Choose **Cisco Unified Client Services Framework - Standard SIP Non-secure Profile**.
SIP Profile	Choose **Standard SIP Profile**.

Associate Device with End User

Use this procedure to associate an end user with the Client Services Framework Device.

Procedure

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

Step 2 Click **Find** and select the user whom you want to associate to the device.

Step 3 In the **Device Information** section, click **Device Association** .
The User Device Association window appears.

Step 4 Click **Find** to view a list of available devices.

Step 5 Select the device that you want to associate, and click **Save Selected/Changes**.

Step 6 From **Related Links**, choose **Back to User**, and click **Go**.
The **End User Configuration** window appears, and the associated device that you chose appears in the **Controlled Devices** pane.

Configure CTI Remote Device

Procedure

	Command or Action	Purpose
Step 1	Configure a CTI Remote Device, on page 355	Create a CTI Remote Device.
Step 2	Add a Directory Number to a Device, on page 359	To register a CTI Remote Device, you must add a Directory Number to that device.
Step 3	Configure a Remote Destination, on page 359	Configure the remote destinations that you want to associate with the CTI remote device.

Configure a CTI Remote Device

Procedure

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

Step 2 Click **Add New**.

Step 3 From the **Phone Type** drop down list, select CTI Remote Device and click **Next**.

Step 4 Configure the fields in the **Phone Configuration** window. See the Related Topics section for more information about the fields and their configuration options.

Step 5 Click **Save**.

CTI Remote Device Configuration Fields

CTI Remote Device Information

Table 55: Device Information

Field	Description
Registration	Specifies the registration status of the CTI Remote Device.
Device Status	Specifies if the device is active or inactive.
Device Trust	Specifies if the device is trusted.
Active Remote Destination	Specifies if the remote destination which is active. The CTI client can specify one remote destination as 'active' at any one given time. Incoming calls and Dial via Office (DVO) calls are routed to the active remote destination.
Owner User ID	From the drop-down list, 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.
Device Name	Specifies the name for the CTI Remote Device that is automatically populated based on the Owner User ID. The format of the device name is *CTIRD<OwnerUserID>* by default. This field is editable. The device name can comprise up to 15 characters. Valid characters include letters, numbers, dashes, dots (periods), spaces, and underscores.
Description	Enter a text description of the CTI remote device. This field can contain up to 128 characters. You can use all characters except quotes (“), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).

Field	Description
Device Pool	Select the device pool which defines the common characteristics for CTI remote devices. For more information on how to configure the device pool, see Device Pool Configuration Settings.
Calling Search Space	From the drop-down list, choose the calling search space or leave the calling search space as the default of <None>.
User Hold MOH Audio Source	From the drop-down list, choose the audio source to use for music on hold (MOH) when a user initiates a hold action.
Network Hold MOH Audio Source	From the drop-down list, choose the audio source to use for MOH when the network initiates a hold action.
Location	From the drop-down list, choose the location that is associated with the phones and gateways in the device pool.
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.
Ignore Presentation Indicators (internal calls only)	Check this check box to configure call display restrictions on a call-by-call basis. When this check box is checked, Cisco Unified CM ignores any presentation restriction that is received for internal calls.

Call Routing Information

Table 56: Inbound/Outbound Calls Information

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.
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.

Table 57: Protocol Specific Information

Field	Description
Presence Group	Configure this field with the Presence feature. If you are not using this application user with presence, leave the default (None) setting for presence group. From the drop-down list, choose a Presence group for the application user. The group selected specifies the destinations that the application user, such as IPMASysUser, can monitor.
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, 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. 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 can configure a calling search space as you do all calling search spaces.
Rerouting Calling Search Space	From the drop-down list, choose a calling search space to use for rerouting. The rerouting calling search space of the referrer is used to find the route to the refer-to target. When the Refer message 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.

Table 58: Do Not Disturb Information

Field	Description
Do Not Disturb	Check this check box to enable Do Not Disturb on the remote device.
DND Option	When you enable DND on the phone, Call Reject 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.

Add a Directory Number to a Device

To register a CTI Remote Device, you must add a Directory Number to that device. You cannot register a CTI Remote Device without a Directory Number. You can add a maximum of five Directory Numbers to the CTI Remote Device.

Procedure

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

Step 2 Specify the filter criteria and click on the CTI Remote Device for which you want to associate the directory number.

Step 3 In the **Association** pane, click **Add a new DN** link.

Step 4 Configure the fields in the **Directory Number Configuration** window. See the online help for more information about the fields and their configuration options.

Step 5 Click **Save**.

Configure a Remote Destination

You can configure one or more remote destinations for a CTI Remote Device. A remote destination is a mobile or other phone that you can configure to perform remote destination pickup (accept transfers from the desk phone of the user) and accept incoming Cisco Unified Mobility calls. The remote destination that is associated with the CTI Remote Device specifies the phone number to reach the remote device. The maximum number of remote destinations that you can configure for a CTI Remote Device is dependent on the Remote Destination limit set for the Owner User ID.

Remote destinations can include any of the following devices:

- Single-mode mobile (cellular) phones
- Smartphones
- Dual-mode phones
- Enterprise IP phones that are not in the same cluster as the desk phone
- Home phone numbers in the PSTN

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone** > **CTI Remote Device** > **Associated Remote Destinations**.

Step 2 Specify the filter criteria and click on the CTI Remote Device for which you want to configure the remote destination.

Step 3 In the **Associated Remote Destinations** pane, select **Add a New Remote Destination**.

Alternatively, you can also use the **Device** > **Phone** > **Add New** menu path to configure a remote destination.

Step 4 Configure the fields in the **Remote Destination Configuration** window. See the Related Topics section for more information about the fields and their configuration options.

Step 5 Click **Save**.

Remote Destination Configuration Fields

Table 59: Remote Destination Configuration Fields

Field	Description
Name	Enter the name of the remote destination.
Destination Number	Enter the number that you would dial from within the enterprise. Include the area code and any additional digits that are required to reach an outside line. The maximum field length is 24 characters; individual characters can take the values 0-9, *, #, and +. Cisco recommends that you configure the caller ID of the remote destination.
Owner User ID	From the drop-down list, choose the owner of the remote destination.
Enable Unified Mobility features	Check the check box to enable Unified Mobility features.
Remote Destination Profile	From drop-down list, choose the profile that you configured.
Enable Single Number Reach	Check the check box to enable Single-Number_Reach for the remote destination.
Enable Move to Mobile	This is an optional field. If your phone is a mobile phone, check this check box.

Configure a Cisco Spark Remote Device

Procedure

	Command or Action	Purpose
Step 1	Configure a Cisco Spark Remote Device, on page 361	Create a Cisco Spark remote device.
Step 2	Add a Directory Number to a Cisco Spark Device, on page 365	To register a Cisco Spark remote device, you must add a Directory Number to that device.

Configure a Cisco Spark Remote Device

Procedure

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

Step 2 Click **Add New**.

Step 3 From the **Phone Type** drop down list, select Cisco Spark Remote Device and click **Next**.

Step 4 Configure the fields in the **Phone Configuration** window. See the Related Topics section for more information about the fields and their configuration options.

Step 5 Click **Save**.

Cisco Spark Remote Device Configuration Fields

Table 60: Webex Remote Device Configuration Fields

Field	Description
Device Information	
Registration	Specifies the registration status of the Webex remote device.
Device Status	Specifies if the device is active or inactive.
Device Trust	Specifies whether the device is trusted or not trusted.
Active Remote Destination	Specifies if the remote destination is active. The Webex client has only one active remote destination by default. All incoming calls are routed to the active remote destination. This field is to none even though it is associated to an active remote destination.
Owner User ID	From the drop-down list, 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.

Field	Description
Device Name	Specifies the name for the Webex remote device that is automatically populated based on the Owner User ID. The format of the device name is *SparkRD<OwnerUserID>* by default. The default device name *SparkRD* must not be changed. This field is editable. The device name can comprise up to 15 characters. Valid characters include letters, numbers, dashes, dots (periods), spaces, and underscores.
Description	Enter a text description of the Webex remote device. This field can contain up to 128 characters. You can use all characters except quotes ("), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).
Device Pool	Select the device pool which defines the common characteristics for Webex remote devices. For more information on how to configure the device pool, see Device Pool Configuration Settings.
Calling Search Space	From the drop-down list, choose the calling search space or leave the calling search space as the default of <None>.
User Hold MOH Audio Source	From the drop-down list, choose the audio source to use for music on hold (MOH) when you initiate a hold action. **Caution** MOH is currently not supported for Cisco Spark remote device as Hold/Resume feature on the device is not implemented.
Network Hold MOH Audio Source	From the drop-down list, choose the audio source to use for MOH when the network initiates a hold action. **Caution** MOH is currently not supported for Cisco Spark remote device as Hold/Resume feature on the device is not implemented.
Location	From the drop-down list, choose the location that is associated with the phones and gateways in the device pool.

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 pool.
Ignore Presentation Indicators (internal calls only)	Check this check box to configure call display restrictions on a call-by-call basis. When this check box is checked, Cisco Unified CM ignores any presentation restriction that is received for internal calls.
Call Routing Information	
Inbound and Outbound Calls Information	
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.
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.
Protocol Specific Information	
Presence Group	Configure this field with the Presence feature. If you are not using this application user with presence, leave the default (None) setting for presence group. From the drop-down list, choose a Presence group for the application user. The group selected specifies the destinations that the application user, such as IPMASysUser, can monitor. **Caution** Presence Group is currently not supported for Cisco Spark remote device .

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, 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. 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 can configure a calling search space as you do all calling search spaces. **Caution** SUBSCRIBE Calling Search Space is currently not supported for Cisco Spark remote device.
Rerouting Calling Search Space	From the drop-down list, choose a calling search space to use for rerouting. The rerouting calling search space of the referrer is used to find the route to the refer-to target. When the Refer message 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.
Do Not Disturb Information	
Do Not Disturb	Check this check box to enable Do Not Disturb on the remote device. **Caution** The calls are not routed to Cisco Spark clients if the DND option is enabled. **Caution** Do Not Disturb is currently not supported for Cisco Spark remote device .

Field	Description
DND Option	When you enable DND on the phone, Call Reject 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. **Caution** Do Not Disturb is currently not supported for Cisco Spark remote device .

Add a Directory Number to a Cisco Spark Device

To register a Webex remote device, add a Directory Number to that device. You cannot register a Webex remote device without a Directory Number. You can add a maximum of five Directory Numbers to the Webex remote device.

Procedure

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

Step 2 Specify the filter criteria and click the Cisco Spark Remote Device for which you want to associate the directory number.

Step 3 In the **Association** pane, click **Add a new DN** link.

Step 4 Configure the fields in the **Directory Number Configuration** window. See the online help for more information about the fields and their configuration options.

Step 5 Click **Save**.

Migrate Phone Data

Procedure

	Command or Action	Purpose
Step 1	Create a Phone Template, on page 366	Create a phone template in Bulk Administration Tool (BAT) for the phone model and protocol to which you want to migrate the data.
Step 2	Migrate Phone Data, on page 366	Migrate phone data to a different phone.

Create a Phone Template

Procedure

Step 1 From Cisco Unified CM Administration, choose **Bulk Administration** > **Phones** > **Phone Template**.

Step 2 Click **Add New**.
The **Add a New Phone Template** window displays.

Step 3 From the **Phone Type** drop-down list, choose the phone model for which you are creating the template. Click **Next**.

Step 4 From the **Select the Device Protocol** drop-down list, choose the device protocol. Click **Next**.
The **Phone Template Configuration** window appears with fields and default entries for the chosen device type.

Step 5 Configure the fields in the **Phone Template Configuration** window. See the online help for more information about the fields and their configuration options.

Step 6 Click **Save**.

Migrate Phone Data

Before you begin

- Unplug the phone from the network.
- Ensure that there are enough device license units for the new phone.
- Ensure that the phone model supports phone migration.

Procedure

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

Step 2 Specify the search criteria and click **Find**.

Step 3 Choose and click the phone configuration that you want to migrate.

Step 4 Choose **Migrate Phone** from the **Related Links** drop-down list.
The **Phone Migration Configuration** window appears.

Step 5 From the drop-down list, choose the phone template for the phone model to which you want to migrate the phone configuration.

Step 6 Enter the **Media Access Control (MAC) address** for the new Cisco Unified IP Phone to which you are migrating the configuration. The MAC address must contain 12 hexadecimal characters.

Step 7 (Optional) Enter a description for the new phone. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).

Step 8 Click **Save**.

Step 9 If a warning displays that the new phone may lose feature functionality, click **OK**.

What to do next

Plug the new phone into the network and register the device.

CHAPTER 44

Configure Call Diagnostics and Quality Reporting for Cisco IP Phones

Diagnostics and Reporting Overview

Cisco Unified Communications Manager offers two options for ensuring call quality on Cisco IP Phones:

- Call Diagnostics—Call diagnostics includes generating Call Management Records (CMR) and voice quality metrics.
- Quality Report Tool QRT)—QRT is a voice-quality and general problem-reporting tool for Cisco Unified IP Phones. This tool allows users to easily and accurately report audio and other general problems with their IP phone.

Call Diagnostics Overview

You can configure Cisco IP Phones that are running SCCP and SIP to collect call diagnostics. Call diagnostics comprises Call Management Records (CMR), also called diagnostic records, and voice quality metrics.

Voice quality metrics are enabled by default and supported on most of the Cisco IP Phones. Cisco IP Phones calculate voice quality metrics based on MOS (Mean Opinion Square) value. Voice quality metrics do not account for noise or distortion, only frame loss.

The CMR records store information about the quality of the streamed audio of the call. You can configure the Unified Communications Manager to generate CMRs. This information is useful for post-processing activities such as generating billing records and network analysis.

Quality Report Tool Overview

The Quality Report Tool (QRT) is a voice-quality and general problem-reporting tool for Cisco IP Phones. This tool allows users to easily and accurately report audio and other general problems with their IP phone.

As a system administrator, you can enable QRT functionality by configuring and assigning a softkey template to display the QRT softkey on a user IP phone. You can choose from two different user modes, depending on the level of user interaction that you want with QRT. You then define how the feature works in your system by configuring system parameters and setting up Cisco Unified Serviceability tools. You can create, customize, and view phone problem reports by using the QRT Viewer application.

When users experience problems with their IP phones, they can report the type of problem and other relevant statistics by pressing the QRT softkey on the Cisco IP Phones during the On Hook or Connected call states. Users can then choose the reason code that best describes the problem that is being reported for the IP phone. A customized phone problem report provides you with the specific information.

QRT attempts to collect the streaming statistics after a user selects the type of problem by pressing the QRT softkey. A call should be active for a minimum of 5 seconds for QRT to collect the streaming statistics.

Prerequisites

Call Diagnostics Prerequisites

Check if your Cisco Unified IP Phone supports Call Diagnostics.

Use this table to determine if your phone supports Call Diagnostics. The Support for Call Diagnostics legend is as follows:

- X—Supported by phones that are running both SCCP and SIP
- S—SCCP feature only

Table 61: Device Support for Call Diagnostics

Device	Support for Call Diagnostics
Cisco Unified IP Phone 7906	X
Cisco Unified IP Phone 7911	X
Cisco Unified IP Phone 7931	X
Cisco Unified IP Phone 7940	S
Cisco Unified IP Phone 7941	X
Cisco Unified IP Phone 7942-G	X
Cisco Unified IP Phone 7942-G/GE	X
Cisco Unified IP Phone 7945	X
Cisco Unified IP Phone 7960	S
Cisco Unified IP Phone 7961	X
Cisco Unified IP Phone 7962-G	X

Device	Support for Call Diagnostics
Cisco Unified IP Phone 7962-G/GE	X
Cisco Unified IP Phone 7965	X
Cisco Unified IP Phone 7972-G/GE	X
Cisco Unified IP Phone 7975	X

Quality Report Tool Prerequisites

Any Cisco IP Phone that includes the following capabilities:

- Support for softkey templates
- Support for IP phone services
- Controllable by CTI
- Contains an internal HTTP server

For more information, see the guide for your phone model.

Diagnostics and Reporting Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure Call Diagnostics, on page 372	Perform this task to configure Cisco Unified Communications Manager to generate CMRs. The CMR records store information about the quality of the streamed audio of the call. For more information about accessing CMRs, see the *Cisco Unified Communications Manager Call Detail Records Administration Guide* . Voice Quality Metrics are automatically enabled on the Cisco IP Phones. For more information about accessing voice quality metrics, see the Cisco Unified IP Phone Administration Guide for your phone model.
Step 2	To Configure the Quality Report Tool, on page 372, perform the following subtasks: • Configure a Softkey Template with the QRT Softkey, on page 373 • Associate a QRT Softkey Template with a Common Device Configuration, on page 374	Configure the Quality Report Tool (QRT) so that users who experience problems with their IP phones can report the type of problem and other relevant statistics by pressing a QRT softkey.

	Command or Action	Purpose
	• Add the QRT Softkey Template to a Phone, on page 376 • Configure QRT in Cisco Unified Serviceability, on page 376 • Configure the Service Parameters for the Quality Report Tool, on page 379	

Configure Call Diagnostics

Procedure

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

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

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

Step 4 In the **Clusterwide Parameters (Device - General)** area, configure the **Call Diagnostics Enabled** service parameter. The following options are available:

- **Disabled**—CMRs are not generated.
- **Enabled Only When CDR Enabled Flag is True**—CMRs are generated only when the Call Detail Records (CDR) Enabled Flag service parameter is set to True.
- **Enabled Regardless of CDR Enabled Flag**—CMRs are generated regardless of the CDR Enabled Flag service parameter value.

Note Generating CMRs without enabling the CDR Enabled Flag service parameter can cause uncontrolled disk space consumption. Cisco recommends that you enable CDRs when CMRs are enabled.

Step 5 Click **Save**.

Configure the Quality Report Tool

Configure the Quality Report Tool (QRT) so that users who experience problems with their IP phones can report the type of problem and other relevant statistics by pressing a QRT softkey.

Procedure

	Command or Action	Purpose
Step 1	Configure a Softkey Template with the QRT Softkey, on page 373	You must configure the On Hook and Connected call states for the QRT Softkey. The following call states are also available: • Connected Conference

	Command or Action	Purpose
		• Connected Transfer
Step 2	(Optional) To Associate a QRT Softkey Template with a Common Device Configuration, on page 374, perform the following subtasks: • Add a QRT Softkey Template to a Common Device Configuration, on page 375 • Associate a Common Device Configuration with a Phone, on page 376	To make the softkey template available to phones, you must complete either this step or the following step. Follow this step if your system uses a **Common Device Configuration** to apply configuration options to phones. This is the most commonly used method for making a softkey template available to phones.
Step 3	(Optional) Add the QRT Softkey Template to a Phone, on page 376	Use this procedure either as an alternative to associating the softkey template with the Common Device Configuration, or in conjunction with the Common Device Configuration. Use this procedure in conjunction with the Common Device Configuration if you need assign a softkey template that overrides the assignment in the Common Device Configuration or any other default softkey assignment.
Step 4	To Configure QRT in Cisco Unified Serviceability, on page 376, perform the following subtasks: • Activate the Cisco Extended Functions Service, on page 377 • Configure Alarms, on page 377 • Configure Traces, on page 378	
Step 5	(Optional) Configure the Service Parameters for the Quality Report Tool, on page 379	

Configure a Softkey Template with the QRT Softkey

You must configure the On Hook and Connected call states for the QRT Softkey. The following call states are also available:

- Connected Conference
- Connected Transfer

Procedure

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

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

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

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

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

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

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

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

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

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

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

Step 9 Click **Save**.

Step 10 Perform one of the following tasks:

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

What to do next

Perform one of the following steps:

- Add a QRT Softkey Template to a Common Device Configuration, on page 375
- Add the QRT Softkey Template to a Phone, on page 376

Associate a QRT Softkey Template with a Common Device Configuration

Optional. There are two ways to associate a softkey template with a phone:

- Add the softkey template to the Phone Configuration.
- Add the softkey template to the Common Device Configuration.

The procedures in this section describe how to associate the softkey template with a Common Device Configuration. Follow these procedures if your system uses a Common Device Configuration to apply configuration options to phones. This is the most commonly used method for making a softkey template available to phones.

To use the alternative method, see Add the QRT Softkey Template to a Phone, on page 376.

Procedure

	Command or Action	Purpose
Step 1	Add a QRT Softkey Template to a Common Device Configuration, on page 375	
Step 2	Associate a Common Device Configuration with a Phone, on page 376	

Add a QRT Softkey Template to a Common Device Configuration

Before you begin

Configure a Softkey Template with the QRT Softkey, on page 373

Procedure

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

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

a) Click **Add New**.

b) Enter a name for the Common Device Configuration in the **Name** field.

c) Click **Save**.

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

a) Click **Find** and enter the search criteria.

b) Click an existing Common Device Configuration.

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

Step 5 Click **Save**.

Step 6 Perform one of the following tasks:

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

What to do next

Associate a Common Device Configuration with a Phone, on page 376

Associate a Common Device Configuration with a Phone

Before you begin

Add a QRT Softkey Template to a Common Device Configuration, on page 375

Procedure

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

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

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

Step 4 Click **Save**.

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

Add the QRT Softkey Template to a Phone

Before you begin

Configure a Softkey Template with the QRT Softkey, on page 373

Procedure

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

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

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

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

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

Configure QRT in Cisco Unified Serviceability

Procedure

	Command or Action	Purpose
Step 1	Activate the Cisco Extended Functions Service, on page 377	Activate the Cisco Extended Functions Service to provide support for voice-quality features such as the Quality Report Tool.
Step 2	Configure Alarms, on page 377	Configure alarms for the QRT to log errors in the Application Logs within SysLog Viewer. This function logs alarms, provides a

	Command or Action	Purpose
		description of the alarms, and recommended actions. You can access the SysLog Viewer from the Cisco Unified Real-Time Monitoring Tool.
Step 3	Configure Traces, on page 378	Configure traces for the QRT to log trace information for your voice application. After configure the information that you want to include in the trace files for the QRT, you can collect and view trace files by using the Trace and Log Central option in the Cisco Unified Real-Time Monitoring Tool.

Activate the Cisco Extended Functions Service

Activate the Cisco Extended Functions Service to provide support for voice-quality features such as the Quality Report Tool.

Procedure

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

Step 2 From the **Server** drop-down list, choose the node on which you want to activate the Cisco Extended Functions service.

Step 3 Check the **Cisco Extended Functions** check box.

Step 4 Click **Save**.

What to do next

Configure Alarms, on page 377

Configure Alarms

Configure alarms for the QRT to log errors in the Application Logs within SysLog Viewer. This function logs alarms, provides a description of the alarms, and recommended actions. You can access the SysLog Viewer from the Cisco Unified Real-Time Monitoring Tool.

Before you begin

Activate the Cisco Extended Functions Service, on page 377

Procedure

Step 1 From the Cisco Unified Serviceability, choose **Alarm** > **Configuration**.

Step 2 From the **Server** drop-down list, choose the node on which you want to configure alarms.

Step 3 From the **Service Group** drop-down list, choose **CM Services**.

Step 4 From the **Service** drop-down list, choose **Cisco Extended Functions**.

Step 5 Check the **Enable Alarm** check box for both Local Syslogs and SDI Trace.

Step 6 From the drop-down list, configure the Alarm Event Level for both Local Syslogs and SDI Trace by choosing one of the following options:

- **Emergency**—Designates the system as unusable.
- **Alert**—Indicates that immediate action is needed.
- **Critical**—The system detects a critical condition.
- **Error**—Indicates that an error condition is detected.
- **Warning**—Indicates that a warning condition is detected.
- **Notice**—Indicates that a normal but significant condition is detected.
- **Informational**—Indicates only information messages.
- **Debug**— Indicates detailed event information that Cisco Technical Assistance Center (TAC) engineers use for debugging.

The default value is **Error**.

Step 7 Click **Save**.

What to do next

Configure Traces, on page 378

Configure Traces

Configure traces for the QRT to log trace information for your voice application. After configure the information that you want to include in the trace files for the QRT, you can collect and view trace files by using the Trace and Log Central option in the Cisco Unified Real-Time Monitoring Tool.

Before you begin

Configure Alarms, on page 377

Procedure

Step 1 From Cisco Unified Serviceability, choose **Trace** > **Configuration**.

Step 2 From the **Server** drop-down list, choose the node on which you want to configure traces.

Step 3 From the **Service Group** drop-down list, choose **CM Services**.

Step 4 From the **Service** drop-down list, choose **Cisco Extended Functions**.

Step 5 Check the **Trace On** check box.

Step 6 From the **Debug Trace Level** drop-down list, choose one of the following options:

- **Error**—Traces all error conditions, as well as process and device initialization messages.
- **Special**—Traces all special conditions and subsystem state transitions that occur during normal operation. Traces call-processing events.
- **State Transition**—Traces all state transition conditions and media layer events that occur during normal operation.

- **Significant**—Traces all significant conditions, as well as entry and exit points of routines. Not all services use this trace level.
- **Entry_exit**—Traces all entry and exit conditions, plus low-level debugging information.
- **Arbitrary**—Traces all Arbitrary conditions plus detailed debugging information.
- **Detailed**— Traces alarm conditions and events. Used for all traces that are generated in abnormal path. Uses minimum number of CPU cycles.

The default value is **Error**.

Tip We recommend that you check all the check boxes in this section for troubleshooting purposes.

Step 7 Click **Save**.

What to do next

(Optional) Configure the Service Parameters for the Quality Report Tool, on page 379

Configure the Service Parameters for the Quality Report Tool

Caution We recommend that you use the default service parameters settings unless the Cisco Technical Assistance Center (TAC) instructs otherwise.

Procedure

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

Step 2 Choose the node where the QRT application resides.

Step 3 Choose the **Cisco Extended Functions** service.

Step 4 Configure the service parameters. See the Related Topics section for more information about the service parameters and their configuration options.

Step 5 Click **Save**.

Related Topics

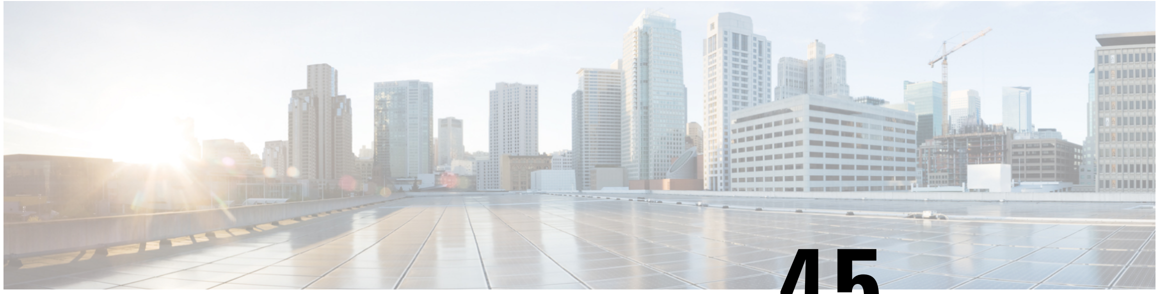
Quality Report Tool Service Parameters, on page 380

Quality Report Tool Service Parameters

Table 62: Quality Report Tool Service Parameters

Parameter	Description
Display Extended QRT Menu Choices	Determines whether extended menu choices are presented to the user. You can choose one of the following configuration options: • Set this field to true to display extended menu choices (interview mode). • Set this field to false to not display extended menu choices (silent mode). • The recommended default value is false (silent mode).
Streaming Statistics Polling Duration	Determines the duration that is to be used for polling streaming statistics. You can choose one of the following configuration options: • Set this field to -1 to poll until the call ends. • Set this field to 0 to not poll at all. • Set it to any positive value to poll for that many seconds. Polling stops when the call ends. • The recommended default value is -1 (poll until the call ends).
Streaming Statistics Polling Frequency (seconds)	Enter the number of seconds to wait between each poll. The value ranges between 30 and 3600. The recommended default value is 30.
Maximum No. of Files	Enter the maximum number of files before the file count restarts and overwrites the old files. Valid values are between 1 and 10000. The recommended default value is 250.
Maximum No. of Lines per File	Enter the maximum number of lines in each file before starting the next file: • The value ranges between 100 and 2000. • The recommended default value specifies 2000.

Parameter	Description
CAPF Profile Instance Id for Secure Connection to CTI Manager	Enter the Instance ID of the Application CAPF Profile for application user CCMQRTSysUser that the Cisco Extended Function service will use to open a secure connection to CTI Manager. You must configure this parameter if CTI Manager Connection Security Flag is enabled. **Note** Turn on security by enabling the CTI Manager Connection Security Flag service parameter. You must restart the Cisco Extended Functions service for the changes to take effect.
CTI Manager Connection Security Flag	Choose whether security for Cisco Extended Functions service CTI Manager connection is enabled or disabled. If enabled, Cisco Extended Functions will open a secure connection to CTI Manager using the Application CAPF Profile configured for the Instance ID for application user CCMQRTSysUser. The value choices are True and False. You must choose True to enable a secure connection to CTI.



CHAPTER 45

Configure Third-Party SIP Phones

Third-Party SIP Endpoints Overview

In addition to the Cisco IP Phones that run SIP, Unified Communications Manager supports a variety of third-party SIP endpoints. You can configure the following third-party SIP endpoints in Cisco Unified Communications Manager Administration:

- Third-Party SIP Device (Advanced)— This eight-line SIP device is an RFC3261-compliant phone that is running SIP from third-party companies.
- Third-Party SIP Device (Basic)— This one-line SIP device is an RFC3261-compliant phone that is running SIP from third-party companies.
- Third-Party AS-SIP Device — Assured Services SIP (AS-SIP) endpoints are SIP endpoints compliant with MLPP, DSCP, TLS/SRTP, and IPv6 requirements. AS-SIP provides multiple endpoint interfaces on the Unified Communications Manager.
- Generic Desktop Video Endpoint —This SIP device supports video, security, configurable trust, and Cisco extensions. This device supports 8 lines; the maximum number of calls and busy trigger for each line is 4 and 2, respectively.
- Generic Single Screen Room System —This SIP device supports single screen telepresence (room systems), video, security, configurable trust, and Cisco extensions. This device supports 8 lines; the maximum number of calls and busy trigger for each line is 4 and 2, respectively.
- Generic Multiple Screen Room System — This SIP device supports multiple screen telepresence (room systems), video, security, configurable trust, and Cisco extensions. This device supports 8 lines; the maximum number of calls and busy trigger for each line is 4 and 2, respectively.

Third-Party SIP Endpoints Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure a Digest User, on page 384	To enable digest authentication, configure an end user that is a digest user. Cisco Unified

	Command or Action	Purpose
		Communications Manager uses the digest credentials that you specify in the **End User Configuration** window to validate the SIP user agent response during a challenge to the SIP trunk. If the third-party SIP phone does not support a digest user, create a user with a user ID that matches the directory number of the third-party SIP phone. For example, create an end user named 1000 and create a directory number of 1000 for the phone. Assign this user to the phone.
Step 2	Configure SIP Profile, on page 348	Provide a set of SIP attributes that are associated with SIP trunks.
Step 3	Configure Phone Security Profile, on page 385	To use digest authentication, you must configure a new phone security profile. If you use one of the standard, nonsecure SIP profiles that are provided for auto-registration, you cannot enable digest authentication.
Step 4	Add a Third-Party SIP Endpoint, on page 386	Configure a third-party endpoint.
Step 5	Associate Device to End User, on page 387	Associate the third-party endpoint with an end user.

What to do next

Provide power, verify network connectivity, and configure network settings for the third-party SIP endpoint. For more information about configuring network settings, see the user guide for your third-party SIP endpoint.

Configure a Digest User

Perform these steps to configure an end user as a digest user. Digest authentication allows Cisco Unified Communications Manager to challenge the identity of a device that is connecting to Cisco Unified Communications Manager. When challenged, the device presents its digest credentials, similar to a username and password, to Cisco Unified Communications Manager for verification. If the credentials that are presented match those that are configured in the database for that device, digest authentication succeeds, and Cisco Unified Communications Manager processes the SIP request.

Procedure

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

Step 2 Click **Add New**.

Step 3 Enter a **User ID**.

Step 4 Enter a **Last Name**.

Step 5 Enter **Digest Credentials**. The digest credentials are a string of alphanumeric characters.

Step 6 Complete any remaining fields in the **End User Configuration** window. See the online help for more information about the fields and their configuration options..

Step 7 Click **Save**.

What to do next

Configure SIP Phone Secure Port, on page 348

Configure SIP Profile

Use this procedure to configure SIP profile with SIP settings for your AS-SIP endpoints and for your SIP trunks.

Before you begin

- Configure SIP Phone Secure Port, on page 348
- Restart Services, on page 348

Procedure

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

Step 2 Click **Find**.

Step 3 For the profile that you want to copy, click the file icon in the **Copy** column.

Step 4 Enter the name and description of the new profile.

Step 5 If you have the IPv6 stack configured and you are deploying two stacks, check the **Enable ANAT** check box.

Note This configuration applies whether you have Unity Connection deployed or not.

Step 6 Click **Save**.

What to do next

Configure Phone Security Profile, on page 385

Configure Phone Security Profile

Cisco Unified Communications Manager provides a set of predefined, nonsecure profiles for autoregistration. If you want to enable security features for a phone, you must configure a new security profile and apply it to the phone. Follow these steps to configure a new security profile:

Before you begin

If you are configuring SIP phones, complete the following procedures:

- Configure SIP Phone Secure Port, on page 348
- Restart Services, on page 348
- Configure SIP Profile, on page 348

Procedure

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

Step 2 Click **Add New**.

Step 3 From the **Phone Security Profile Type** drop-down list, choose the Universal Device Template to create a profile that you can use when provisioning through the device templates.

Note Optionally, you can also create security profiles for specific device models.

Step 4 Select the protocol.

Step 5 Enter an appropriate name for the profile in the **Name** field.

Step 6 If you want to use TLS signaling to connect to the device, set the **Device Security Mode** to **Authenticated** or **Encrypted** and the Transport Type to **TLS**.

Step 7 (Optional) Check the **Enable OAuth Authentication** check box if you want the phone to use digest authentication.

Step 8 (Optional) Check the **TFTP Encrypted Config** check box if you want to use encrypted TFTP.

Step 9 Complete the remaining fields in the Phone Security Profile Configuration window. For help with the fields and their settings, see the online help.

Step 10 Click **Save**.

Add a Third-Party SIP Endpoint

Before you begin

Configure a Digest User, on page 384

Procedure

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

Step 2 Perform one of the following steps:

- Click **Add New** to create a new third-party endpoint.
- Click **Find** to search and select an existing third-party endpoint.

Step 3 From the **Phone Type** drop-down list, choose one of the following:

- Third-party SIP Device (Basic)
- Third-party SIP Device (Advanced)

- Third-Party AS-SIP Device
- Third-party AS-SIP Endpoint
- Generic Desktop Video Endpoint
- Generic Single Screen Room System
- Generic Multiple Screen Room System

Step 4 From the **Digest User** drop-down list, choose the user that you created.

Step 5 Configure the fields in the **Phone Configuration** window. See the online help for more information about the fields and their configuration options.

Step 6 Click **Save**.

Step 7 To configure a directory number for the third-party endpoint, 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 appears.

Step 8 Configure the fields in the Directory Number Configuration window. For help with the fields and their settings, see the online help.

What to do next

Associate Device to End User, on page 387

Associate Device to End User

Use this procedure to associate an end user to the third-party endpoint.

Procedure

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

Step 2 Click **Find** and select the user whom you want to associate to the device.

Step 3 In the **Device Information** section, click **Device Association** .
The User Device Association window appears.

Step 4 Click **Find** to view a list of available devices.

Step 5 Select the device that you want to associate, and click **Save Selected/Changes**.

Step 6 From **Related Links**, choose **Back to User**, and click **Go**.
The **End User Configuration** window appears, and the associated device that you chose appears in the **Controlled Devices** pane.

Third-Party Interactions and Restrictions

Third-Party Restrictions

Table 63: Third-Party SIP Endpoints Restrictions

Restriction	Description
Ringback tone restriction for Cisco Video Communications Server (VCS) registered to third-party SIP Endpoints	Blind transfer or switch to request the transfer which occurs over VCS registered endpoints with Cisco Unified Communications Manager will not have a ringback tone. If you do a supervised transfer, then you allocate Music On Hold (MOH) but, not a ringback tone.

CHAPTER 46

Device Profiles and Templates

Device Profiles and Templates Overview

This chapter explains how to configure device profiles and templates. For information about configuring specific features, see the *Feature Configuration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Device Profiles

A device profile defines the services, features, and directory numbers that associate with a particular device. You can configure a device profile and then you can assign the user device profile to a user, so that when the user logs in to a device, those features and services are available on that device.

SIP Profiles for End Points

A SIP profile comprises the set of SIP attributes that are associated with 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.

Device Profiles and Templates

Cisco Unified Communications Manager also supports a default device profile. Cisco Unified Communications Manager uses the default device profile whenever a user logs on to a phone model for which no user device profile exists.

Peer-to-Peer Image Distribution

The peer firmware sharing feature provides these advantages in high-speed campus LAN settings:

- Limits congestion on TFTP transfers to centralized TFTP servers.
- Eliminates the need to manually control firmware upgrades.

- Reduces phone downtime during upgrades when large numbers of devices are reset simultaneously.

In most conditions, the peer firmware sharing feature optimizes firmware upgrades in branch deployment scenarios over bandwidth-limited WAN links.

When the feature is enabled, it allows the phone to discover similar phones on the subnet that are requesting the files that make up the firmware image and to automatically assemble transfer hierarchies on a per-file basis. The individual files that make up the firmware image get retrieved from the TFTP server by only the root phone in the hierarchy and are then rapidly transferred down the transfer hierarchy to the other phones on the subnet using TCP connections.

Configure Device Profiles and Templates Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure a Softkey Template on the Default Device Profile, on page 391	Add the default device profile to a softkey template.
Step 2	Associate a Softkey Template with a Common Device Configuration, on page 392	Optional. To make the softkey template available to phones, you must associate the template to a Common Device Configuration or directly to a phone. Follow this step if your system uses a common device configuration to apply configuration options to phones (this is the most commonly used method for making a softkey template available to phones). **Note** For information on how to associate a common device configuration on multiple phones by using the Bulk Administration Tool, see the *Cisco Unified Communications Manager Bulk Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.
Step 3	Associate a Softkey Template with a Phone, on page 394	Optional. Use this procedure either as an alternative to associating the softkey template with the common device configuration, or in conjunction with the common device configuration. Use this procedure in conjunction with the common device configuration if you need assign a softkey template that overrides the assignment in the common device configuration or any other default softkey assignment.
Step 4	Configure Feature Control Policy Task Flow, on page 394	Optional. Use this procedure as an alternative to configuring softkey templates. Configure

	Command or Action	Purpose
		feature control policies to enable or disable a particular feature and thereby control the appearance of softkeys that display on the phone. You can create a feature control policy for a group of users that wants to use a common set of features. For example, call park and call pickup features are typically used by the employees from the sales group and not all the employees in a company. You can create a feature control policy that enables only these two features and assign that policy to the sales group. After you create a feature control policy, you can associate that policy with an individual phone, a group of phones, or with all phones in the system.
Step 5	Configure a Phone Button Template, on page 397 • Associate a Button Template with a Phone, on page 398	Use this procedure to include default templates for each Cisco IP Phone model. When you add phones, you can assign one of these templates to the phone or create a template of your own.
Step 6	Configure Device Profile, on page 398	Configure the device profile for any phone model that supports SIP or SCCP.
Step 7	Configure SIP Profiles for Endpoints, on page 399	To configure a new SIP profile for the phone.
Step 8	Configure Default Device Profiles, on page 399	Configure the default device profile for any phone model that supports SIP or SCCP.

Configure a Softkey Template on the Default Device Profile

Cisco Unified Communications Manager includes standard softkey templates for call processing and applications. When creating custom softkey templates, copy the standard templates and make modifications as required.

Procedure

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

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

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

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

a) Click **Find** and enter the search criteria.

b) Select the required existing template.

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

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

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

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

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

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

Step 9 Click **Save**.

Step 10 Perform one of the following tasks:

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

What to do next

You can apply a customized softkey template to a device by selecting the template from the Softkey Template drop-down in one of the following configuration windows:

- Phone Configuration
- Universal Device Template
- BAT Template
- Common Device Configuration
- Device Profile
- Default Device Profile
- UDP Profile

Associate a Softkey Template with a Common Device Configuration

Optional. There are two ways to associate a softkey template with a phone:

- Add the softkey template to the **Phone Configuration**.
- Add the softkey template to the **Common Device Configuration**.

The procedures in this section describe how to associate the softkey template with a **Common Device Configuration**. Follow these procedures if your system uses a **Common Device Configuration** to apply configuration options to phones. This is the most commonly used method for making a softkey template available to phones.

To use the alternative method, see the section *Associate a Softkey Template with a Phone* .

Procedure

Step 1 Add a Softkey Template to a Common Device Configuration , on page 393

Step 2 Associate a Common Device Configuration with a Phone, on page 393

Add a Softkey Template to a Common Device Configuration

Procedure

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

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

a) Click **Add New**.

b) Enter a name for the Common Device Configuration in the **Name** field.

c) Click **Save**.

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

a) Click **Find** and enter the search criteria.

b) Click an existing Common Device Configuration.

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

Step 5 Click **Save**.

Step 6 Perform one of the following tasks:

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

Associate a Common Device Configuration with a Phone

Procedure

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

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

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

Step 4 Click **Save**.

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

Associate a Softkey Template with a Phone

Optional. Use this procedure as an alternative to associating the softkey template with the Common Device Configuration. This procedure also works in conjunction with the Common Device Configuration. You can use it when you need to assign a softkey template that overrides the assignment in the Common Device Configuration or any other default softkey assignment.

Procedure

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

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

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

Step 4 Click **Save**.

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

Configure Feature Control Policy Task Flow

Procedure

	Command or Action	Purpose
Step 1	Generate a Phone Feature List, on page 395	Login to Cisco Unified Reporting and run a phone feature list report to determine which phones support Feature Control Policy.
Step 2	Create a Feature Control Policy, on page 395	Create a Feature Control Policy for Cisco IP Phones.
Step 3	Perform one of the following tasks: • Apply Feature Control Policy to a Phone, on page 396 • Apply Feature Control Policy to a Common Phone Profile, on page 396 • Apply Feature Control Policy to All Phones, on page 397	After you create a Feature Control Policy, you must associate that policy to an individual phone, a group of phones, or to all phones in the system. The Feature Control Policy for an individual phone overrides the clusterwide feature control policy.

	Command or Action	Purpose
		Note For information on how to apply Feature Control Policy on multiple phones by using the Bulk Administration Tool, see the *Cisco Unified Communications Manager Bulk Administration Guide*.

Generate a Phone Feature List

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

Procedure

Step 1 From Cisco Unified Reporting, choose **System Reports**.

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

Step 3 Perform one of the following steps:

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

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

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

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

Create a Feature Control Policy

Follow these steps to create a feature control policy. Use this policy to enable or disable a particular feature and hence control the appearance of softkeys that display on the phone.

Procedure

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

Step 2 Perform one of the following tasks:

- To modify the settings for an existing policy, enter search criteria, click **Find** and choose the policy from the resulting list.
- To add a new policy, click **Add New**.

The **Feature Control Policy Configuration** window is displayed.

Step 3 In the **Name** field, enter a name for the feature control policy.

Step 4 In the **Description** field, enter a brief description for the feature control policy.

Step 5 In the **Feature Control Section**, for each feature listed, choose whether you want to override the system default and enable or disable the setting:

- If the feature is enabled by default and you want to disable the setting, check the check box under **Override Default** and uncheck the check box under **Enable Setting**.
- If the feature is disabled by default and you want to enable the setting, check the check box under **Override Default** and check the check box under **Enable Setting**.

Step 6 Click **Save**.

Apply Feature Control Policy to a Phone

Before you begin

- Ensure that the phone model supports Feature Control Policy. For more information, see Generate a Phone Feature List, on page 395.
- Create a Feature Control Policy, on page 395

Procedure

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

Step 2 Enter the search criteria and click **Find**.
A list of phones that are configured on the **Cisco Unified Communications Manager** is displayed.

Step 3 Choose a phone to which you want to apply a Feature Control Policy.

Step 4 From the **Feature Control Policy** drop-down list, choose the required Feature Control Policy.

Step 5 Click **Save**.

Step 6 Click **Apply Config**.

Step 7 Click **OK**.

Apply Feature Control Policy to a Common Phone Profile

Common Phone Profiles allow you to configure Feature Control Policy settings and then apply those settings to all the phones in your network that use that profile.

Before you begin

Create a Feature Control Policy, on page 395

Procedure

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

Step 2 Enter the search criteria and click **Find**.

Step 3 Choose a common phone profile to which you want to apply a Feature Control Policy.

Step 4 From the **Feature Control Policy** drop-down list, choose the required Feature Control Policy.

Step 5 Click **Save**.

Step 6 Click **Apply Config**.

Step 7 Click **OK**.

Apply Feature Control Policy to All Phones

Before you begin

Create a Feature Control Policy, on page 395

Procedure

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

Step 2 From the **Feature Control Policy** drop-down list, choose the required Feature Control Policy.

Step 3 Click **Save**.

Step 4 Click **Apply Config**.

Step 5 Click **OK**.

Configure a Phone Button Template

Procedure

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

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

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

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

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

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

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

Step 6 Click **Save**.

Step 7 Perform one of the following tasks:

- Click **Apply Config** if you modified a template that is already associated with devices to restart the devices.

- If you created a new softkey template, associate the template with the devices and then restart them.

Associate a Button Template with a Phone

Before you begin

Configure a Phone Button Template, on page 397

Procedure

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

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

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

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

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

Configure Device Profile

A device profile comprises the set of attributes that associate with a particular device. You can associate the device profile that you create to an end user in order to use the Cisco Extension Mobility feature.

Procedure

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

Step 2 In the **Device Profile Configuration** window, from the **Device Profile Type** drop-down list, choose the appropriate Cisco Unified IP Phone.

Step 3 Click **Next**.

Step 4 From the **Device Protocol** drop-down list, choose the appropriate protocol.

Step 5 Click **Next**.

Step 6 From the **Phone Button Template** drop-down list, choose a template.

Step 7 (Optional) From the **Softkey Template** drop-down list, select a softkey template.

Step 8 Configure the fields in the **Device Profile Configuration** window. See the online help for more information about the fields and their configuration options.

Step 9 Click **Save**.

Note For details on using Device Profiles to setup Cisco Extension Mobility, see the *Feature Configuration Guide for Cisco Unified Communications Manager, Release 12.5(1)SU1*.

Configure SIP Profiles for Endpoints

Cisco Unified Communications Manager uses SIP profiles to define SIP attributes that are associated with SIP trunks and Cisco Unified IP Phones.

Procedure

Step 1 In the **Cisco Unified CM Administration** window, choose **Device** > **Device Settings** > **SIP Profiles**.

Step 2 To add a new SIP Profile, click the **Add New** button.

Step 3 Configure the fields in the **SIP Profile Configuration** window. See the online help for more information about the fields and their configuration options.

Step 4 Click **Apply Config**.

Configure Default Device Profiles

The phone takes on the default device profile whenever a user logs into a phone for which that user does not have a user device profile.

A default device profile includes device type (phone), user locale, phone button template, softkey template, and multilevel precedence and preemption (MLPP) information.

Procedure

Step 1 From the **Cisco Unified CM Administration** window, choose **Device** > **Device Settings** > **Default Device Profile**.

Step 2 In the **Default Device Profile Configuration** window, from the **Device Profile Type** drop-down list, choose the appropriate Cisco Unified IP Phone.

Step 3 Click **Next**.

Step 4 From the **Device Protocol** drop-down list, choose the appropriate protocol.

Step 5 Click **Next**.

Step 6 Configure the fields in the **Default Device Profile Configuration** window. See the online help for more information about the fields and their configuration options.

Step 7 Click **Save**.

Configure Peer-to-Peer Image Distribution Feature for Phones

Procedure

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

Step 2 In the **Find and List Phones** window, to select a phone, specify the appropriate filters in the **Find Phone where** field, click **Find** to retrieve a list of phones, and then select the phone from the list.

Step 3 In the **Phone Configuration** window, from the **Peer Firmware Sharing** drop-down list in the Product Specific Configuration Layout pane, choose one the following options.

- **Enabled** (default)—Indicates that the phone supports Peer-to-Peer Image Distribution (PPID).
- **Disabled**—Indicates that the phone does not support Peer-to-Peer Image Distribution (PPID).

Step 4 Click **Apply Config**.

CHAPTER 47

Associate Users with Endpoints

Users to Endpoints Association Overview

This chapter describes how to associate devices with end users and application users. End users can control the devices that you associate with them. Applications that are identified as users can control devices, such as phones and Computer Telephony Integration (CTI) ports.

Associate Users with Endpoints Prerequisites

Configure end users and application users before you associate them with endpoints. See Associate End Users with Devices, on page 401 and Associate Application Users with Devices, on page 404.

Users and Devices Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Associate End Users with Devices, on page 401.	Associate end users with devices.
Step 2	Associate Application Users with Devices, on page 404.	Associate application users with devices.

Associate End Users with Devices

Cisco Unified Communications Manager does not allow duplicate end user IDs.

Procedure

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

Step 2 From the **Find and List Application Users** window, click **Find**.

Step 3 From the window that displays a list of end users, click the link for the relevant end user.

Step 4 From the **End User Configuration** window, scroll down to the **Device Information** area and select the devices that you want to associate with the end user. In the **Available Devices** box, choose a device that you want to associate with the application user and click the down arrow below the box.

Note If no devices exist in the **Device Information** area, click the **Device Association** button to open the **User Device Association** window. Select one or multiple devices and click the **Save Selected/Changes** button. The selected devices appear in the **Controlled Devices** list box of the **Device Information** area. Then, follow Steps 1 to 4 and associate a device.

Step 5 (Optional) To associate a line appearance to an end user for presence and to enable the on-the-phone status information to IM and Presence clients when this line appearance is off-hook, click the **Line Appearance Association from Presence** button. The **Line Appearance Association for Presence** window appears from where you can choose product type, device name, directory, partition, or description. The choices available in this window depend on the lines associated with the controlled devices. Click **Save**.

Step 6 Configure the fields from the **End User Configuration** window. See the Related Topics section for more information about the fields and their configuration options.

Step 7 Click **Save**.

End User and Device Configuration Settings

Table 64: User Information

Field	Description
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
PIN	Enter five or more numeric characters for the Personal Identification Number.
Last Name	Enter the end user last name. You may use the following special characters: =,+, <, >, #, ;, \, , “”, and blank spaces

Field	Description
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 65: Device Associations

Field	Description
Product Type	From the drop-down list, 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, 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, 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. • 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.

Field	Description
Extension	Enter an extension for the new user and phone. You may use the following characters: 0 to 9, ?, [,], +, -, *, ^, #, !. This field represents the primary directory number for the end user. End users can have multiple lines on their phones.
Route Partition	From the drop-down list, choose a partition for the directory number that you specified in the Extension field.
Voice Mail Profile	From the drop-down list, 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 add the new user, you can use the **User Management** > **End User** menu option to choose an Extension Mobility profile.

Associate Application Users with Devices

You can associate devices over which application users have control. Application users can control 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

Associate End Users with Devices, on page 401.

Procedure

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

Step 2 From the **Find and List Application Users** window, click **Find**.

Step 3 From the list of application users, click the link for the relevant Application User.

Step 4 From the **Application User Configuration** window, scroll down to the **Device Information** area. In the **Available Devices** box, choose a device that you want to associate with the application user and click the down arrow below the box.
The device is moved to the **Controlled Devices** box.

Step 5 To add to the list of available devices, click one of the following buttons:

- **Find more Phones**—To find the phones to associate with this application user.
- **Find more Route Points**—To find the CTI route points to associate with this application user.

- **Find more Pilot Points**—To find the pilot points to associate with this application user.

Step 6 Repeat Step 5 for each device that you want to assign to the application user.

Step 7 Click **Save**.

Interactions and Restrictions for Associating Users with Endpoints

Interactions for Associating Users with Endpoints

Table 66: Users with Endpoints Association Interactions

Feature	Interaction
Non-CTI-controllable devices	For devices that are not CTI-controllable, such as H.323 devices, an asterisk (*) appears next to the device icon in the list of available devices.
Cisco Extension Mobility	Use Cisco Extension Mobility feature to configure a Cisco IP Phone to temporarily display as the phone of an end user. The end user can sign in to a phone, and the Extension Mobility profile (including line and speed-dial numbers) for the end user resides on the phone. This feature applies primarily in environments where end users are not permanently assigned to physical phones.
IM and Presence Service	Use Cisco Unified Communications Manager Administration to assign end users to IM and Presence Service server nodes and clusters for end users to receive the availability and Instant Messaging services of IM and Presence Service.

Restrictions for Associating Users with Endpoints

Table 67: Users with Endpoints Association Restrictions

Restriction	Description
Modification of end user information	You can modify end user information only if synchronization with an LDAP server is not enabled. To check whether synchronization with an LDAP server is enabled, choose **System** > **LDAP** > **LDAP System**.

PART VII

Integrate Applications

CHAPTER 48

Integrate Applications Overview

About Integrating Applications

The chapters in this part describe how to extend the functionality of your system by integrating applications. You can add various functions such as voicemail, contact center features, rich conferencing, or features to monitor the health of your system. Some applications, such as the Cisco Unified Real-Time Monitoring Tool, are built into your system and can be downloaded from the administration interface. Other applications, such as Cisco Jabber or Cisco Unified Contact Center Express, are external to your system and can be configured to interoperate with Unified Communications Manager.

Integrate Applications

Complete the following task flows to integrate applications for your system.

Procedure

	Command or Action	Purpose
Step 1	Application Servers Task Flow, on page 411	Configure application servers to add other product servers to your cluster and establish secure operations between them.
Step 2	Install Plugins Task Flow, on page 415	Use application plugins to extend the functionality of your system.
Step 3	Presence Redundancy Group Task Flow, on page 420	Configure a presence redundancy group which is comprised of two IM and Presence Service nodes from the same cluster. This group provides both redundancy and recovery for IM and Presence Service clients and applications.
Step 4	Cisco Unity Connection, on page 437	Integrate Cisco Unity Connection with your system so that you can provide voicemail and messaging features to your users.

	Command or Action	Purpose
Step 5	Cisco Unified Contact Center Enterprise, on page 441	Configure Cisco Unified Contact Center Enterprise (Unified CCE) to deploy an advanced, distributed contact center. Unified CCE provides intelligent call routing, network-to-desktop Computer Telephony Integration (CTI), and multichannel contact management to contact center agents over an IP network.
Step 6	Cisco Unified Contact Center Express, on page 443	Configure Cisco Unified Contact Center Express (Unified CCX) to provide your system with the features of a large contact center packaged in a single- or dual-server deployment.
Step 7	Configure CTI Applications Task Flow, on page 447	Use computer telephony integration (CTI) to take advantage of computer-processing functions while making, receiving, and managing telephone calls. CTI applications allow you to perform such tasks as retrieving customer information from a database based on a caller ID, or to work with the information gathered by an interactive voice response (IVR) system to route a customer's call, along with their information, to the appropriate customer service representative.
Step 8	Cisco TelePresence, on page 455	Integrate TelePresence functionality into your system. If Unified Communications Manager is your main call processing agent, you can add the Cisco Video Communications Server (VCS) to provide full-featured interoperability with H.323 endpoints and interworking with SIP, integration with third-party video endpoints, and alternate solutions for conferencing. You can also add Cisco TelePresence Conductor which works in conjunction with your system or Cisco VCS to simplify conferencing and the management of multipoint devices. TelePresence Conductor is able to manage multiple conference bridges (Cisco MCUs and TelePresence Servers) for ad-hoc, rendezvous, and scheduled conferences.
Step 9	Configure Cisco Jabber, on page 457	Configure Cisco Jabber, a suite of Unified Communications applications, to allow your users seamless interaction with their contacts from anywhere. This suite offers IM, availability, audio and video calling, voicemail, and conferencing on a variety of platforms.

CHAPTER 49

Configure Application Servers

Application Servers Overview

Use the application server function to maintain associations between the Cisco Unified Communications Manager and off-cluster, external applications, such as Cisco Unity Connection and Cisco Emergency Responder. Application servers also synchronize information between Cisco Unified Communications Manager and applications such as Cisco WebDialer.

Application Servers Prerequisites

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

Application Servers Task Flow

Perform either of the following tasks, depending on the type of application server that you want to configure.

Procedure

	Command or Action	Purpose
Step 1	Configure Application Servers, on page 412	Configure application servers that you want to securely join, interoperate, and share information within your cluster.
Step 2	Configure Cisco WebDialer Servers, on page 412	Configure Cisco WebDialer application servers as an alternative to the **List of WebDialers** service parameter, which limits the number of characters that you can enter. After you add a Cisco WebDialer application server in the

	Command or Action	Purpose
		Application Server Configuration window, the server appears in the List of WebDialers field in the **Service Parameter Configuration** window for the Cisco WebDialer Web Service. For complete details about configuring Cisco WebDialer, see the *Feature Configuration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

Configure Application Servers

Configure application servers that you want to securely join, interoperate, and share information within your cluster.

Procedure

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

Step 2 Click **Add New**.

Step 3 From the **Application Server Type** drop-down list, choose one of the following server options:

- **Cisco Unity Voice Mail 4.x or later**
- **Cisco Unity Connection**
- **CUMA Provisioning Server**
- **CER Location Management**
- **Remote System Log Server**

Step 4 Click **Next**.

Step 5 Configure the fields on the **Application Server Configuration** window. See the online help for more information about the fields and their configuration options.

Step 6 Click **Save**.

Configure Cisco WebDialer Servers

Configure Cisco WebDialer application servers as an alternative to the **List of WebDialers** service parameter, which limits the number of characters that you can enter. After you add a Cisco WebDialer application server in the **Application Server Configuration** window, the server appears in the List of WebDialers field in the **Service Parameter Configuration** window for the Cisco WebDialer Web Service. For complete details about configuring Cisco WebDialer, see the *Feature Configuration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

Procedure

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

Step 2 Click **Add New**.

Step 3 From the **Application Server Type** drop-down list, choose **Cisco Web Dialer**, and then click **Next**.

Step 4 In the **Hostname or IP Address** field, enter the hostname or IP address of the WebDialer server.

Step 5 From the **Redirector Node** drop-down list, choose **< None >** or a specific Unified Communications Manager node.

< None > indicates the WebDialer Server would apply to all nodes.

Step 6 Click **Save**.

Step 7 From Cisco Unified Serviceability, choose **Tools** > **Control Center - Feature Services**

Step 8 Click the **Cisco WebDialer Web Service** radio button.

Step 9 Click **Restart**.

CHAPTER 50

Install Plugins

Plugins Overview

Application plugins extend the functionality of your system.

The following plugins are available from the **Application** > **Plugins** menu:

- Cisco AXL Toolkit—Lets developers create applications that create, read, update and delete provisioning objects on the publisher node. The zip file contains Java-based libraries that use SOAP over HTTP/HTTPS to send and receive AXL requests and responses.
- Cisco JTAPI Client—Provides a standard programming interface for communication-enabled applications that are written in the Java programming language.
- Cisco TAPI Client—Provides a standard programming interface for communication-enabled applications that are running on Microsoft Windows.
- Cisco Tool for Auto-Registered Phone Support (TAPS)—Helps users remotely download preconfigured phone settings to provision their devices.
- Cisco Unified CM Assistant Console—Helps assistants more effectively handle calls for their managers. The assistant console connects to the Cisco Unified Communications Manager IP Manager Assistant (IPMA) Service for login and directory services.
- Cisco Unified Real-Time Monitoring Tool—Monitors device status system performance device discovery and CTI applications running on your cluster in real-time. RTMT also connects directly to devices to aid in troubleshooting.

Install Plugins Task Flow

Perform the following tasks as needed.

Procedure

	Command or Action	Purpose
Step 1	Download a Plugin, on page 416	Download a plugin, and then follow installation instructions from the executable or ZIP file. After you upgrade your system, you must reinstall all plugins.
Step 2	(Optional) Update the Plugin URLs, on page 416	Update the plugin URLs if your domain name server (DNS) changes. At the time of your system installation, the DNS provides the basis for the plugin URL. If the DNS changes, the URL is not automatically updated.

Download a Plugin

Download a plugin, and then follow installation instructions from the executable or ZIP file. After you upgrade your system, you must reinstall all plugins.

Before you begin

Temporarily disable all intrusion detection or antivirus services that run on the server where you plan to install the plugin.

Procedure

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

Step 2 Enter search criteria or leave the dialog box blank, and then click **Find**.

The window that appears contains more information about the application plugins.

Step 3 Click **Download** for the plugin that you want to download and install.

You can also right click **Download** and click **Save As** to choose a folder that is easy for you to find.

Step 4 (Optional) If your plugin is a ZIP file, unzip this file using a built-in or third-party zip program.

Step 5 Run the executable file or, if applicable, consult the readme file contained in a ZIP file.

What to do next

Walk through the instructions in the executable file to install the plugin.

Update the Plugin URLs

Update the plugin URLs if your domain name server (DNS) changes. At the time of your system installation, the DNS provides the basis for the plugin URL. If the DNS changes, the URL is not automatically updated.

Procedure

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

Step 2 Click **Find**.

Step 3 Click the plugin name that you want to update.

Step 4 In the **Custom URL** field, enter the updated URL for the plugin.

Step 5 Click **Save**.

CHAPTER 51

Configure Presence Redundancy Groups

Presence Redundancy Group Overview

A presence redundancy group is comprised of two IM and Presence Service nodes from the same cluster. Each node in the presence redundancy group monitors the status, or heartbeat, of the peer node. You can configure a presence redundancy group to provide both redundancy and recovery for IM and Presence Service clients and applications.

- Failover—Occurs in a presence redundancy group when one or more critical services fails on an IM and Presence Service node in the group or a node in the group fails. Clients automatically connect to the other IM and Presence Service node in that group.
- Fallback—Occurs when a fallback command is issued from the CLI or Cisco Unified Communications Manager during either of these conditions:
  - The failed IM and Presence Service node comes back into service and all critical services are running. The failed-over clients in that group reconnect with the recovered node when it becomes available.
  - The backup activated IM and Presence Service node fails due to a critical service failure, and the peer node is in the Failed Over state and supports the automatic recovery fallback.

For example, if you are using presence redundancy groups, Cisco Jabber clients will fail over to a backup IM and Presence Service node if the services or hardware fail on the local IM and Presence Service node. When the failed node comes online again, the clients automatically reconnect to the local IM and Presence Service node if you have configured automatic fallback. If you have not configured automatic fallback, you can manually initiate the fallback when the failed node comes online.

In addition to redundancy and recovery, presence redundancy groups also allow you to configure high availability for your cluster.

High Availability

The IM and Presence Service supports high availability for multiple-node deployments.

After you configure a presence redundancy group, you can enable high availability for the group. A pair of nodes is required for high availability. Each node has an independent database and set of users operating with a shared availability database that is able to support common users.

All IM and Presence Service nodes must belong to a presence redundancy group, which can consist of a single IM and Presence Service node or a pair of IM and Presence Service nodes.

You can configure high availability using two different modes:

- Balanced mode: This mode provides redundant high availability with automatic user load balancing and user failover in the event that one nodes fails because of component failure or power outage.
- Active/standby mode: The standby node automatically takes over for the active node if the active node fails. It does not provide automatic load balancing.

We recommend that you configure your IM and Presence Service deployments as high availability deployments. Although you are permitted to have both high availability and non-high availability presence redundancy groups configured in a single deployment, this configuration is not recommended.

Presence Redundancy Group Prerequisites

For deployments over the WAN, a minimum of 10 megabits per second of dedicated bandwidth is required for each IM and Presence Service cluster, with no more than an 80-millisecond round-trip latency. Any bandwidth less than this recommendation can adversely impact performance.

Presence Redundancy Group Task Flow

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

Procedure

	Command or Action	Purpose
Step 1	Verify Database Replication, on page 421	Ensure that database replication is setup in the IM and Presence Service cluster.
Step 2	Verify Services, on page 421	Make sure critical services are running on the nodes that you plan to add to a presence redundancy group.
Step 3	Configure a Presence Redundancy Group, on page 422	Provide redundancy and recovery for IM and Presence Service clients and applications.
Step 4	Configure Heartbeat Interval for Failover, on page 423	Optional. Each node in the presence redundancy group monitors the status, or heartbeat, of its

	Command or Action	Purpose
		peer node. You can configure the intervals by which each node monitors its peer.
Step 5	Enable High Availability, on page 424	Optional. Follow this procedure if you did not enable high availability when you configured the presence redundancy group.
Step 6	Configure User Assignment Mode, on page 425	Configure how you want the Sync Agent to distribute users across various nodes in the IM and Presence Service cluster. This setting affects how your system handles failover and load balancing.

Verify Database Replication

Ensure that database replication is setup in the IM and Presence Service cluster before you enable high availability for a presence redundancy group.

Procedure

Step 1 Start a CLI session using one of the following methods:

- From a remote system, use SSH to connect securely to the Cisco Unified Operating System. In your SSH client, enter your **`ssh`** ***`adminname@hostname`*** and enter your password.
- From a direct connection to the serial port, enter your credentials at the prompt that displays automatically.

Step 2 Execute the **utils dbreplication status** command to check for errors or mismatches in the database tables.

Step 3 Execute the **utils dbreplication runtimestate** command to check if the database replication is active on the node.

The output lists all the nodes and if database replication is set up and in a good state, the **replication setup** value for each node is **2**.

If a value other than 2 is returned, you must resolve the errors before proceeding.

What to do next

Verify Services, on page 421

Verify Services

Make sure critical services are running on the nodes that you plan to add to a presence redundancy group. Critical services must be running before you turn on high availability. If critical services are not running on either node, the presence redundancy group will go into a Failed state when you turn on high availability. If critical services are not running on one node, then that node fails over to the other node when you turn on high availability.

Before you begin

Verify Database Replication, on page 421

Procedure

Step 1 From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Network Services**.

Step 2 From the **Server** list, choose the appopriate node and click **Go**.

Step 3 In the **IM and Presence Services** area, ensure that the following services are started:

- **Cisco Client Profile Agent**
- **Cisco Sync Agent**
- **Cisco XCP Router**

Step 4 From the **Related Links** drop-down list, select **Control Center - Network Services** and click **Go**.

Step 5 In the **IM and Presence Services** area, ensure that the following services are started:

- **Cisco SIP Proxy**
- **Cisco Presence Engine**

What to do next

Configure a Presence Redundancy Group, on page 422

Configure a Presence Redundancy Group

Use Cisco Unified Communications Manager to configure redundancy for IM and Presence Service nodes.

Each presence redundancy group can contain two IM and Presence Service nodes. Each node can be assigned to only one presence redundancy group. Both nodes in the presence redundancy group must be on the same cluster and have the same IM and Presence Service database publisher node.

Before you begin

- Verify Services, on page 421
- Ensure that the IM and Presence Service nodes you are adding to a presence redundancy group are running the same software version.

Procedure

Step 1 From **Cisco Unified CM Administration**, choose **System** > **Presence Redundancy Groups**.

Step 2 Click **Add New**.

Step 3 Enter a unique name for the presence redundancy group.

You can enter a maximum of 128 alphanumeric characters, including underscore (_) and dash (-).

Step 4 Enter a description of the group.

You can enter a maximum of 128 alphanumeric characters including symbols, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), forward slash (\), or angle brackets (<>).

Step 5 Choose two different IM and Presence Service nodes in the **Presence Server** fields to assign them to the group.

Step 6 (Optional) Check the **Enable High Availability** check box to enable high availability for the presence redundancy group.

Step 7 Click **Save**.

What to do next

Configure Heartbeat Interval for Failover, on page 423

Configure Heartbeat Interval for Failover

Configure optional service parameters that determine the keep alive settings by which each peer in a presence redundancy group monitors the heartbeat (i.e., the status) of its peer node in order to confirm that the peer is active. A failover can be initiated if the peer node is unresponsive after a configured timer expires.

Note Cisco recommends that you use the default values for these service parameters. However, you can also reconfigure the values to suit your needs.

Procedure

Step 1 In Cisco Unified CM IM and Presence Administration, choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down, select an IM and Presence node

Step 3 From the **Service** drop-down, select **Cisco Server Recovery Manager (Active)**.

Step 4 Under **General Server Recovery Manager Parameters (Clusterwide)**, configure the clusterwide Keep Alive settings that each node in a Presence Redundancy Group uses to monitor monitor the heartbeat of its peer node. A failover can be initiated if the peer node is unresponsive.

- **Service Port**— This parameter specifies the port that Cisco Server Recovery Manager uses to communicate with its peer. The default is 22001.
- **Admin RPC Port**—This parameter specifies the port that Cisco Server Recovery Manager uses to provide admin rpc requests. The default is 20075.
- **Critical Service Delay**—This parameter specifies the duration in seconds that a critical service can be down before failover is initiated. The default is 90.
- **Enable Automatic Fallback**—This parameter specifies whether to do automatic fallback. In the event of a failover, the IM and Presence Service moves users automatically from the backup node to the primary node thirty minutes after the primary node returns to a healthy state. The default value is False.
- **Initialization Keep Alive (Heartbeat) Timeout**—This parameter specifies the duration in seconds that the heartbeat can be lost with the peer during initialization before failover is initiated. The default is 120.

- **Keep Alive (Heartbeat) Timeout**—This parameter specifies the duration in seconds that the heartbeat can be lost with the peer before failover is initiated. the default is 60.
- **Keep Alive (HeartBeat) Interval**—This parameter specifies the interval in seconds between keep alive (heart beat) messages being sent to the peer. The default is 15.

Step 5 Configure the following additional parameters, which tell CUPC 8.5 and higher clients how long to wait before attempting to relogin. Unlike the above parameters, these parameters must be configured separately for each cluster node.

- **Client Re-Login Lower Limit**—This parameter specifies the minimum number of seconds which CUPC 8.5 (and higher) should wait before attempting to re-login to this server. The default is 120.
- **Client Re-Login Upper Limit**—This parameter specifies the maximum number of seconds which CUPC 8.5 (and higher) should wait before attempting to re-login to this server. The default is 537.

Step 6 Click **Save**.

What to do next

If you did not enable high availability when you configured the presence redundancy group, Enable High Availability, on page 424 now.

Enable High Availability

⚠ **Caution** Failure to set up replication in the IM and Presence Service cluster and ensure that all critical services are running may result in an immediate failover when high availability is enabled for the presence redundancy group.

Before you begin

- Configure a Presence Redundancy Group, on page 422
- Ensure that replication is set up in the IM and Presence Service cluster.
- Ensure that all critical services are running.

Procedure

Step 1 From **Cisco Unified CM Administration**, choose **System** > **Presence Redundancy Groups**.

Step 2 Specify search criteria and then click **Find**.

Step 3 Choose the presence redundancy group that you configured.

Step 4 To enable high availability, check the **Enable High Availability** check box.

Step 5 Click **Save**.

Configure User Assignment Mode

Use this procedure to configure the way in which the sync agent distributes users to the nodes in the cluster. This setting helps to manage failover and load balancing.

Procedure

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

Step 2 In the **User Management Parameters** Area, choose one of the following options for the **User Assignment Mode for Presence Server** parameter:

- **Balanced**—This mode assigns users equally to each node in each subcluster and attempts to balance the total number of users equally across each node. This is the default option.
- **Active-Standby**—This mode assigns all users to the first node of the subcluster, leaving the secondary server as a backup.
- **None**—This mode results in no assignment of the users to the nodes in the cluster by the sync agent.

Step 3 Click **Save**.

Redundancy Interactions and Restrictions

Feature	Interaction
Adding Users	You cannot add new users to an IM and Presence Service cluster while one of the cluster nodes is in a failover state.
Multiple Device Messaging	The Multiple Device Messaging feature causes a delay with server recovery on the IM and Presence Service if failover occurs. If server failover occurs on a system where Multiple Device Messaging is configured, the failover times generally are twice as long as the times specified with the **Cisco Server Recovery** Manager service parameters.

Feature	Interaction
Push Notifications High Availability	High Availability is supported for Push Notifications deployments as of 11.5(1)SU3. If Push Notifications is enabled, and a node fails over, the following occurs for Cisco Jabber on iPhone and iPad clients: • For Cisco Jabber clients in foreground mode, the Jabber client logs in automatically to the backup node, which takes over until the main node recovers. There is no interruption in services, either when the backup node takes over, or when the main node recovers. • For Cisco Jabber clients in background mode, the backup node takes over, but there is a delay before any Push Notifications are sent. Because the Jabber client is in background mode, it does not have an active connection to the network so it doesn't log in automatically to the backup node. The backup node must recreate JSM sessions for all failed over users who were in background mode before any Push Notifications can be sent. The length of the delay depends on the system load. Testing has shown that for a 15,000 user OVA with users evenly distributed in an HA pair, it takes 10-20 minutes for Push Notifications to be sent following a failover. This delay is observed when the backup node takes over, and again after the main node recovers. **Note** In the event of a node failure or unexpected crash of the Cisco XCP Router, the user's IM session, including the IM history, is maintained without the need for any user action. However, if the Cisco Jabber on iPhone or iPad client was in suspended mode, it will be unable to retrieve unread messages that were queued on the server when it crashed.
Temporary presence status of a user	The temporary presence status of a user displays the stale presence status after Failover, Fallback, and user moves. This is because the subscription to temporary presence will be deleted and the user must re-subscribe to temporary presence to see the valid temporary presence status of the user. For example, If User A is subscribed to user B's temporary presence and a failover occurs on the IM and Presence node where User B is assigned, then user B displays offline to User A even after User B re-logins to the backup node. It is because the subscription to temporary presence of User B is deleted and User A is not aware of the deletion. User A must re-subscribe to temporary presence of User B again. When User A deletes search of User B from Jabber client, User A needs to wait at least 30 seconds before It tries to search the temporary presence of User B. If not, then User A sees the stale presence of User B. Jabber client must wait for at least 30 seconds between two searches for same user to get a valid temporary presence status.

Feature	Interaction
IM and Presence status	When a user is moved from one Presence Redundancy Group to another, The user has to be logged out from Jabber session, for the IM and Presence status to be visible in the current Presence Redundancy Group which the user has moved into.

Manual Failover, Fallback, and Recovery

Use Cisco Unified Communications Manager Administration to initiate a manual failover, fallback, and recovery for IM and Presence Service nodes in a presence redundancy group. You can also initiate these actions from Cisco Unified Communications Manager or IM and Presence Service using the CLI. See the *Command Line Interface Guide for Cisco Unified Communications Solutions* for details.

- Manual failover: When you initiate a manual failover, the Cisco Server Recovery Manager stops the critical services on the failed node. All users from the failed node are disconnected and must re-login to the backup node.

Note After a manual failover occurs, critical services will not be started unless we invoke manual fallback.

- Manual fallback: When you initiate a manual fallback, the Cisco Server Recovery Manager restarts critical services on the primary node and disconnects all users that had been failed over. Those users must then re-login to their assigned node.
- Manual recovery: When both nodes in the presence redundancy group are in a failed state and you initiate a manual recovery, the IM and Presence Service restarts the Cisco Server Recovery Manager service on both nodes in the presence redundancy group.

Initiate Manual Failover

You can manually initiate a failover of IM and Presence Service nodes in a presence redundancy group using Cisco Unified Communications Manager Administration.

Procedure

Step 1 Select **System** > **Presence Redundancy Groups**.

The **Find and List Presence Redundancy Groups** window displays.

Step 2 Select the presence redundancy group search parameters, and then click **Find**.

Matching records appear.

Step 3 Select the presence redundancy group that is listed in the **Find and List Presence Redundancy Group** window.

The **Presence Redundancy Group Configuration** window appears.

Step 4 Click **Failover** in the ServerAction field.

Note This button appears only when the server and presence redundancy group are in the correct states.

Initiate Manual Fallback

Use Cisco Unified Communications Manager Administration to manually initiate the fallback of an IM and Presence Service node in a presence redundancy group that has failed over. For more information about presence redundancy group node status, see topics related to node state, state change causes, and recommended actions.

Procedure

Step 1 Select **System** > **Presence Redundancy Groups**.

The **Find and List Presence Redundancy Groups** window displays.

Step 2 Select the presence redundancy group search parameters, and then click **Find**.

Matching records appear.

Step 3 Select the presence redundancy group that is listed in the **Find and List Presence Redundancy Group** window.

The **Presence Redundancy Group Configuration** window appears.

Step 4 Click **Fallback** in the ServerAction field.

Note This button appears only when the server and presence redundancy group are in the correct states.

Initiate Manual Recovery

A manual recovery is necessary when both nodes in the presence redundancy group are in the failed state. Use Cisco Unified Communications Manager Administration to manually initiate the recovery of IM and Presence Service nodes in a presence redundancy group that is in the failed state.

For more information about presence redundancy group node status, see topics related to node state, state change causes, and recommended actions.

Before you begin

A manual recovery is necessary when both nodes in the presence redundancy group are in the failed state. Use Cisco Unified Communications Manager Administration to manually initiate the recovery of IM and Presence Service nodes in a presence redundancy group that is in the failed state.

Procedure

Step 1 Select **System** > **Presence Redundancy Groups**.

The **Find and List Presence Redundancy Groups** window displays.

Step 2 Select the presence redundancy group search parameters, and then click **Find**.

Matching records appear.

Step 3 Select the presence redundancy group that is listed in the **Find and List Presence Redundancy Group** window.

The **Presence Redundancy Group Configuration** window appears.

Step 4 Click **Recover**.

Note This button appears only when the server and presence redundancy group are in the correct states.

Node State Definitions

Table 68: Presence Redundancy Group Node State Definitions

State	Description
Initializing	This is the initial (transition) state when the Cisco Server Recovery Manager service starts; it is a temporary state.
Idle	IM and Presence Service is in Idle state when failover occurs and services are stopped. In Idle state, the IM and Presence Service node does not provide any availability or Instant Messaging services. In Idle state, you can manually initiate a fallback to this node using the **Cisco Unified CM Administration** user interface.
Normal	This is a stable state. The IM and Presence Service node is operating normally. In this state, you can manually initiate a failover to this node using the **Cisco Unified CM Administration** user interface.
Running in Backup Mode	This is a stable state. The IM and Presence Service node is acting as the backup for its peer node. Users have moved to this (backup) node.
Taking Over	This is a transition state. The IM and Presence Service node is taking over for its peer node.
Failing Over	This is a transition state. The IM and Presence Service node is being taken over by its peer node.
Failed Over	This is a steady state. The IM and Presence Service node has failed over, but no critical services are down. In this state, you can manually initiate a fallback to this node using the **Cisco Unified CM Administration** user interface.

State	Description
Failed Over with Critical Services Not Running	This is a steady state. Some of the critical services on the IM and Presence Service node have either stopped or failed.
Falling Back	This is a transition state. The system is falling back to this IM and Presence Service node from the node that is running in backup mode.
Taking Back	This is a transition state. The failed IM and Presence Service node is taking back over from its peer.
Running in Failed Mode	An error occurs during the transition states or Running in Backup Mode state.
Unknown	Node state is unknown. A possible cause is that high availability was not enabled properly on the IM and Presence Service node. Restart the Server Recovery Manager service on both nodes in the presence redundancy group.

Node States, Causes, and Recommended Actions

You can view the status of nodes in a presence redundancy group on the **Presence Redundancy Group Configuration** window when you choose a group using the **Cisco Unified CM Administration** user interface.

Table 69: Presence Redundancy Group Node High-Availability States, Causes, and Recommended Actions

Node 1		Node 2		
State	**Reason**	**State**	**Reason**	**Cause/Recommended Actions**
Normal	Normal	Normal	Normal	Normal
Failing Over	On Admin Request	Taking Over	On Admin Request	The administrator initiated a manual failover from node 1 to node 2. The manual failover is in progress.
Idle	On Admin Request	Running in Backup Mode	On Admin Request	The manual failover from node 1 to node 2 that the administrator initiated is complete.
Taking Back	On Admin Request	Falling Back	On Admin Request	The administrator initiated a manual fallback from node 2 to node 1. The manual fallback is in progress.
Idle	Initialization	Running in Backup Mode	On Admin Request	The administrator restarts the SRM service on node 1 while node 1 is in “Idle” state.
Idle	Initialization	Running in Backup Mode	Initialization	The administrator either restarts both nodes in the presence redundancy group, or restarts the SRM service on both nodes while the presence redundancy group was in manual failover mode.

Node 1		Node 2		
State	**Reason**	**State**	**Reason**	**Cause/Recommended Actions**
Idle	On Admin Request	Running in Backup Mode	Initialization	The administrator restarts the SRM service on node 2 while node 2 is running in backup mode, but before the heartbeat on node 1 times out.
Failing Over	On Admin Request	Taking Over	Initialization	The administrator restarts the SRM service on node 2 while node 2 is taking over, but before the heartbeat on node1 times out.
Taking Back	Initialization	Falling Back	On Admin Request	The administrator restarts the SRM service on node 1 while taking back, but before the heartbeat on node 2 times out. After the taking back process is complete, both nodes are in Normal state.
Taking Back	Automatic Fallback	Falling Back	Automatic Fallback	Automatic Fallback has been initiated from node 2 to node 1 and is currently in progress.
Failed Over	Initialization or Critical Services Down	Running in Backup Mode	Critical Service Down	Node 1 transitions to Failed Over state when either of the following conditions occur: • Critical services come back up due to a reboot of node 1. • The administrator starts critical services on node 1 while node 1 is in Failed Over with Critical Services Not Running state. When node 1 transitions to Failed Over state the node is ready for the administrator to perform a manual fallback to restore the nodes in the presence redundancy group to Normal state.
Failed Over with Critical Services not Running	Critical Service Down	Running in Backup Mode	Critical Service Down	A critical service is down on node 1. IM and Presence Service performs an automatic failover to node 2. **Recommended Actions:** **1.** Check node 1 for any critical services that are down and try to manually start those services. **2.** If the critical services on node 1 do not start, then reboot node 1. **3.** When all the critical services are up and running after the reboot, perform a manual fallback to restore the nodes in the presence redundancy group to the Normal state.

Node 1		Node 2		
State	**Reason**	**State**	**Reason**	**Cause/Recommended Actions**
Failed Over with Critical Services not Running	Database Failure	Running in Backup Mode	Database Failure	A database service is down on node 1. IM and Presence Service performs an automatic failover to node 2. **Recommended Actions:** **1.** Reboot node 1. **2.** When all the critical services are up and running after the reboot, perform a manual fallback to restore the nodes in the presence redundancy group to the Normal state.
Running in Failed Mode	Start of Critical Services Failed	Running in Failed Mode	Start of Critical Services Failed	Critical services fail to start while a node in the presence redundancy group is taking back from the other node. **Recommended Actions.** On the node that is taking back, perform the following actions: **1.** Check the node for critical services that are down. To manually start these services, click **Recovery** in the **Presence Redundancy Group Configuration** window. **2.** If the critical services do not start, reboot the node. **3.** When all the critical services are up and running after the reboot, perform a manual fallback to restore the nodes in the presence redundancy group to the Normal state.
Running in Failed Mode	Critical Service Down	Running in Failed Mode	Critical Service Down	Critical services go down on the backup node. Both nodes enter the failed state. **Recommended Actions:** **1.** Check the backup node for critical services that are down. To start these services manually, click **Recovery** in the **Presence Redundancy Group Configuration** window. **2.** If the critical services do not start, reboot the node.

Node 1		Node 2		
State	**Reason**	**State**	**Reason**	**Cause/Recommended Actions**
Node 1 is down due to loss of network connectivity or the SRM service is not running.		Running in Backup Mode	Peer Down	Node 2 has lost the heartbeat from node 1. IM and Presence Service performs an automatic failover to node 2. **Recommended Action.** If node 1 is up, perform the following actions: **1.** Check and repair the network connectivity between nodes in the presence redundancy group. When you reestablish the network connection between the nodes, the node may go into a failed state. Click **Recovery** in the **Presence Redundancy Group Configuration** window to restore the nodes to the Normal state. **2.** Start the SRM service and perform a manual fallback to restore the nodes in the presence redundancy group to the Normal state. **3.** (If the node is down) Repair and power up node 1. **4.** When the node is up and all critical services are running, perform a manual fallback to restore the nodes in the presence redundancy group to the Normal state.
Node 1 is down (due to possible power down, hardware failure, shutdown, reboot)		Running in Backup Mode	Peer Reboot	IM and Presence Service performs an automatic failover to node 2 due to the following possible conditions on node 1: • hardware failure • power down • restart • shutdown **Recommended Actions:** **1.** Repair and power up node 1. **2.** When the node is up and all critical services are running, perform a manual fallback to restore the nodes in the presence redundancy group to the Normal state.

Node 1		Node 2		
State	**Reason**	**State**	**Reason**	**Cause/Recommended Actions**
Failed Over with Critical Services not Running OR Failed Over	Initialization	Backup Mode	Peer Down During Initialization	Node 2 does not see node 1 during startup. **Recommended Action:** When node1 is up and all critical services are running, perform a manual fallback to restore the nodes in the presence redundancy group to the Normal state.
Running in Failed Mode	Cisco Server Recovery Manager Take Over Users Failed	Running in Failed Mode	Cisco Server Recovery Manager Take Over Users Failed	User move fails during the taking over process. **Recommended Action:** Possible database error. Click **Recovery** in the **Presence Redundancy Group Configuration** window. If the problem persists, then reboot the nodes.
Running in Failed Mode	Cisco Server Recovery Manager Take Back Users Failed	Running in Failed Mode	Cisco Server Recovery Manager Take Back Users Failed	User move fails during falling back process. **Recommended Action:** Possible database error. Click **Recovery** in the **Presence Redundancy Group Configuration** window. If the problem persists, then reboot the nodes.
Running in Failed Mode	Unknown	Running in Failed Mode	Unknown	The SRM on a node restarts while the SRM on the other node is in a failed state, or an internal system error occurs. **Recommended Action:** Click **Recovery** in the **Presence Redundancy Group Configuration** window. If the problem persists, then reboot the nodes.
Backup Activated	Auto Recover Database Failure	Failover Affected Services	Auto Recovery Database Failure.	The database goes down on the backup node. The peer node is in failover mode and can take over for all users in the presence redundancy group. Auto-recovery operation automatically occurs and all users are moved over to the primary node.
Backup Activated	Auto Recover Database Failure	Failover Affected Services	Auto Recover Critical Service Down	A critical service goes down on the backup node. The peer node is in failover mode and can take over for all users in the presence redundancy group. Auto-recovery operation automatically occurs and all users are moved over to the peer node.

Node 1		Node 2		
State	**Reason**	**State**	**Reason**	**Cause/Recommended Actions**
Unknown		Unknown		Node state is unknown. A possible cause is that high availability was not enabled properly on the IM and Presence Service node. **Recommended Action:** Restart the Server Recovery Manager service on both nodes in the presence redundancy group.

CHAPTER 52

Configure Cisco Unity Connection for Voicemail and Messaging

Cisco Unity Connection

As you start configuring your voicemail and messaging system, be aware of the options that you have for adding users, enabling features, and integrating Cisco Unified Communications Manager with Cisco Unity Connection.

When integrated with Cisco Unified Communications Manager, Cisco Unity Connection (the voicemail and messaging system) provides voice-messaging features for users that you configure manually, through AXL services, or through LDAP integration. After receiving voice messages in their mailboxes, users receive message-waiting lights on their phones. Users can retrieve, listen to, reply to, forward, and delete their messages by accessing the voice-messaging system with an internal or external call.

Your system supports both directly connected and gateway-based messaging systems. Directly connected voice-messaging systems communicate with Cisco Unified Communications Manager by using a packet protocol. A gateway-based voice-messaging system connects to Cisco Unified Communications Manager through analog or digital trunks that then connect to Cisco gateways.

When you integrate Unified Communications Manager and Cisco Unity Connection, you can configure the following features for your users:

- Call forward to personal greeting

- Call forward to busy greeting

- Caller ID

- Easy message access (a user can retrieve messages without entering an ID; Cisco Unity Connection identifies a user based on the extension from which the call originated; a password may be required)

- Identified user messaging (Cisco Unity Connection automatically identifies a user who leaves a message during a forwarded internal call, based on the extension from which the call originated)

- Message waiting indication (MWI)

- The configuration of a secure SIP trunk integration between a Cisco Unified Communications Manager and Cisco Unity Connection server requires that the Cisco Unified Communications Manager cluster is configured in mixed mode.

Cisco Unified Communications Manager interacts with Cisco Unity Connection through one of the following interfaces:

- SIP Trunk—You can integrate Cisco Unity Connection and Unified Communications Manager by using SIP. Instead of multiple SCCP ports involved with traditional integrations, SIP uses a single trunk per Unity Connection server. The SIP integration eliminates the requirement to configure directory numbers for Voicemail Ports and message-waiting indicators (MWI).
- SCCP Protocol—You configure the interface to directly connected voice-messaging systems by creating voicemail ports. These establish a link between Unified Communications Manager and Cisco Unity Connection.

  To handle multiple, simultaneous calls to a voice-messaging system, you create multiple voicemail ports and place the ports in a line group and the line group in a route/hunt list.

  Cisco Unified Communications Manager generates SCCP messages, which are translated by Cisco Unity Connection. The voicemail system sends message-waiting indications (MWIs) by calling a message-waiting on and off number.

  When you configure security for voicemail ports and Cisco Unity SCCP devices, a TLS connection (handshake) opens for authenticated devices after each device accepts the certificate of the other device; likewise, the system sends SRTP streams between devices; that is, if you configure the devices for encryption.

  When the device security mode is set to authenticated or encrypted, the Cisco Unity TSP connects to Cisco Unified Communications Manager through the Unified Communications Manager TLS port. When the security mode is nonsecure, the Cisco Unity TSP connects to Cisco Communications Manager through the Unified Communications Manager SCCP port.

For more information about configuring Cisco Unity Connection to integrate with your system, see the *Cisco Unified Communications Manager SCCP Integration Guide for Cisco Unity Connection* or the *Cisco Unified Communications Manager SIP Trunk Integration Guide for Cisco Unity Connection* at http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-installation-and-configuration-guides-list.html.

Cisco Unity Connection for Voicemail and Messaging Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure Cisco Unity Connection for Voicemail and messaging.	To configure Cisco Unity Connection, see the *Cisco Unified Communications Manager SCCP Integration Guide* for Cisco Unity Connection or the *Cisco Unified Communications Manager SIP Trunk Integration Guide for Cisco Unity*

	Command or Action	Purpose
		Connection at http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-installation-and-configuration-guides-list.html
Step 2	Enable PIN Synchronization , on page 439	Optional. Use this procedure to enable a common PIN synchronization so that

Enable PIN Synchronization

Use this procedure to enable PIN synchronization so that the end users can log in to Extension Mobility, Conference Now, Mobile Connect, and the Cisco Unity Connection Voicemail using the same PIN.

Note The pin synchronization between Cisco Unity Connection and Cisco Unified Communications Manager is successful, only when Cisco Unified Communications Manager publisher database server is running and completes its database replication. Following error message is displayed when the pin synchronization fails on Cisco Unity Connection: `Failed to update PIN on CUCM. Reason: Error getting the pin.`

If the PIN Synchronization is enabled and the end user changes the pin, then pin is updated in Cisco Unified Communications Manager. This happens only when the pin update is successful in at least one of the configured Unity Connection Application servers.

Note For PIN Synchronization to take effect, administrators must force the users to change their PIN after successfully enabling the feature.

Before you begin

This procedure assumes that you already have your application server connection to Cisco Unity Connection setup. If not, for more information on how to add a new application server, see the Related Topics section.

To enable PIN Synchronization feature, you need to first upload a valid certificate for the Cisco Unity Server connection from the Cisco Unified OS Administration page to the Cisco Unified Communications Manager tomcat-trust. For more information on how to upload the certificate, see the "Manage Security Certificates" chapter in the *Administration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

The user ID in the Cisco Unity Connection Server must match the user ID in Cisco Unified Communications Manager.

Procedure

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

Step 2 Select the application server that you set up for Cisco Unity Connection.

Step 3 Check the **Enable End User PIN Synchronization** check box.

Step 4 Click **Save**.

Related Topics

Configure Application Servers, on page 412

CHAPTER 53

Configure Cisco Unified Contact Center Enterprise

Cisco Unified Contact Center Enterprise

You can use Cisco Unified Contact Center Enterprise (Unified CCE) in your system to integrate intelligent call routing, network-to-desktop computer telephony integration (CTI), and multichannel contact management to contact center agents over an IP network. Unified CCE combines software IP automatic call distribution (ACD) with Cisco Unified Communications so that you can rapidly deploy an advanced, distributed contact center.

For detailed tasks about how to configure Unified CCE to integrate with your system, see the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

CHAPTER 54

Configure Cisco Unified Contact Center Express

Cisco Unified Contact Center Express

Cisco Unified Contact Center Express (Unified CCX) provides your system with the features of a large contact center packaged into a single- or dual-server deployment. Unified CCX scales up to 400 concurrent agents, 42 supervisors, 150 agent groups, and 150 skill groups. It includes email, chat, outbound calling, inbound calling, workforce optimization, and reporting.

Unified CCX works with Unified Communications Manager, which manages all contact center calls on behalf of Unified CCX. When a call is placed to your help desk, your call system recognizes that the number is destined for the Unified CCX application server. With this configuration, Unified CCX receives the incoming call and handles the request based on the extension number that was dialed. The script plays prompts, collects digits and, if necessary, uses the information from the caller to select an appropriate agent. If an assigned agent is not available, the call is put into an appropriate queue and a recorded message or music is streamed to the caller. As soon as an agent is available, Unified CCX instructs Unified Communications Manager to call the agent's phone.

When the agent picks up, relative call context is provided in the agent's desktop application. This step ensures that agents have the proper information in front of them to support the customer.

For detailed tasks about how to configure Unified CCX to integrate with your system, see the *Cisco Unified CCX Administration Guide* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-installation-and-configuration-guides-list.html.

CHAPTER 55

Configure CTI Applications

CTI Applications Overview

You can use Computer Telephony Integration (CTI) to take advantage of computer-processing functions while making, receiving, and managing telephone calls. CTI applications allow you to perform such tasks as retrieving customer information from a database using a caller ID, or to work with the information gathered by an Interactive Voice Response (IVR) system to route a customer's call, along with their information, to the appropriate customer service representative.

Applications that want to terminate media for calls at route points must specify the media and port for the call on a per-call basis. CTI applications can terminate media on CTI ports and CTI route points using either static or dynamic IP addresses and port numbers.

This chapter describes how to configure Cisco Unified Communications Manager to work with CTI applications. For information about how to configure specific applications, see the *Feature Configuration Guide for Cisco Unified Communications Manager.*

Some of the Cisco CTI applications available are:

- Cisco IP Communicator: A desktop application which turns your computer into a full-feature telephone with the added advantages of call tracking, desktop collaboration, and one-click dialing from online directories.
- Cisco Unified Communications Manager Auto-Attendant: Works with Unified Communications Manager to receive calls on specific telephone extensions and to allow the caller to choose an appropriate extension.
- Cisco Web Dialer: Allows Cisco IP Phone users to make calls from web and desktop applications.
- Cisco Unified Communications Manager Assistant: Enables managers and their assistants to work together more effectively. The feature comprises a call-routing service, enhancements to phone capabilities for the manager and the assistant, and assistant console interfaces that are primarily used by the assistant.

Note To determine which Unified Communications Manager CTI applications support SIP IP phones, see the application-specific documentation.

CTI Route Points Overview

A CTI route point virtual device can receive multiple, simultaneous calls for application-controlled redirection. You can configure one or more lines on a CTI route point that users can call to access the application. Applications can answer calls at a route point and can also redirect calls to a CTI port or IP phone. When a CTI application requests to redirect a call by using the Redirect API, Cisco Unified Communications Manager uses the configuration for the line/device calling search space for the redirected party.

With CTI route points you can:

- Answer a call
- Make and receive multiple active calls
- Redirect a call
- Hold a call
- Unhold a call
- Drop a call

CTI Redundancy on Cisco Unified Communications Manager

When a Unified Communications Manager node in a cluster fails, the CTIManager recovers the affected CTI ports and route points by reopening these devices on another Unified Communications Manager node. If an application has a phone device open, the CTIManager also reopens the phone when the phone fails over to a different Unified Communications Manager. If the Cisco IP Phone does not fail over to a different Unified Communications Manager, the CTIManager cannot open the phone or a line on the phone. The CTIManager uses the Unified Communications Manager group that is assigned to the device pool to determine which Unified Communications Manager to use to recover the CTI devices and phones that the applications opened.

CTI Redundancy on CTIManager

When a CTIManager fails, the applications that are connected to the CTIManager can recover the affected resources by reopening these devices on another CTIManager. An application determines which CTIManager to use on the basis of CTIManagers that you defined as primary and backup when you set up the application (if supported by the application). When the application connects to the new CTIManager, it can reopen the devices and lines that previously opened. An application can reopen a Cisco IP Phone before the phone rehomes to the new Unified Communications Manager; however, it cannot control the phone until the rehoming completes.

Note The applications do not rehome to the primary CTIManager when it comes back in service. Applications fail back to the primary CTIManager if you restart the application or if the backup CTIManager fails.

CTI Redundancy for Application Failure

When an application (TAPI/JTAPI or an application that directly connects to the CTIManager) fails, the CTIManager closes the application and redirects unterminated calls at CTI ports and route points to the configured call forward on failure (CFOF) number. The CTIManager also routes subsequent calls into those CTI ports and route points to the configured Call Forward No Answer (CFNA) number until the application recovers and reregisters those devices.

CTI Applications Prerequisites

You must have device pools configured before you can configure Cisco Unified Communications Manager for CTI Applications.

Add and configure IP phones for each CTI application. For further information on adding and configuring IP Phones see, Cisco Unified IP Phones.

Configure the end users and application users that will use CTI applications.

Computer Telephony Integration (CTI) provides IP address information through the JTAPI and TAPI interfaces, which can support IPv4 and IPv6 addresses. If you want to support IPv6 addresses, make sure that your applications are using a JTAPI /TAPI client interface version that supports IPv6.

Configure CTI Applications Task Flow

To configure Cisco Unified Communications Manager for CTI applications follow these tasks.

Procedure

	Command or Action	Purpose
Step 1	Activate the CTIManager Service, on page 448	Activate the CTIManager service on the appropriate servers, if not already activated.
Step 2	Configure CTIManager and Cisco Unified Communications Manager Service Parameters, on page 448	Configure CTIManager advanced clusterwide service parameters that are used in conjunction with the CTI Super Provider capability.
Step 3	To configure CTI Route Points perform the following procedure: • Configure CTI Route Points, on page 449 • Configure New Call Accept Timer, on page 449 • Configure Simultaneous Active Calls, on page 450 • Synchronize CTI Route Point, on page 450	Configure one or more CTI route point virtual devices which can receive multiple, simultaneous calls for application-controlled redirection.
Step 4	Configure CTI Device Directory Number, on page 451	Configure the directory number for the CTI device.
Step 5	Associate Devices with Groups, on page 451	Associate all devices that the application will use for application users and end users with the appropriate Cisco Unified Communications Manager group (via the device pool).

	Command or Action	Purpose
Step 6	Add End Users and Application Users, on page 451	Allow a CTI application to control any CTI-controllable devices that are configured in the Cisco Unified Communications Manager system by adding the end users and application users to the Standard CTI Enabled user group.
Step 7	(Optional) Configure CTI Redundancy for Application Failure, on page 453	To define the interval at which CTIManager expects to receive a message from an application within two consecutive intervals.

Activate the CTIManager Service

Procedure

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

Step 2 Choose the node from the **Server** drop-down list.

Step 3 Check the **Cisco CTIManager** check box in the CM Services section.

Step 4 Click **Save**.

Configure CTIManager and Cisco Unified Communications Manager Service Parameters

Configure CTIManager advanced clusterwide service parameters that are used in conjunction with the CTI Super Provider capability.

Note If the configured limits are exceeded, CTI generates alarms, but the applications continue to operate with the extra devices.

Procedure

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

Step 2 Choose the node from the **Server** drop-down list.

Step 3 Choose Cisco CTIManager (Active) from the **Service** drop-down list.

Step 4 On the **Service Parameter Configuration** window, click **Advanced**.

Step 5 In the **Maximum Devices Per Provider** field, enter the maximum number of devices that a single CTI application can open. The default is 2000 devices.

Step 6 In the Maximum Devices Per Node field, enter the maximum number of devices that all CTI applications can open on any CTIManager node in the Unified Communications Manager system. The default is 800 devices.

Step 7 Click **Save**.

Configure CTI Route Points Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure CTI Route Points, on page 449	Add a new, or modify an existing CTI route point.
Step 2	Configure New Call Accept Timer, on page 449	Configure the New Call Accept Timer so that when a call arrives at a route point, the application will handle (accept, answer, redirect) it within the time specified.
Step 3	Configure Simultaneous Active Calls, on page 450	Configure the number of simultaneous active calls on the route point.
Step 4	**Optional**: Synchronize CTI Route Point, on page 450	Synchronize a CTI route point with the most recent configuration changes, 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.)

Configure CTI Route Points

Add a new, or modify an existing CTI route point.

Procedure

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

Step 2 Perform one of the following tasks:

- Click **Add New**, to add a new gateway.
- Click **Find** and select a CTI route point from the resulting list to modify the settings for an existing CTI route point, enter search criteria.

Step 3 Configure the fields in the **CTI Route Point Configuration** window. For more information on the fields and their configuration options, see the system Online Help..

Step 4 Click **Save**.

Configure New Call Accept Timer

Configure the New Call Accept Timer so that when a call arrives at a route point, the application will handle (accept, answer, redirect) it within the time specified.

Procedure

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

Step 2 Choose the node from the **Server** drop-down list.

Step 3 Choose **Cisco CallManager (Active)** from the Service drop-down list.

Step 4 In the **CTI New Call Accept Timer** field, specify the time that you want to allow for a call to be answered. The default value is 4.

Step 5 Click **Save**.

Configure Simultaneous Active Calls

Configure the number of simultaneous active calls on the route point.

Note If you are planning to use a TAPI application to control CTI port devices by using the Cisco CallManager Telephony Service Provider (TSP), you may only configure one line per CTI port device.

Procedure

Step 1 From Cisco Unified CM Administration, click **Call Routing** > **Directory Number**.

Step 2 On the Directory Number Configuration window, click **Add New**.

Step 3 Fill in the required fields.

Step 4 Click **Save**.

Synchronize CTI Route Point

Synchronize a CTI route point with the most recent configuration changes, 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 From Cisco Unified CM Administration, click **Device** > **CTI Route Point**.

Step 2 On the **Find and List CTI Route Points** window, click **Find** to display the list of CTI route points.

Step 3 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 4 Click **Apply Config to Selected**.

Step 5 Click **OK**.

Configure CTI Device Directory Number

Configure the directory number for the CTI device.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Directory Number**.

Step 2 On the **Find and List Directory Numbers** window, click **Add New**.

Step 3 On the **Directory Number Configuration** window, and enter the required fields.

Step 4 Click **Save**.

Associate Devices with Groups

Associate all devices that the application will use for application users and end users with the appropriate Cisco Unified Communications Manager group (via the device pool).

Procedure

Step 1 From Cisco Unified CM Administration, click **User Management** > **Application User**.

Step 2 On the **Find and List Application Users** window, click **Add New**. This brings you to the Application User Configuration window.

Step 3 In the Device Information pane, associate your devices by moving them from the Available Devices list to the Controlled Devices list.

Step 4 Click **Save**.

Step 5 To Associate Devices for end users, click **User Management** > **End User**.

Step 6 Repeat steps 2 - 4.

Add End Users and Application Users

Allow a CTI application to control any CTI-controllable devices that are configured in the Cisco Unified Communications Manager system by adding the end users and application users to the Standard CTI Enabled user group.

Procedure

Step 1 From Cisco Unified CM Administration, click **User Management** > **User Settings** > **Access Control Group**.

Step 2 On the **Find and List Access Control Groups** window, click **Find** to display the current list of access control groups.

Step 3 Click **Standard CTI Enabled**, this brings you to the Access Control Group Configuration window for this group. Ensure all CTI users are in the Standard CTI Enabled user group. See Access Control Group Configuration Options, for a full list of available groups and their capabilities.

Step 4 If you want to add end users, click **Add End Users to Group** or, if you want to add application users, click **Add App Users to Group**.

Step 5 Click **Find**, to display the list of current users.

Step 6 Check the users you want to assign to the Standard CTI Enabled user group.

Step 7 Click **Add Selected**.

Access Control Group Configuration Options

Note The CTI application must support the specified user group to which it is assigned.

Note Cisco recommends that users who are associated with the Standard CTI Allow Control of All Devices user group also be associated with the Standard CTI Secure Connection user group.

Note You must add the particular device under **Controlled Devices** for all the roles, listed in the following table, to work properly.

Field	Description
Standard CTI Allow Call Monitoring	This user group allows an application to monitor calls.
Standard CTI Allow Call Park Monitoring	This user group allows an application to receive a notification when calls are parked/unparked to all Call Park directory numbers.
Standard CTI Allow Call Recording	This user group allows an application to record calls.
Standard CTI Allow Calling Number Modification	This user group allows an application to modify the calling party number in supported CTI applications.
Standard CTI Allow Control of All Devices	This user group allows an application to control or monitor any CTI-controllable device in the system.
Standard CTI Allow Reception of SRTP Key Material	This user group allows an application to receive information that is necessary to decrypt encrypted media streams. This group typically gets used for recording and monitoring purposes.
Standard CTI Enabled	This user group, which is required for all CTI applications, allows an application to connect to Cisco Unified Communications Manager and to access CTI functionality.
Standard CTI Secure Connection	Inclusion into this group requires that the application has a secure (TLS) CTI connection to Cisco Unified Communications Manager and that the Cisco Unified Communications Manager cluster has security enabled.

Configure CTI Redundancy for Application Failure

To define the interval at which CTI Manager expects to receive a message from an application within two consecutive intervals.

Procedure

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

Step 2 Choose the node from the **Server** drop-down list.

Step 3 Choose **Cisco CTIManager (Active)** from the **Service** drop-down list.

Step 4 On the **Service Parameter Configuration** window, click **Advanced**.

Step 5 In the **Application Heartbeat Minimum Interval** field, enter the time for the minimum interval. The default is 5.

Step 6 In the **Application Heartbeat Maximum Interval** field, enter the time for the maximum interval. The default is 3600.

Step 7 Click **Save**.

CHAPTER 56

Configure Cisco TelePresence

Cisco TelePresence

Cisco TelePresence Conductor

The Cisco TelePresence Conductor simplifies multiparty video communications. The conductor lies within a video communications network, working in conjunction with one or more conference bridges and one or more call control devices (either Cisco TelePresence Video Communication Servers (VCSs) or Unified Communications Managers). It allows the video network to be configured so you can spontaneous or rendezvous conferences can be easily provisioned, initiated, accessed, and managed.

For ad hoc conferences, a SIP trunk is used from Unified Communications Manager to TelePresence Conductor. Set up the relevant TelePresence Conductor Location's ad hoc IP address as the destination of a SIP trunk on Unified Communications Manager. Ad hoc calls for that location can then be routed down that SIP trunk.

For rendezvous conferences a separate SIP trunk is used from Unified Communications Manager to TelePresence Conductor. Set up the relevant TelePresence Conductor Location's rendezvous IP address as the destination of a SIP trunk on Unified Communications Manager. Rendezvous calls for that location can then be routed down that SIP trunk.

For detailed tasks about how to configure your system with Cisco TelePresence Conductor, see the deployment guides at http://www.cisco.com/c/en/us/support/conferencing/telepresence-conductor/products-installation-and-configuration-guides-list.html.

Cisco TelePresence Conference Bridges

The Cisco TelePresence Server is a scalable videoconferencing bridge that works with Cisco Unified Communications Manager to bring multiparty video to your unified communications deployments. It offers flexible video, audio, and content-sharing capabilities for multiparty videoconferencing. You can easily create, launch, and join meetings using standards-based video endpoints, mobile devices, Cisco Webex clients, and third-party video endpoints.

The Cisco TelePresence Multipoint Control Unit (MCU) is a high definition multipoint video conferencing bridge. It delivers up to 1080p at 30 frames per second, full continuous presence for all conferences, full transcoding, and is ideal if you want to configure mixed high definition endpoint environments. The Cisco

TelePresence MCU supports SIP as the signaling call control protocol. It has a built in Web Server that allows for complete configuration, control, and monitoring of the system and conferences.

The Cisco TelePresence Server is primarily controlled by Cisco TelePresence Conductor. For detailed tasks about how to configure these conference bridges within your system, see the deployment guides at http://www.cisco.com/c/en/us/support/conferencing/telepresence-conductor/products-installation-and-configuration-guides-list.html.

Cisco TelePresence Video Communication Server

The Cisco TelePresence Video Communication Server (VCS) simplifies session management and control of telepresence conferences. The VCS delivers provides secure communications, simplified large-scale provisioning, and network administration in conjunction with Cisco TelePresence Management Suite (Cisco TMS). The VCS interworks with Cisco Unified Communications Manager (Unified Communications Manager), bringing rich telepresence services to your system.

For detailed tasks about how to configure Cisco TelePresence VCS to integrate with your system, see the deployment guides at http://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-vcs/products-installation-and-configuration-guides-list.html.

CHAPTER 57

Configure Cisco Jabber

Configure Cisco Jabber

Cisco Jabber is a suite of Unified Communications applications that allow seamless interaction with your contacts from anywhere. Cisco Jabber offers IM, presence, audio and video calling, voicemail, and conferencing.

The applications in the Cisco Jabber family of products are:

- Cisco Jabber for Windows
- Cisco Jabber for Mac
- Cisco Jabber for iPhone and iPad
- Cisco Jabber for Android
- Cisco Jabber Softphone for VDI

For more information about the Cisco Jabber suite of products, see https://www.cisco.com/go/jabber or https://www.cisco.com/c/en/us/products/unified-communications/jabber-softphone-for-vdi/index.html .

For detailed information about how to configure your system to work with Cisco Jabber, see the *Cisco Jabber Deployment and Installation Guide* at http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html.

OAuth Refresh Logins for Cisco Jabber

Cisco Jabber clients, as of Jabber Release 11.9, can use OAuth Refresh Logins to authenticate with Cisco Unified Communications Manager and the IM and Presence Service. This feature improves the user experience for Cisco Jabber by providing the following benefits:

- After an initial login, provides seamless access to resources over the life of the refresh token.
- Removes the need for Cisco Jabber clients to re-authenticate frequently.

- Provides consistent login behavior in SSO and non-SSO environments.

With OAuth Refresh Logins, Cisco Unified Communications Manager issues clusterwide access tokens and refresh tokens that use the OAuth standard. Cisco Unified Communications Manager and IM and Presence Service use the short-lived access tokens to authenticate Jabber (the default lifespan for an access token is 60 minutes). The longer-lived refresh tokens provide Jabber with new access tokens as the old access tokens expire. So long as the refresh token is valid the Jabber client can obtain new access tokens dynamically without the user having to re-enter credentials (the default refresh token lifespan is 60 days).

All access tokens are encrypted, signed, and self-contained using the JWT format (RFC7519). Refresh tokens are signed, but are not encrypted.

Note OAuth authentication is also supported by Cisco Expressway and Cisco Unified Connection. Make sure to check with those products for compatible versions. Refer to Cisco Jabber documentation for details on Jabber behavior if you are running incompatible versions.

Authentication Process

When a Cisco Jabber client authenticates, or when a refresh token is sent, Cisco Unified Communications Manager checks the following conditions, each of which must be met for authentication to succeed.

- Verifies the signature.
- Decrypts and verifies the token.
- Verifies that the user is an active user. For example, an LDAP-synced user whom is subsequently removed from the external LDAP directory, will remain in the database, but will appear as an inactive user in the User Status of End User Configuration.
- Verifies that the user has access to resources, as provided by their role, access control group, and user rank configuration.

Note For backward compatibility, older Jabber clients and supporting applications such as the Cisco Unified Real-Time Monitoring Tool can authenticate using the implicit grant flow model, which is enabled by default.

Cisco Jabber Prerequisites

The following prerequisites exist for Cisco Jabber integration:

- If you want to use OAuth Refresh Logins, you must enable the feature on all of your UC systems. Make sure that your Cisco Jabber, Cisco Unity Connection and Cisco Expressway deployments support OAuth refresh logins.
- If you are deploying Push Notifications for Cisco Jabber on iPhone or iPad, refer to Push Notifications for *Cisco Jabber on iPhone and iPad with Cisco Unified Communications Manager* for a complete list of Push Notifications prerequisites and configurations.

Cisco Jabber Configuration Task Flow

Complete these tasks in Cisco Unified Communications Manager to configure the system for Cisco Jabber clients.

Procedure

	Command or Action	Purpose
Step 1	Configure Refresh Logins for Cisco Jabber, on page 460	Enable Cisco Unified Communications Manager and the IM and Presence Service to use OAuth refresh logins for Cisco Jabber authentication. **Note** OAuth Refresh Logins are disabled by default in Cisco Unified Communications Manager, but are disabled by default in Cisco Expressway. If you choose not to enable the feature in Cisco Unified Communications Manager, you must disable the feature in Cisco Expressway or a configuration mismatch will result.
Step 2	Configure Push Notifications, on page 625	If you are deploying Cisco Jabber for iPhone or iPad, enable Push Notifications on your system. **Note** Push Notifications is a mandatory configuration for Cisco Jabber on iPhone and iPad. The feature is not required for Android, Mac, or Windows users.
Step 3	Configure additional Cisco Jabber settings.	Refer to the *On-Premises Deployment for Cisco Jabber* guide for your platform. • Android—http://www.cisco.com/c/en/us/support/unified-communications/jabber-android/products-installation-guides-list.html • iPhone or iPad—http://www.cisco.com/c/en/us/support/customer-collaboration/jabber-iphone-ipad/products-installation-guides-list.html • Mac—http://www.cisco.com/c/en/us/support/unified-communications/jabber-mac/products-installation-guides-list.html

	Command or Action	Purpose
		• Windows—http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html

Configure Refresh Logins for Cisco Jabber

Use this procedure to enable Refresh Logins with OAuth access tokens and refresh tokens in Unified Communications Manager. OAuth Refresh Logins provides a streamlined login flow that doesn't require users to re-login after network changes.

Note To ensure compatibility, make sure that the various Unified Communications components of your deployment, such as Cisco Jabber, Cisco Expressway and Cisco Unity Connection, support refresh logins. Once OAuth Refresh Logins are enabled, disabling the feature will require you to reset all Cisco Jabber clients.

Before you begin

You must be running a minimum release of Cisco Jabber 11.9. Older versions of Jabber will use the Implicit Grant Flow authentication model from previous releases.

Procedure

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

Step 2 Under **SSO Configuration**, do either of the following:

- Choose the **OAuth with Refresh Login Flow** enterprise parameter to **Enabled** to enable OAuth Refresh Logins.
- Choose the **OAuth with Refresh Login Flow** enterprise parameter to **Disabled** to disable OAuth Refresh Logins. This is the default setting.

Step 3 If you enabled OAuth Refresh Logins, configure expiry timers for access tokens and refresh tokens by configuring the following enterprise parameters:

- **OAuth Access Token Expiry Timer (minutes)**—This parameter specifies the expiry timer, in minutes, for individual OAuth access tokens. The OAuth access token is invalid after the timer expires, but the Jabber client can request and obtain new access tokens without the user having to re-authenticate so long as the refresh token is valid. The valid range is from 1 - 1440 minutes with a default of 60 minutes.
- **OAuth Refresh Token Expiry Timer (days)**—This parameter specifies the expiry timer, in days, for OAuth refresh tokens. After the timer expires, the refresh token becomes invalid and the Jabber client must re-authenticate to get a new refresh token. The valid range is from 1 - 365 days with a default of 60 days.

Step 4 Click **Save**.

Note Once you've saved the configuration, reset all Cisco Jabber and Webex clients.

Regenerate Keys for OAuth Refresh Logins

Use this procedure to regenerate both the encryption key and the signing key using the Command Line Interface. Complete this task only if the encryption key or signing key that Cisco Jabber uses for OAuth authentication with Unified Communications Manager has been compromised. The signing key is asymmetric and RSA-based whereas the encryption key is a symmetric key.

After you complete this task, the current access and refresh tokens that use these keys become invalid.

We recommend that you complete this task during off-hours to minimize the impact to end users.

The encryption key can be regenerated only via the CLI below, but you can also use the Cisco Unified OS Administration GUI of the publisher to regenerate the signing key. Choose **Security** > **Certificate Management**, select the **AUTHZ** certificate, and click **Regenerate**.

Procedure

Step 1 From the Unified Communications Manager publisher node, log in to the **Command Line** Interface .

Step 2 If you want to regenerate the encryption key:

a) Run the `set key regen authz encryption` command.
b) Enter `yes`.

Step 3 If you want to regenerate the signing key:

a) Run the `set key regen authz signing` command.
b) Enter `yes`.
The Unified Communications Manager publisher node regenerates keys and replicates the new keys to all Unified Communications Manager cluster nodes, including any local IM and Presence Service nodes.

You must regenerate and sync your new keys on all of your UC clusters:

- IM and Presence central cluster—If you have an IM and Presence centralized deployment, your IM and Presence nodes are running on a separate cluster from your telephony. In this case, repeat this procedure on the Unified Communications Manager publisher node of the IM and Presence Service central cluster.
- Cisco Expressway or Cisco Unity Connection—Regenerate the keys on those clusters as well. See your Cisco Expressway and Cisco Unity Connection documentation for details.

Note Restart the Cisco CallManager Service on all nodes in the cluster after the keys are reassigned.

Revoke Existing OAuth Refresh Tokens

Use an AXL API to revoke existing OAuth refresh tokens. For example, if an employee leaves your company, you can use this API to revoke that employee's current refresh token so that they cannot obtain new access tokens and will no longer be able to log in to the company account. The API is a REST-based API that is protected by AXL credentials. You can use any command-line tool to invoke the API. The following command provides an example of a cURL command that can be used to revoke a refresh token:

```
curl -k -u "admin:password" https://<UCMaddress:8443/ssosp/token/revoke?user_id=<end_user>
```

where:

- `admin:password` is the login ID and password for the Cisco Unified Communications Manager administrator account.
- `UCMaddress` is the FQDN or IP address of the Cisco Unified Communications Manger publisher node.
- `end_user` is the user ID for the user for whom you want to revoke refresh tokens.

Cisco Jabber Interactions and Restrictions

Feature	Interactions
Graceful registration	Graceful registration covers dual registration attempts from two Cisco Jabber clients with the same device name (for example, Jabber running on both an office laptop and a home office laptop). The feature de-registers the initial registration automatically so that the second registration can proceed. The de-registered Jabber client does not re-register. Graceful registration is supported automatically for Cisco Jabber, except when Jabber is deployed in a Mobile and Remote Access (MRA) deployment. In MRA deployments, the de-registered Jabber client attempts to re-register. For MRA deployments, if you have Cisco Jabber running on two devices with the same device name, make sure to log Jabber out of one device before you use the other.

Troubleshooting OAuth SSO Configuration

The following table highlights useful logs for troubleshooting OAuth SSO configuration. Trace does not need to be configured for these logs.

Note To set SAML SSO logs to a detailed level, run the `set samltrace level debug` CLI command.

Table 70: Logs for Troubleshooting OAuth Refresh Logins

Logs	Log Details
SSO Logs	Each time a new SSO App operation is completed, new log entries are generated here: `/var/log/active/platform/log/ssoApp.log`

Logs	Log Details
Ssosp Logs	SSO and OAuth operations are logged in ssosp logs. Each time SSO is enabled a new log file is created here: `/usr/local/thirdparty/Jakarta-tomcat/logs/ssosp/log4j/`
SSO and OAuth Configuration	Certificate logs are located at the following location. Each time the Authz certificate is regenerated, a new log file is generated: `/var/log/active/platform/log/certMgmt*.log`

PART VIII

Configure Media Resources

CHAPTER 58

Media Resources Overview

About Media Resources

Cisco Unified Communications Manager functionality requires the use of media resources. Cisco Unified Communications Manager includes media resources such as:

- Annunciators
- Interactive Voice Response (IVR)
- Media Termination Points (MTP)
- Transcoders
- Trusted Relay Points
- Conference Bridges
- Music On Hold/Video on Hold

You can make media resources available to calls by assigning them to a media resource group list, and then assigning that list to a device pool, or to an individual device. The default setting for individual devices is to use the media resources that are assigned to the device pool that the device is using.

Note For information on configuring Music On Hold, refer to the *Feature Configuration Guide for Cisco Unified Communications Manager*.

Media Resources Configuration Task Flow

Complete the following task flows to configure media resources for your system.

Procedure

	Command or Action	Purpose
Step 1	Media Resource Group Task Flow, on page 470	Use the procedures in this chapter to define logical groupings of media servers.
Step 2	Trusted Relay Points Task Flow, on page 476	Insert trusted relay points into a media stream to act as a control point for that stream. This device provides further processing on that stream or as a method to ensure that the stream follows a specific path.
Step 3	Annunciator Configuration Task Flow, on page 485	Configure the annunciator to enable Unified Communications Manager to play prerecorded announcements (.wav files) and to send tones to devices such as Cisco IP Phones and gateways that are configured for Cisco Multilevel Precedence and Preemption.
Step 4	Interactive Voice Response Configuration Task Flow, on page 493	Use the Interactive Voice Response (IVR) device to play prerecorded feature announcements (.wav files) to devices such as Cisco IP Phones and Gateways. These announcements play on devices that use features which require IVR announcements, like Conference Now.
Step 5	Video on Hold Configuration Task Flow, on page 498	Configure video on hold in video contact centers where customers calling into the video contact center are able to watch a specific video after initial consultation with the agent at the contact center.
Step 6	Announcements Configuration Task Flow, on page 502	Use the procedures in this chapter to use pre-defined announcements or upload custom announcements.
Step 7	Conference Bridge Configuration Task Flow, on page 509	Configure software and hardware applications that allow ad hoc and meet-me voice conferencing, as well as video conferencing.
Step 8	DSCP Settings Configuration Task Flow, on page 515	Use flexible DSCP marking and video promotion to configure a policy that specifies which applications receive the most favorable call admission control (CAC) and quality of service (QoS) treatment.
Step 9	Transcoders and MTPs Configuration Task Flow, on page 526	Configure transcoders to convert an input stream from one codec into an output stream that uses a different codec.

CHAPTER 59

Define Media Resources

Media Resource Group Overview

Media resource groups define logical groupings of media servers. You can associate a media resource group with a geographical location or 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 required.

The system has a two-tiered approach to managing media resources:

- Media resource groups—A logical grouping a media servers.
- Media resource group lists—A prioritized list of media resource groups. An application selects the required media resource, such as a music on hold server from the available media resources according to the priority order that you define in a media resource group list. Media resource group lists, which are associated with devices, provide media resource group redundancy.

You can group devices of the following types into a media resource group:

- Conference Bridge (CFB)
- Media Termination Point (MTP)
- Music On Hold Server (MOH)
- Transcoder (XCODE)
- Annunciator (ANN)

Note After you configure media resources and if you have not defined any media resource groups, all media resources belong to the default group, and all media resources are available to all Cisco Unified Communications Managers within a given cluster.

Media Resource Group List

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 the available media resources according to the priority order that you define in a media resource group List. Media resource group lists, which are associated with devices or device pools, provide media resource group redundancy.

Media Resource Group Prerequisites

Ensure that Cisco Unified Communications Manager has media resources to provide services, such as annunciator, transcoding, conferencing, music on hold, and media termination.

Media Resource Group Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure Media Resource Groups, on page 471.	Configure media resource group to define a logical groupings of media servers.
Step 2	Assign Device to a Media Resource Group, on page 471.	Assign a device to a media resource group. **Note** Order of assigning a device is not significant.
Step 3	Configure Media Resource Group Lists, on page 472.	Create media resource group list to specify a list of prioritized media resource groups. Media resource group lists, which are associated with devices or device pools, provide media resource group redundancy. **Note** Order of assigning a device is significant.
Step 4	Assign Media Resource Group to Media Resource Group List, on page 472.	Assign the newly created media resource group to the media resource group list.
Step 5	Assign Media Resources to Device or Device Pool, on page 473.	Assign the existing or newly created media resource group list to a device or a device pool.
Step 6	(Optional) Configure Media Resource Redundancy, on page 473.	Confirm media resources redundancy for a scenario when a media resource fails.

Configure Media Resource Groups

A media resource group contains a list of media resources that you want to assign to endpoints, or groups of endpoints.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Media Resources** > **Media Resource Group**.

Step 2 Do either of the following:

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

Step 3 Configure the fields in the **Media Resource Group Configuration** window. See the online help about the fields and their configuration options.

Step 4 Enter a **Name** and **Description** for the group.

Step 5 From **Available Media Resources**, select the resources you want to add to this group, and use the arrows to move the resources to **Selected Media Resources**.

Step 6 (Optional) To use multicast for Music On Hold audio, check the **Use Multi-cast for MOH Audio** check box.

Step 7 Click **Save**.

Assign Device to a Media Resource Group

You can assign devices, such as annunciators (ANN), interactive voice responses (IVR), conference bridges (CFB), media termination points (MTP), music on hold (MOH) servers and transcoders to a media resource group. The order is which you assign the devices is not significant.

Before you begin

Configure Media Resource Groups, on page 471.

Procedure

Step 1 From the Cisco Unified CM Administration, choose **Media Resources** > **Media Resource Group**.

Step 2 To configure an existing media resource group, **Find and List Media Resource Group** window, specify the appropriate filters and click **Find**.

Step 3 To configure new media resource group, click **Add New**.

Step 4 From the **Available Media Resources** field, choose the one or multiple devices and click the down-arrow key.
The selected devices appear in the **Selected Media Resources** field.

Step 5 Click **Save**.

What to do next

Configure Media Resource Group Lists, on page 472.

Configure Media Resource Group Lists

Create a prioritized listing of media resource groups. You can assign this list to individual devices or to to a device pool.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Media Resources** > **Media Resource Group List**.

Step 2 Do either of the following:

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

Step 3 Enter a **Name** for the media resource group list.

Step 4 From **Available Media Resource Groups**, select the groups you want to add, and use the arrows to move them to **Selected Media Resource Groups**.

Step 5 Click **Save**.

Note For endpoints to use these media resources, you must assign the list to a device pool, gateway port, or to a device.

Assign Media Resource Group to Media Resource Group List

Before you begin

Configure Media Resource Group Lists, on page 472.

Procedure

Step 1 From the Cisco Unified CM Administration, choose **Media Resources** > **Media Resource Group**.

Step 2 To configure an existing media resource group, from the **Find and List Media Resource Group** window, specify the appropriate filters and click **Find**.

Step 3 From the **Available Media Resources** list, select one or multiple media resources and click the down arrow key.
The selected media resources appear in the **Selected Media Resources** list.

Step 4 Click **Save**.

What to do next

Assign Media Resources to Device or Device Pool, on page 473.

Assign Media Resources to Device or Device Pool

Assign media resources to endpoints by associating the prioritized media resource group list to a device pool, or to an individual device.

Procedure

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

- To add media resources to a device pool, choose **System** > **Device Pools**.
- To add media resource directly to an endpoint, choose **Device** > **Phone**.

Step 2 Click **Find** and select the device pool or device to which you want to assign these media resources.

Step 3 From the **Media Resource Group List** drop-down, select a list.

Step 4 Click **Save**.

Step 5 Click **Apply Config to Selected**.
The **Apply Configuration** window appears showing the device name and the applicable configuration changes.

Configure Media Resource Redundancy

Media resource group lists provide media resource redundancy by specifying a prioritized list of media resource groups. An application can select required media resources from among the available ones according to the priority order that is defined in the media resource list.

To configure media resource groups and media resource group lists for redundancy, perform the Configure Media Resource Groups, on page 471 and Media Resource Group List, on page 470 procedures.

Media Resource Group Interactions and Restrictions

Media Resource Group Interactions

Table 71: Media Resource Group Interactions

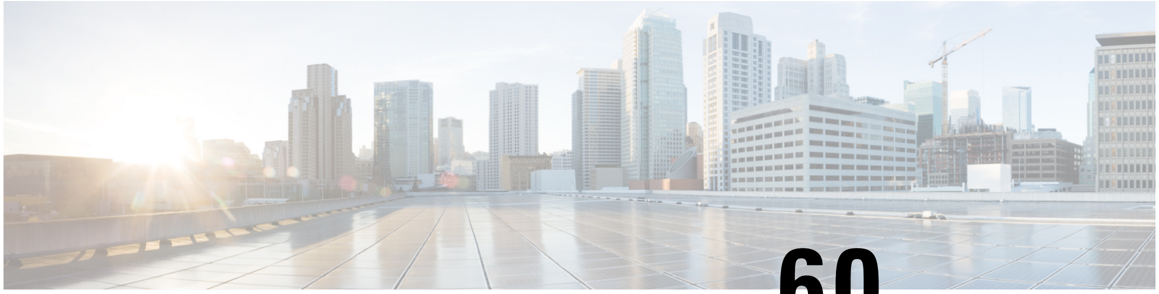
Feature	Interaction
Call processing	Call processing uses a media resource group list in the device level if you select the media resource group list. If a resource is not found, call processing may retrieve it from the default allocation. Call processing uses media resource group list in the device pool only if you do not select a media resource group list in the device level. If a resource is not found, call processing may retrieve it from the default allocation.

Feature	Interaction
Annunciator resource support	Cisco Unified Communications Manager provides annunciator resource support to a conference bridge if the media resource group list that contains the annunciator is assigned to the device pool where the conference bridge exists. Cisco Unified Communications Manager does not provide annunciator resource support for a conference bridge if the media resource group list is assigned directly to the device that controls the conference.
Video conference	To ensure that only a video conference bridge gets used when a user wants to hold a video conference, add the video conference bridge to a media resource group. Add the media resource group to a media resource group list and assign the media resource group list to the device or device pool that will use the video conference bridge.

Media Resource Group Restrictions

Table 72: Media Resource Group Restrictions

Restriction	Description
Deletion of a media resource group	You cannot delete a media resource group that is assigned to a Media Resource Group List.
Deletion of a transcoder	You cannot delete a transcoder that is assigned to a media resource group.
Deletion of a media resource	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.



CHAPTER 60

Configure Trusted Relay Points

Trusted Relay Point Overview

A Trusted Relay Point (TRP) is an MTP or transcoder that Cisco Unified Communications Manager can insert into the media stream to act as a control point for call media. The TRP can provide further processing on the stream and can ensure that the stream follows a specific path.

When a call requires a trusted relay point, Cisco Unified Communications Manager allocates an MTP or transcoder that has been enabled with TRP functionality.

Configuration

Both MTPs and transcoders can be configured to provide TRP functionality by checking the **Trusted Relay Point** check box in the **Media Termination Point Configuration** or **Transcoder Configuration** window.

You can configure the TRP requirement for individual calls by setting the **Use Trusted Relay Point** field to **On** for the following configuration windows:

- Phone Configuration
- Gateway Configuration
- Voicemail Port Configuration
- Trunk Configuration
- CTI Route Point Configuration
- Common Device Configuration
- Universal Device Template Configuration
- Various media resource configurations (Annunciator, IVR, MTPs, Transcoders, Conference Bridges, Music On Hold)

Trusted Relay Points Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure Trusted Relay Point for a Device, on page 476.	Configure trusted relay points (TRP) for one or multiple devices where media ends and insert TRP in Cisco Unified Communications Manager.
Step 2	Configure Trusted Relay Point for Media Termination Point, on page 477.	Configure media termination point (MTP) so that you can use the device as a trusted relay point. **Note** Ensure that a device that is configured as a TRP in Cisco Unified Communications Manager has the appropriate network connectivity and configuration between the TRP and any endpoints that are involved in the call.
Step 3	Configure Trusted Relay Point for Transcoder, on page 477.	Configure transcoder so that you can use the device as a trusted relay point. **Note** Ensure that a device that is configured as a TRP in Cisco Unified Communications Manager has the appropriate network connectivity and configuration between the TRP and any endpoints that are involved in the call.
Step 4	Enable Trusted Relay Point Service Parameter, on page 478.	Enable the TRP service parameter to determine whether a call that requires a TRP is allowed to proceed if no TRP resource is available.

Configure Trusted Relay Point for a Device

You can configure trusted relay points (TRP) for one or multiple devices where media ends and insert TRP in Cisco Unified Communications Manager. By configuring the TRP for a device, the device provides further processing on that stream or acts as a method to ensure that the stream follows a specific path.

Procedure

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

Step 2 To configure a trusted relay point for an existing device, from the **Find and List Common Device Configurations** window, specify the appropriate filters and click **Find**.

Step 3 To configure trusted relay point for a new device, from the **Common Device Configuration** window, click **Add New**.

Step 4 Configure the fields in the **Common Device Configuration** window. See the online help for more information about the fields and their configuration options.

Step 5 In the **Common Device Configuration Information** section, click the **Use Trusted Relay Point** check box.

Step 6 Click **Save**.

What to do next

Configure Trusted Relay Point for Media Termination Point, on page 477.

Configure Trusted Relay Point for Media Termination Point

You can configure a media termination point (MTP) so that you can use a device as a trusted relay point.

Before you begin

Configure Trusted Relay Point for a Device, on page 476.

Procedure

Step 1 From the Cisco Unified CM Administration, choose **Media Resources** > **Media Termination Point**.

Step 2 To configure a trusted relay point for an existing media termination point, from the **Find and List Media Termination Points** window, specify the appropriate filters and click **Find**.

Step 3 To configure trusted relay point for a new media termination point, click **Add New**.

Step 4 Configure the fields on the **Media Termination Point Configuration** window. See the online help for more information about the fields and their configuration options.

Step 5 In the **Media Termination Point Information** section, click the **Use Trusted Relay Point** check box.

Step 6 Click **Save**.

What to do next

Configure Trusted Relay Point for Transcoder, on page 477.

Configure Trusted Relay Point for Transcoder

You can configure a transcoder so that you can use the device as a trusted relay point.

Before you begin

Configure Trusted Relay Point for Media Termination Point, on page 477.

Procedure

Step 1 From the Cisco Unified CM Administration, choose **Media Resources** > **Transcoder**.

Step 2 To configure a trusted relay point for an existing transcoder, from the **Find and List Transcoder** window, specify the appropriate filters and click **Find**.

Step 3 To configure trusted relay point for a new transcoder, click **Add New**.

Step 4 Configure the fields on the **Transcoder Configuration** window. See the online help for more information about the fields and their configuration options.

Step 5 In the **Media Server Transcoder Info** section, click the **Use Trusted Relay Point** check box.

Step 6 Click **Save**.

What to do next

Enable Trusted Relay Point Service Parameter, on page 478.

Enable Trusted Relay Point Service Parameter

You can enable the TRP service parameter to determine whether a call that requires a TRP is allowed to proceed if no TRP resource is available.

Before you begin

Configure Trusted Relay Point for Transcoder, on page 477.

Procedure

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

Only **Server** drop-down list appears.

Step 2 From the **Service Parameter Configuration** window, choose a server from the **Server** drop-down list.
The **Service** drop-down list appears.

Step 3 Choose a Cisco Unified Communications Manager server from the **Server** drop-down list.
Based on the selected server and service, the service parameters appear.

Step 4 From the Clusterwide Parameters (Device - General) section, choose `True` for **Fail Call If Trusted Relay Point Allocation Fails** drop-down list. See the Related Topics section about the fields and their configuration options.

Step 5 From the Clusterwide Parameters (Device - H323) section, choose `True` for **Fail Call If MTP Allocation Fails** drop-down list. See the Related Topics section about the fields and their configuration options.

Step 6 Click **Save**.

Call Status When MTP and TRP Service Parameters are Selected

If you check both the **Media Termination Point Required** and the **Use Trusted Relay Point** check boxes for an endpoint, Cisco Unified Communications Manager allocates a Media Termination Point (MTP) that is also a Trusted Relay Point (TRP). If the administrator fails to allocate such an MTP or TRP, the call status appears.

The following table shows the call status with the values of the **Fail Call If Trusted Relay Point Allocation Fails** and the **Fail Call if MTP Allocation Fails** service parameters when a call fails.

Fail Call If TRP Allocation Fails	Fail Call If MTP Allocation Fails	Fail Call?
True	True	Yes
True	False	Yes
False	True	Yes, if MTP is rec MTP is required f
False	False	No

Call Status When MTP and TRP Service Parameters are Not Selected

If both the **Fail Call If Trusted Relay Point Allocation Fails** service parameter and the **Fail Call If MTP Allocation Fails** service parameter are set to `False`, the following table shows the call behavior in relationship to the MTP that is required and **Use Trusted Relay Point** configuration and the resource allocation status.

MTP Required	Use TRP	Resource Allocation Status	Call B
Y	Y	TRP allocated	Audic
Y	Y or N	MTP only	Audic
Y	Y or N	None allocated	If MT servic
N	Y	TRP allocated	Audic admis
N	Y	None allocated	Audic suppc

Trusted Relay Points Interactions and Restrictions

Trusted Relay Points Interactions and Restrictions

Feature	Interactions and Restrictions
Resource Reservation Protocol (RSVP)	If RSVP is enabled for the call, Cisco Unified Communications Manager first tries to allocate an RSVPAgent that is also labeled as TRP. Otherwise, another TRP device is inserted between the RSVPAgent and the endpoint.

Feature	Interactions and Restrictions
Transcoder for call	If you need a transcoder for the call and need to allocate it on the same side as the endpoint that needs TRP, Cisco Unified Communications Manager first tries to allocate a transcoder that is also labeled as TRP. Otherwise, another TRP device is inserted between the transcoder and the endpoint.
MTP allocation for endpoint	If you check both the **Media Termination Point Required** check box and the **Use Trusted Relay Point** check box for an endpoint, Cisco Unified Communications Manager should allocate an MTP that is also a TRP. If the administrator fails to allocate such an MTP or TRP, the call status appears.
TRP allocation	In most instances, TRP is allocated after users answer the call, so if a call fails due to failure to allocate the TRP, users may receive fast-busy tone after answering the call. (The SIP outbound leg with MTP required, or H.323 outbound faststart, represents an exception.)
TRP Insertion for endpoint	Cisco Unified Communications Manager must insert a TRP for the endpoint if you have checked the **Use Trusted Relay Point** check box for either the endpoint or the device pool that is associated with the device. The call may fail if Cisco Unified Communications Manager fails to allocate a TRP while the **Fail Call If Trusted Relay Point Allocation Fails** service parameter is set to `True`.
TRP and remote users	TRP is not recommended for providing secure solution for work from home remote users. Expressway's Mobile and Remote Access is the recommended solution.

Trusted Relay Points Restrictions

Table 73: Trusted Relay Points Restrictions

Restriction	Description
Insertion of trusted relay point for an endpoint	Cisco Unified Communications Manager must insert a TRP for the endpoint if you have checked the **Use Trusted Relay Point** check box for either the endpoint or the device pool that is associated with the device. The call may fail if Cisco Unified Communications Manager fails to allocate a TRP while the **Fail Call If Trusted Relay Point Allocation Fails** service parameter is set to `True`.
Allocation of media termination point for an endpoint	If you check both the **Media Termination Point Required** check box and the **Use Trusted Relay Point** check box for an endpoint, Cisco Unified Communications Manager should allocate an MTP that is also a TRP. If the administrator fails to allocate such an MTP or TRP, the call status appears.

Restriction	Description
Allocation of trusted relay point	In most instances, TRP is allocated after users answer the call, so if a call fails due to failure to allocate the TRP, users may receive fast-busy tone after answering the call. (The SIP outbound leg with MTP required, or H.323 outbound faststart, represents an exception.)

CHAPTER 61

Configure Annunciator

Annunciator Overview

An annunciator is an SCCP software devices that runs on Cisco Unified Communications Manager and which allows you to send prerecorded messages and tones to Cisco IP Phones and gateways. The annunciator is activated on a cluster node by turning on the Cisco IP Voice Media Streaming service on that node. Features such as MLPP, SIP trunks, IOS gateways, and software conference bridges rely on the annunciator to send the predefined message to the phone or gateway via a one-way media stream. In addition:

- Both IPv4 and IPV6 are supported. The annunciator is configured automatically in dual mode when the system's platform is configured for IPv6 and the IPv6 enterprise parameter is enabled.
- SRTP is supported

Annunciator Scalability

By default, an annunciator supports 48 simultaneous media streams. You can add capacity by activating the annunciator on additional nodes or by changing the default number of annunciator media streams via the **Call Count** service parameter. However, it's not recommended to increase this value on a node unless the **Cisco CallManager** service is deactivated on that node.

If the annunciator runs on a dedicated subscriber node where the **Cisco CallManager** service does not run, the annunciator can support up to 255 simultaneous announcement streams. If the dedicated subscriber node meets the OVA virtual machine configuration for 10,000 users, the annunciator can support up to 400 simultaneous announcement streams.

Caution We recommend that you do not activate the annunciator on Unified Communications Manager nodes that have a high call-processing load.

Annunciator with Conference Bridge

The Annunciator is available to a conference bridge under the following conditions:

- If the media resource group list that contains the annunciator is assigned to the device pool where the conference bridge exists.
- If the annunciator is configured as the default media resource.

The annunciator is not available to a conference bridge if the media resource group list is assigned directly to the device that controls the conference.

Each conference supports only one announcement. If the system requests another announcement while the current announcement is playing, the new announcement preempts the one that is playing.

Default Annunciator Announcements and Tones

Cisco Unified Communications Manager automatically provides a set of prerecorded annunciator announcements when you activate the Cisco IP Media Streaming Application service. An announcement or a tone is played for the following conditions:

- Announcement — Played for devices that are configured for Cisco Multilevel Precedence and Preemption.
- Barge tone — Heard before a participant joins an ad hoc conference.
- Ring back tone — When you transfer a call over the PSTN through an IOS gateway, the annunciator plays the tone because the gateway cannot play the tone when the call is active.
- Ring back tone — When you transfer calls over an H.323 intercluster trunk, a tone is played.
- Ring back tone — When you transfer calls to the SIP client from a phone that is running SCCP, a tone is played.

You cannot change the default prerecorded annunciator announcements or add additional announcements. Localization of the announcement is supported if the Cisco Unified Communications Manager Locale Installer is installed and the locale settings are configured for the Cisco Unified IP Phone or device pool. For information about the Locale Installer and the files to install for user and (combined) network locales, see *Installing Cisco Unified Communications Manager*. To download the locale installer, see the support pages at www.cisco.com.

Table 74: Prerecorded Annunciator Announcements

Condition	Announcement
An equal or higher precedence call is in progress.	Precedence access limitation has prevented the completion of your call. Please hang up and try again. This is a recording.
A precedence access limitation exists.	Precedence access limitation has prevented the completion of your call. Please hang up and try again. This is a recording.
Someone attempted an unauthorized precedence level.	The precedence used is not authorized for your line. Please use an authorized precedence or ask your operator for assistance. This is a recording.
The call appears busy, or the administrator did not configure the directory number for call waiting or preemption.	The number you have dialed is busy and not equipped for call waiting or preemption. Please hang up and try again. This is a recording.

Condition	Announcement
The system cannot complete the call.	Your call cannot be completed as dialed. Please consult your directory and call again or ask your operator for assistance. This is a recording.
A service interruption occurred.	A service disruption has prevented the completion of your call. In case of emergency call your operator. This is a recording.

The following table lists the tones that the annunciator supports.

Table 75: Tone Description

Type	Description
Busy tone	A busy tone is heard when the dialed number is busy.
Barge tone	A conference barge-in tone is heard before the participant joins an ad hoc conference.
Ring back tone	An alert tone is heard for the following scenarios: • When you transfer a call over the PSTN through an IOS gateway. • When you transfer a call over an H.323 intercluster trunk. • When you transfer a call to the SIP client from an SCCP phone.

Annunciator Use With Conference Bridges

The Annunciator is available to a conference bridge under the following conditions:

- If the media resource group list that contains the annunciator is assigned to the device pool where the conference bridge exists.
- If the annunciator is configured as the default media resource.

The annunciator is not available to a conference bridge if the media resource group list is assigned directly to the device that controls the conference.

Each conference supports only one announcement. If the system requests another announcement while the current announcement is playing, the new announcement preempts the one that is playing.

Annunciator Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Activate the Annunciator, on page 486	Activate the Cisco IP Voice Media Streaming Application service on the node to activate the annunciator for that node. Activate only one Cisco IP Voice Media Streaming Application

	Command or Action	Purpose
		service for each annunciator device in the cluster.
Step 2	Required: Media Resource Group Task Flow, on page 470	Add the annunciator to media resource groups and lists to manage your media resources using Cisco Unified Communications Manager Administration. You can see which media resource groups have annunciators from the **Dependency Records Summary** window.
Step 3	Configure Device Pools, on page 56	Add the media resource group that includes the annunciator to a device pool using Cisco Unified Communications Manager Administration. Repeat this step for each annunciator. Each annunciator must belong to a device pool.
Step 4	(Optional) Change the Default Number of Media Streams, on page 487	You can change the default number of media streams for an annunciator.
Step 5	(Optional) Override the Annunciator Security Mode, on page 487	When Cisco Unified Communications Manager is configured in a secured deployment, the media streaming between the annunciator and security enabled devices is automatically encrypted using the Secure Real-Time Protocol (SRTP). You can override the annunciator security settings so that media streamed from the secured annunciator is not encrypted.
Step 6	(Optional) View List of Media Resource Groups That Have Annunciators, on page 488	You can see which media resource groups use the annunciator device.
Step 7	(Optional) Configure Annunciator for Conference Bridges, on page 488	You can use the annunciator with conference bridges when the annunciator and conference bridge belong to the same device pool.

Activate the Annunciator

Activate only one Cisco IP Voice Media Streaming Application service for each annunciator device in the cluster.

⚠ **Caution** We recommend that you do not activate the annunciator on Cisco Unified Communications Manager nodes that have a high call-processing load.

Procedure

Step 1 From the Serviceability GUI, choose **Tools** > **Activation**. The **Service Activation** window appears.

Step 2 Select the node in the **Server** field and click **Go**.

Step 3 Check **Cisco IP Voice Media Streaming Application**, and then click **Save**.

What to do next

If you haven't yet set up your media resource group and assigned it to a device pool, Media Resources Configuration Task Flow, on page 467.

Otherwise, Change the Default Number of Media Streams, on page 487.

Change the Default Number of Media Streams

An annunciator supports 48 simultaneous media streams by default. You can change the default number of media streams using the annunciator service parameter; however, we recommend that you do not exceed 48 annunciator streams on a node.

Before you begin

Activate the Annunciator, on page 486

Procedure

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

Step 2 In the **Service Parameters Configuration** window, select the server and then select the service called Cisco IP Voice Media Streaming App.

Step 3 In the **Service Parameter Configuration** window, enter the number of simultaneous media streams in the **Call Count** field of the **Annunciator (ANN) Parameters** section, and then click **Save**.

When you update the annunciator, the changes automatically occur when the annunciator is idle and no active announcements are playing.

What to do next

Override the Annunciator Security Mode, on page 487

Override the Annunciator Security Mode

When the enterprise parameter called Cluster Security Mode is set to 1 (mixed mode), annunciator devices are automatically enable for security. The annunciator registers as a secured SRTP device on Cisco Unified Communications Manager nodes that have Secure Real-Time Protocol (SRTP) enabled. A locked icon appears on SRTP capable devices. Announcements from a secured annunciator are encrypted if the receiving device is also SRTP capable; otherwise, unsecured announcements and tones are sent.

You can override the annunciator security mode using the service parameter called Make Annunciator Non-secure when Cluster Security is Mixed. When the annunciator security mode is overridden, an unencrypted announcement is played even if the receiving device is SRTP capable.

Before you begin

Change the Default Number of Media Streams, on page 487

Procedure

Step 1 Required: From Cisco Unified Communications Manager Administration, choose **System** > **Service Parameters**.

Step 2 Select the node in the **Server** field.

Step 3 Select **Cisco Unified IP Voice Media Streaming Application** in the **Service** field.

Step 4 Set **Make Annunciator Non-secure when Cluster Security is Mixed** to **True**, and then click **Save**.

Tip Click **Advanced** if you do not see the Make Annunciator Non-secure when Cluster Security is Mixed parameter.

What to do next

View List of Media Resource Groups That Have Annunciators, on page 488

View List of Media Resource Groups That Have Annunciators

View the **Dependency Records Summary** window to see which media resource groups use the annunciator device.

Before you begin

Override the Annunciator Security Mode, on page 487

Procedure

Step 1 From Cisco Unified CM Administration, choose **Media Resources** > **Annunciator**.

Step 2 Select the annunciator that is set up for your system.

Step 3 From the **Related Links** drop-down list box, choose **Dependency Records** and click **Go**.
The **Dependency Records Summary** window displays the media resource groups that use the annunciator device.

What to do next

Configure Annunciator for Conference Bridges, on page 488

Configure Annunciator for Conference Bridges

You can use the annunciator with conference bridges.

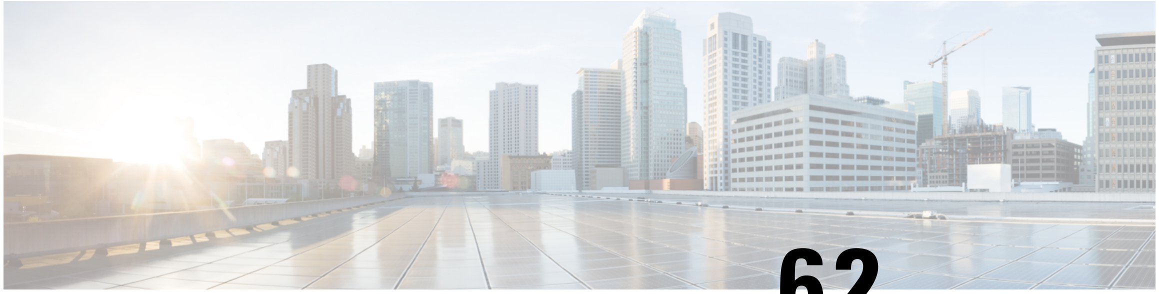
Before you begin

View List of Media Resource Groups That Have Annunciators, on page 488

Procedure

Step 1 Add the annunciator to a media resource group list.

Step 2 Assign the media resource group list that contains the annunciator to the device pool of the conference bridge to make the annunciator available to all devices in the cluster.



CHAPTER 62

Configure Interactive Voice Response

Interactive Voice Response Overview

The Interactive Voice Response (IVR) device enables Cisco Unified Communications Manager to play prerecorded feature announcements (.wav files) to devices such as Cisco Unified IP Phones and Gateways. These announcements play on devices that use features which require IVR announcements, like Conference Now.

When you add a node, an IVR device is automatically added to that node. The IVR device remains inactive until the Cisco IP Voice Media Streaming Application service is activated on that node.

An IVR supports 48 simultaneous callers by default. You can change the number of IVR callers using the Cisco IP Voice Media Streaming Application service parameter. However, we recommend that you do not exceed 48 IVR callers on a node. You can configure the number of callers for IVR based on expected simultaneous calls to IVR for joining Conference Now.

Caution Do not activate the IVR device on Cisco Unified Communications Manager nodes that have a high call-processing load.

Default IVR Announcements and Tones

Cisco Unified Communications Manager automatically provides a set of prerecorded Interactive Voice Response (IVR) announcements when you activate the Cisco IP Media Streaming Application service. You can replace the default prerecorded IVR announcements. An announcement is played for the following conditions:

Table 76: Prerecorded IVR Announcements

Announcement	Condition
ConferenceNowAccessCodeFailed Announcement	Plays when an attendee enters the wrong access code to join Conference Now after exceeding the maximum number of attempts.
ConferenceNowAccessCodeInvalid Announcement	Plays when an attendee enters the wrong access code.
ConferenceNowCFBFailed Announcement	Plays when the conference bridge capacity limit is exceeded while initiating Conference Now.
ConferenceNowEnterAccessCode Announcement	Plays when an attendee joins Conference Now and the host sets an attendee access code.
ConferenceNowEnterPIN Announcement	Plays when a host or attendee tries to join a meeting.
ConferenceNowFailedPIN Announcement	Plays after the host exceeds the maximum number of attempts to enter a correct PIN.
ConferenceNowGreeting Announcement	Plays a greeting prompt for Conference Now.
ConferenceNowInvalidPIN Announcement	Plays when the host enters a wrong PIN.
ConferenceNowNumberFailed Announcement	Plays when a host or attendee enters the wrong meeting number after exceeding the maximum number of attempts.
ConferenceNowNumberInvalid Announcement	Plays when a host or attendee enters a wrong meeting number.

Interactive Voice Response Restrictions

Feature	Restriction
Load Balancing	The Interactive Voice Response (IVR) uses Real-Time Protocol (RTP) streams through a common media device driver. This device driver is also used by other software media devices provided by the Cisco IP Voice Media Streaming Application services such as Music On Hold (MOH), Software Media Termination Point (MTP), Software Conference Bridge (CFB), and Annunciator. Configuring a larger call volume affects the system performance. This also impacts call processing if the Call Manager service is active on the same server node.
DTMF Digits	The IVR supports only Out-Of-Band (OOB) DTMF digit collection method. If there is a DTMF capability mismatch between the calling device and the IVR, an MTP will be allocated.

Feature	Restriction
Codecs	The IVR only supports codec G.711 (a-law and mu-law), G.729, and Wide Band 256k. If there is a codec mismatch between the calling device and the IVR, a transcoder will be allocated.

Interactive Voice Response Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Activate the Interactive Voice Response, on page 493	Activate the Cisco IP Voice Media Streaming Application service on the node to activate the IVR for that node. Activate only one Cisco IP Voice Media Streaming Application service for each IVR device in the cluster.
Step 2	Required: View List of Media Resource Groups That Have IVR, on page 494	Add the IVR to media resource groups and lists to manage your media resources using Cisco Unified Communications Manager Administration.
Step 3	(Optional) Change the Default Number of Media Streams, on page 487	You can change the default number of media streams for an IVR.

Activate the Interactive Voice Response

Activate one or more Cisco IP Voice Media Streaming Application service for each node to have Interactive Voice Response (IVR) device registered in the cluster.

⚠ **Caution** Do not activate the IVR on Cisco Unified Communications Manager nodes that have a high call-processing load.

Procedure

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

Step 2 Select the node in the **Server** field and click **Go**.

Step 3 Check the **Cisco IP Voice Media Streaming Application** check box, and then click **Save**.

View List of Media Resource Groups That Have IVR

Procedure

Step 1 From Cisco Unified CM Administration, choose **Media Resources** > **Interactive Voice Response (IVR)**. The **Find and List Interactive Voice Response (IVR)** window is displayed.

Step 2 From the **Find and List Interactive Voice Response (IVR) where** window, click **Find**. A list of IVRs that are available on Cisco Unified Communications Manager is displayed.

Step 3 Choose the IVR on which you want to see the associated list of media resource groups.

Step 4 Choose **Dependency Records** from the **Related Links** drop-down list and click **Go**.

If the dependency records are not enabled for the system, the **Dependency Records Summary** window displays a message.

IVR Settings

Field	Description
Server	Displays the preconfigured server (servers are added at installation), by default.
Name	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 IVR_.
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, choose the appropriate location for this IVR. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this IVR 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 details on setting up a location-based CAC across intercluster trunks, see the *System Configuration Guide for Cisco Unified Communications Manager* .

Field	Description
Use Trusted Relay Point	From the drop-down list, enable or disable whether Unified Communications Manager inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values: • Off—Choose this value to disable the use of a TRP with this device. • On—Choose this value to enable the use of a TRP with this device. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Unified Communications Manager places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVPAgent). If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. If both TRP and RSVPAgent are needed for the endpoint, Unified Communications Manager searches for an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified Communications Manager searches for a transcoder that is also designated as a TRP.

Change IVR Parameters

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **System** > **Service Parameters**. The **Service Parameters Configuration** window appears.

Step 2 Select the server and then select the service called Cisco IP Voice Media Streaming App. The **Service Parameter Configuration** window appears.

Step 3 Enter the number of simultaneous media streams in the **Call Count** field of the **Interactive Voice Response (IVR) Parameters** section, and then click **Save**.

When you update the IVR, the changes automatically occur when the IVR is idle and no active announcements are playing.

CHAPTER 63

Configure Video On Hold Server

Video On Hold Overview

The video on hold feature is for video contact centres where customers calling into the video contact centre are able to watch a specific video after initial consultation with the agent at the contact centre. In this case, the agent selects the video stream that is played to the customer while the customer is on hold.

The video on hold server is a media content server that can stream audio and video content when directed by Cisco Unified Communications Manager. The media content server is an external device that can store and stream audio and video content under Unified Communications Manager control using SIP as the signal protocol. The media content server is capable of providing hi-definition video content at 1080p, 720p, or lower resolutions such as 360p. Cisco MediaSense is used as the media content server.

In addition to the video contact centre, video on hold can be deployed within any enterprise if the deployment requires a generic video on hold capability. You can configure a **Default Video Content Identifier** for the video on hold server which identifies the video stream that is played to the user that is on hold.

Note In a Unified Contact Center with Customer Voice Portal (CVP) post-routed deployment, to get video on hold functionality, you must allocate video on hold resources in the SIP trunk that runs between Unified Communications Manager and CVP.

Video on Hold Configuration Task Flow

Before you begin

Procedure

	Command or Action	Purpose
Step 1	Create a SIP Trunk to Cisco MediaSense Server, on page 498	Configure a SIP trunk to the Cisco MediaSense cluster.
Step 2	Configure a Video On Hold Server, on page 499	Configure a video on hold server in Cisco Unified Communications Manager that identifies the video content that is stored on the MediaSense server.

Create a SIP Trunk to Cisco MediaSense Server

You must configure Unified Communications Manager with a SIP trunk to a Cisco MediaSense cluster. The SIP trunk to the Cisco MediaSense server contains the IP addresses of the Cisco MediaSense nodes. The Unified Communications Manager SIP trunk supports up to 16 destination IP addresses.

Note Cisco MediaSense cluster should have two or more nodes for redundancy and scalability purposes.

You configure the SIP trunk with default configuration. Other configurations on the SIP trunk are not supported for the video on hold feature.

Procedure

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

Step 2 Click **Add New**.

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

Step 4 From the **Device Protocol** drop-down list, ensure that **SIP** is entered as the protocol and click **Next**.

Step 5 In the **Device Information** area, enter the following fields:

- **Device Name**—Enter a trunk name.
- **Description**—Enter a trunk description.
- **Device Pool**—Choose the appropriate device pool for the SIP trunk.
- **Location**—Choose the appropriate location for this trunk.

Step 6 In the **SIP Information** area, enter the following fields:

- **Destination Address**—Enter the IP address of the Cisco MediaSense server. You can specify mulitple IP addresses.

- **Destination Port**—Enter the port number, we recommend that you accept the default port number, 5060. You can specify multiple ports.
- **SIP Trunk Security Profile**—From the drop-down list, choose a SIP trunk security profile.
- **SIP Profile**—From the drop-down list, choose a SIP profile. Select a SIP profile with the option ping configured. If none exists, create one. This is not mandatory but will improve the user experience.

Step 7 Click **Save**.

What to do next

Configure a Video On Hold Server, on page 499

Configure a Video On Hold Server

The SIP trunk for the video on hold server points to the Cisco MediaSense server and the default content identifier points to a stream ID that exists on the MediaSense server. The content identifier can be any alphanumeric string.

Before you begin

Create a SIP Trunk to Cisco MediaSense Server, on page 498

Procedure

Step 1 In **Cisco Unified Communications Manager Administration**, choose **Media Resources** > **Video on Hold Server**.

Step 2 Click **Add New** to set up a new video on hold server.

Step 3 Enter the name of the video on hold server.

Step 4 Enter a description for the server.

Step 5 Enter an alphanumeric string for the **Default Video Content Identifier**.

Step 6 Select the SIP trunk to be used from the drop-down list. If a new SIP trunk needs to be created, click the **Create SIP Trunk** button

Step 7 Click **Save**.

Video On Hold Interactions

For the Enhanced Location Call Admission Control feature, the Cisco MediaSense servers can be co-located in a Unified Communications Manager cluster (the Cisco MediaSense cluster is directly connected to the cluster where the holding party is registered). In that case, the Unified Communications Manager cluster is responsible for deducting the bandwidth between the location of the party on hold and the Cisco MediaSense location. Since video on hold interactions make use of 720p or 1080p video streams, it is important to take the bandwidth usage into account before allowing new sessions in order to maintain video quality of existing sessions.

CHAPTER 64

Configure Announcements

Announcements Overview

In Cisco Unified Communications Manager Administration, use the **Menu Resources** > **Announcements** menu path to configure announcements. There are two classifications of announcements:

- System Announcements—Pre-defined announcements that are used in normal call processing or provided as sample feature announcements.
- Feature Announcements—Used by features such as Music on Hold (MOH), Hunt Pilots with Call Queuing or External Call Control. You can customize your own feature announcements by uploading Cisco-provided audio files or uploading custom `.wav` files. Upload all custom announcement `.wav` files to all servers in the cluster.

Note You can hear custom announcements such as warning or reorder tones if you are connected through a trunk or gateway. However, you cannot hear custom announcements on calls between two IP phones or IP phones and Jabber clients.

Formats

The recommended format for announcements includes the following specifications:

- 16-bit PCM wav file
- Stereo or mono
- Sample rates of 48 kHz, 44.1 kHz, 32 kHz, 16 kHz, or 8 kHz

Default Announcements

You can upload custom announcement .wav files or change the Cisco-provided file for a system announcement. However, you cannot change the announcement identifier. For example, the System announcement

(VCA_00121) is played when a caller dials an invalid number. This is commonly known as the vacant call announcement.

Table 77: Announcements in the Find and List Announcements Window

Announcement Identifier	Description
Gone_00126	System: Gone
MLPP-BNEA_00123	System: MLPP Busy not equipped
MLPP-BPA_00122	System: MLPP Higher precedence
MLPP-ICA_00120	System: MLPP Service disruption
MLPP-PALA_00119	System: MLPP Precedence access limit
MLPP-UPA_00124	System: MLPP Unauthorized precedence
Mobility_VMA	Please press 1 to be connected
MonitoringWarning_00055	System: Monitoring or Recording
RecordingWarning_00038	System: Recording
TemporaryUnavailable_00125	System: Temporary unavailable
VCA_00121	System: Vacant number / invalid number dialed
Wait_In_Queue_Sample	Builtin: Sample queued caller periodic announcement
Welcome_Greeting_Sample	Builtin: Sample caller greeting

Announcements Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure Announcement, on page 503.	Configure an announcement that you can use with features, such as Music On Hold (MoH) along with Hunt Pilot call queuing or External Call Control.
Step 2	Upload a Customized Announcement, on page 503.	Upload custom announcement .wav files or change the Cisco-provided file for a system announcement. However, you cannot change the announcement identifier. The customized announcements are underlined with a hyperlink and appear in the **Find and List Announcements** window of Cisco Unified Communications Manager.

Configure Announcement

You can configure an announcement that you can use as a system announcement or as a feature announcement. A system announcement is used for call processing or for the use of sample feature announcements whereas a feature announcement is used for specific features, such as music on hold (MOH) in association with hunt pilot call queuing or external call control.

You can modify an existing announcement or configure a new announcement in Cisco Unified Communications Manager.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Media Resources** > **Announcement**.

Step 2 Do one of the following:

- Click **Find** and select an existing announcement to edit.
- Click **Add New** to add a new announcment.

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

Step 4 Click **Save**.

Upload a Customized Announcement

You can modify a default announcement with an uploaded custom .wav file with a different announcement. When you import an audio source file, Unified Communications Manager processes the file and converts the file to the proper formats for use by the music on hold (MOH) server.

Note Announcements are specific to the locale (language). If your installation is using more than one language locale, you have to record each custom announcement each language as a separate .wav file and upload with the correct locale assignment. This task also requires that the correct locale package is installed on each server before uploading custom announcement .wav files for languages other than United States English.

Similar to MOH audio source files, the recommended format for announcements includes the following specifications:

- 16-bit PCM .wav file
- Stereo or mono
- Sample rates of 48 kHz, 44.1 kHz, 32 kHz, 16 kHz, or 8 kHz

You cannot update announcements that are not hyperlinked in the **Find and List Announcements** window in Unified Communications Manager. You can add customized announcements for Cisco-provided announcements that are underlined with a hyperlink in this window. For example, MLPP-ICA_00120 and MonitoringWarning_00055.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Media Resources** > **Announcement**.

Step 2 From the **Find and List Announcements** window, enter search criteria, click **Find**, and click the hyperlink for the announcement from the resulting list.

Step 3 From the **Announcement Configuration** window, click **Upload File**.

Step 4 From the **Upload File** pop-up window, choose the locale, enter the filename and browse to select the .wav file, and click **Upload File**.

The upload process begins and the status is updated after the processing is complete. Select **Close** to close the **Upload File** window.

Step 5 (Optional) If you want Unified Communications Manager to play the customized announcement instead of playing the Cisco-provided announcement, check the **Enable** check box appears in the **Announcement by Locale** pane in the **Announcements Configuration** window.

If the **Enable** check box is unchecked, Unified Communications Manager plays the Cisco-provided announcement.

Step 6 Click **Save**.

What to do next

Upload the announcement on each node in the cluster as the announcement files are not propagated between servers in a cluster. Browse for Cisco Unified Communications Manager Administration on each server in the cluster and repeat the upload process.

CHAPTER 65

Configure Conference Bridges

Conference Bridges Overview

Conference bridge for Cisco Unified Communications Manager is a software or hardware application that is designed to allow both ad hoc and meet-me voice conferencing. Additional conference bridge types support other types of conferences, including video conferences. Each conference bridge can host several simultaneous, multiparty conferences. Both hardware and software conference bridges can be active at the same time. Software and hardware conference bridges differ in the number of streams and the types of codec that they support. When you add a new server, the system automatically adds software conference bridges.

Note When Cisco Unified Communications Manager server is created, the Conference Bridge Software is also created automatically and it cannot be deleted. You cannot add Conference Bridge Software to Cisco Unified Communications Manager Administration.

Conference Bridge Types

The following conference bridge types are available in Cisco Unified Communications Manager Administration.

Table 78: Conference Bridge Types

Conference Bridge Type	Description
Cisco Conference Bridge Hardware	This type supports the Cisco Catalyst 4000 and 6000 Voice Gateway Modules and the following number of conference sessions: **Cisco Catalyst 6000** • G.711 or G.729a conference - 32 participants per port; six participants maximum per conference; 256 total participants per module; 10 bridges with three participants. • GSM - 24 participants per port; six participants maximum per conference; 192 total participants per module. **Cisco Catalyst 4000** G.711 conference only - 24 conference participants; maximum of four conferences with six participants each.
Cisco Conference Bridge Software	Software conference devices support G.711 codecs by default. The maximum number of callers for this type equals 256. With a setting of 256, the software conference bridge can support 64 conference sessions of 4 parties each. The maximum number of caller parties in a conference session is specified via the **Maximum Ad Hoc Conference** and **Maximum MeetMe Conference Unicast** service parameters. **Caution** This type of conference bridge (SW Conference Bridge) is a simplified implementation. It does not identify parties that are silent and uses a simple summing algorithm which may cause audio quality and low volume levels for the conference when there is a large number of participants.
Cisco IOS Conference Bridge	• Uses the NM-HDV or NM-HDV-FARM network modules. • G.711 a/mu-law, G.729, G.729a, G.729b, and G.729ab participants can join in a single conference call • Up to six parties can join in a single conference call Cisco Unified Communications Manager assigns conference resources to calls on a dynamic basis. For more information about Cisco IOS Conferencing and Transcoding for Voice Gateway Routers, see the Cisco IOS documentation that you received with this product.

Conference Bridge Type	Description
Cisco IOS Enhanced Bridges	• Uses the onboard Cisco Packet Voice/Fax Digital Signal Processor Modules (PVDM2) on the Cisco 2800 and 3800 series voice gateway routers or uses the NM-HD or NM-HDV2 network modules. • G.711 a-law/mu-law, G.729, G.729a, G.729b, G.729ab, GSM FR, and GSM EFR participants can join in a single conference • Up to eight parties can join in a single call. **Note** With ISR4000 router and any of the SM-X-PVDM-3000/ SM-X-PVDM-2000/ SM-X-PVDM-1000/ SM-X-PVDM-500, each Conference Bridge Profile can register up to a maximum of 512 sessions, due to the Unified Communications Manager 4096 maximum stream limitation. Cisco Unified Communications Manager assigns conference resources to calls on a dynamic basis. For more information about Cisco IOS Enhanced Conferencing and Transcoding for Voice Gateway Routers, see the Cisco IOS documentation that you received with this product. This conference bridge type supports SRTP media encryption with AES_CM_128_HMAC_SHA1_80 for supported SIP phones where an ISR 4000 series gateway is deployed. SCCP phones and non-supported SIP phones fall back to AES_CM_128_HMAC_SHA1_32 encryption. **Note** Make sure that the gateway load supports the cipher. Please review your gateway documentation for support details.
Cisco Conference Bridge (WS-SVC-CMM)	This conference bridge type supports the Cisco Catalyst 6500 series and Cisco 7600 series Communication Media Module (CMM). It supports up to eight parties per conference and up to 64 conferences per port adapter. This conference bridge type supports the following codecs: This conference bridge type supports ad hoc conferencing. • G.711 a-law/mu-law • G.729 annex A and annex B • G.723.1
Cisco Video Conference Bridge (IPVC-35xx)	The Cisco Video Conference Bridge provides audio and video conferencing functions for Cisco IP video phones, H.323 endpoints, and audio-only Cisco Unified IP Phones. The Cisco Video Conference Bridge supports the H.261, H.263, and H.264 codecs for video.

Conference Bridge Type	Description
Cisco TelePresence MCU	Cisco TelePresence MCU is a set of hardware conference bridges for Cisco Unified Communications Manager. The Cisco TelePresence MCU is a high-definition (HD) multipoint video conferencing bridge. It delivers up to 1080p at 30 frames per second, full continuous presence for all conferences, full transcoding, and is ideal for mixed HD endpoint environments. The Cisco TelePresence MCU supports SIP as the signaling call control protocol. It has a built in Web Server that allows for complete configuration, control, and monitoring of the system and conferences. The Cisco TelePresence MCU provides XML management API over HTTP. Cisco TelePresence MCU allows both ad hoc and meet-me voice and video conferencing. Each conference bridge can host several simultaneous, multiparty conferences. Cisco Unified Communications Manager supports presentation sharing with the Binary Floor Control Protocol (BFCP) between Unified Communications Manager and a Cisco TelePresence MCU. Cisco TelePresence MCU must be configured in Port Reservation mode. For more information, consult the *Cisco TelePresence MCU Configuration Guide*. **Note** Cisco TelePresence MCU does not support a common out-of-band DTMF method. Under the default setting, Cisco Unified Communications Manager will not require a Media Termination Point (MTP). However, if the Media Termination Point Required check box is checked, Cisco Unified Communications Manager will allocate an MTP and the SIP trunk will negotiate DTMF according to RFC 2833.
Cisco TelePresence Conductor	Cisco TelePresence Conductor provides intelligent conference administrative controls and is scalable, supporting device clustering for load balancing across MCUs and multiple device availability. Administrators can implement the Cisco TelePresence Conductor as either an appliance or a virtualized application on VMware with support for Cisco Unified Computing System (Cisco UCS) platforms or third-party-based platforms. Cisco TelePresence Conductor dynamically selects the most appropriate Cisco TelePresence resource for each new conference. Ad hoc, “MeetMe”, and scheduled voice and video conferences can dynamically grow and exceed the capacity of individual MCUs. Up to three Cisco TelePresence Conductor appliances or virtualized applications may be clustered to provide greater resilience. One Cisco TelePresence Conductor appliance or Cisco TelePresence Conductor cluster has a system capacity of 30 MCUs or 2400 MCU ports.

Conference Bridge Type	Description
Cisco Meeting Server	The Cisco Meeting Server conference bridge solution allows Ad Hoc, Meet-Me, Conference Now, and Rendezvous conferences. This conference bridge offers premises-based audio, video, and web conferencing, and works with third-party on-premises infrastructure. It scales for small or large deployments. You can add capacity incrementally as needed, to ensure that you can support the current and future needs of your organization. This conference bridge provides advanced interoperability. Any number of participants can create and join meetings from: • Cisco or third-party room or desktop video systems • Cisco Jabber Client • Cisco Meeting App (can be native or with a WebRTC compatible browser) • Skype for Business A minimum release of Cisco Meeting Server 2.0 is required to use the Cisco Meeting Server conference bridge. The Cisco Meeting Server supports SIP as the signaling call control protocol. It has a built in Web Server that allows for complete configuration, control, and monitoring of the system and conferences. The Cisco Meeting Server provides XML management API over HTTP. **Note** Cisco Meeting Server does not support H.265 video codec and Far End camera Control.

Conference Bridge Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure Conference Bridges, on page 509	Configure a hardware or software conference bridge to allow ad hoc and meet-me voice conferencing.
Step 2	Configure Service Parameters for Conference Bridges, on page 510	Perform this procedure when your network includes both Cisco IOS Conference Bridge and Cisco IOS Enhanced Conference Bridge.
Step 3	Configure SIP Trunk Connection to Conference Bridge, on page 510	Perform this procedure to configure a SIP trunk connection to your conference bridge.

Configure Conference Bridges

You must configure a hardware or software conference bridge to allow ad hoc and meet-me voice conferencing.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Media Resources** > **Conference Bridge**.

Step 2 Click **Add New**.

Step 3 Configure the fields in the **Conference Bridge Configuration** window. For detailed field descriptions, refer to the online help.

Step 4 Click **Save**.

What to do next

If your network includes both Cisco IOS Conference Bridge and Cisco IOS Enhanced Conference Bridge, Configure Service Parameters for Conference Bridges, on page 510.

Configure Service Parameters for Conference Bridges

Perform this procedure when your network includes both Cisco IOS Conference Bridge and Cisco IOS Enhanced Conference Bridge.

Procedure

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

Step 2 In the *Service Parameter Configuration* window, choose a server and choose the Cisco CallManager service.

Step 3 In the Clusterwide Parameters (Features - Conference) section, set the following parameters to 6:

- Maximum Ad Hoc Conference
- Maximum MeetMe Conference Unicast

Step 4 Click **Save**.

Configure SIP Trunk Connection to Conference Bridge

Procedure

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

Step 2 Complete one of the following steps:

- To create a new SIP trunk, click **Add New**.
- To add the connection to an existing trunk, click Find and select the appropriate trunk.

Step 3 Select the **Device Protocol** as **SIP**.

Step 4 Select the **Trunk Service Type** as **None**.

Step 5 Create an entry for the conference bridge in the **Destination** area by adding the IP address or hostname for the conference bridge. If you need a new line, you can click **(+)** to add it.

Step 6 From the **Normalization Script** drop-down list box, select a normalization script. For example, the following scripts are mandatory

- **cisco-telepresence-conductor-interop** – select this script if you are connecting this trunk to a Cisco TelePresence Conductor.
- **cisco-telepresence-mcu-ts-direct-interop** – select this script if you are connecting this trunk to a Cisco TelePresence MCU.
- **cisco-meeting-server-interop** – select this script if you are connecting this trunk to a Cisco Meeting Server.

Step 7 Complete any remaining fields in the Trunk Configuration window. For help with the fields and their settings, refer to the online help.

Step 8 Click Save.

CHAPTER 66

Configure Flexible DSCP Marking and Video Promotion

Flexible DSCP Marking and Video Promotion Overview

Devices and applications use Differentiated Services Code Point (DSCP) markings to indicate the Quality of Service (QoS) treatment of IP communications. For example, desktop video endpoints may use multimedia conferencing AF41 marking for video media streams, while high-definition video room systems may use real-time interactive CS4 marking. When an application sends and receives IP communications to and from the same type of application, the DSCP markings are symmetric, and the QoS treatments of the IP communications that each application sends and receives are the same. However, when an application sends and receives media to and from a different type of application, the DSCP markings may be asymmetric, and the QoS treatments of the IP communications that each application sends and receives may be inconsistent. For example, the QoS treatment of the video media stream that a video room system receives from a desktop video endpoint may be inadequate to support the expected quality of the video room system.

Devices and applications are subjected to Call Admission Control (CAC) to ensure that adequate bandwidth is available for the duration of established sessions. The bandwidth that is utilized by established sessions is updated as the sessions begin and end. Attempts to establish new sessions that would exceed the available bandwidth are blocked. The amount of bandwidth available may be tracked independently for devices and applications of different types. For example, independent tracking of bandwidth may be available for desktop video endpoints and high-definition video room systems to send and receive video media streams.

When devices and applications of the same type send and receive communications, the same type of bandwidth deductions are made in each direction. However, when devices and applications of different types send and receive communications, different types of bandwidth deductions must be made in each direction. Moreover, the bandwidth deductions are usually symmetric in amount, by design, to reflect the usual behavior of an IP network. As a result, when devices and applications of different types send and receive communications, the total bandwidth deductions may be up to double the amount of network bandwidth that is actually utilized. This inconsistency in bandwidth accounting may cause attempts to establish new sessions to be blocked unnecessarily.

The Flexible DSCP Marking and Video Promotion feature allows you to configure a Video Promotion policy that reconciles the inconsistency in bandwidth accounting in favor of the application that receives more favorable CAC and QoS treatment. For example, if a session between a desktop video endpoint and a high-definition video room system is reconciled in favor of the video room system, then the reconciliation is deemed a promotion for the desktop video endpoint.

When reconciliation is in effect between devices and applications of different types, bandwidth is deducted only for the type of application that is favored by reconciliation. If sufficient bandwidth is available for a session of this type to be admitted, the device or application of the type that is not favored by reconciliation is instructed to change the DSCP markings that it uses to those that are used by the device or application of the type that is favored by reconciliation. For example, if a desktop video endpoint is promoted in a session with a high-definition video room system, bandwidth accounting takes place as if the desktop video endpoint were an application of the same type as the video room system. The desktop video endpoint is instructed to change its DSCP markings to those that are used by the video room system. The QoS treatment is consistent in both directions, bandwidth is deducted for a session between devices and applications of the same type as the video room system, and bandwidth is not deducted for a session between devices and applications of the same type as the desktop video endpoint.

When you activate the Flexible DSCP Marking and Video Promotion feature, Unified Communications Manager dynamically signals desktop video devices a Traffic Class Label that is indicative of the DSCP marking for each negotiated media stream.

Custom QoS Settings for Users

You can customize Quality of Service (QoS) settings within a SIP profile and apply those settings to your users. The **SIP Profile Configuration** window has been enhanced with the following types of QoS settings:

- Custom DSCP values for audio and video streams
- Custom UDP port ranges for audio and video streams

Custom DSCP Values for Audio and Video

You can configure DSCP values for audio and video calls within a SIP profile and apply them to the SIP phones that use that profile. The **SIP Profile Configuration** window includes custom DSCP settings for the following types of calls:

- Audio calls
- Video calls
- Audio portion of a video call
- TelePresence calls
- Audio portion of a TelePresence call

If your company has a set of employees, such as a sales force, or a CEO, who require higher QoS priority settings than the majority of your employees, you can use the SIP profile configurations to configure custom DSCP values for those users. The settings within the SIP profile override the corresponding clusterwide service parameter settings.

Custom UDP Port Ranges for Audio and Video

You can configure separate UDP port ranges for the audio stream and video stream of a SIP call. Because video typically requires considerably more bandwidth than audio, creating dedicated port ranges for each media type simplifies network bandwidth management. It also protects against audio stream degradation by guaranteeing that the audio stream will have a dedicated channel that is separate from the higher-bandwidth video stream.

You can apply this configuration by setting the **Media Port Ranges** field in the SIP profile to **Separate Port Ranges for Audio and Video**. You can then apply the configuration to a phone by associating the SIP profile to a phone.

Traffic Class Label

The Flexible DSCP and Video Promotion feature uses the Traffic Class Label (TCL) to instruct the SIP endpoint dynamically to mark its DSCP on a per call basis, based on the Video Promotion policy that you configure. Because TCL is a SIP Session Description Protocol (SDP) attribute that is defined per media line, the TCL and its associated DSCP markings can be different for the audio media line and the video media line of a video call. You can choose different DSCP markings for the audio stream and the video stream of the video call.

DSCP Settings Configuration Task Flow

Perform the following tasks to configure DSCP values and a video promotion policy for your network.

Procedure

	Command or Action	Purpose
Step 1	Configure Flexible DSCP Marking and Video Promotion Policy, on page 515	Configure a video promotion policy to handle the different types of video.
Step 2	Configure Custom QoS Policy for Users, on page 517	If your company has users that require higher priority than other users in your company, configure a SIP Profile that includes custom DSCP values for audio and video streams. For example, if your company has a telephone sales force or CEO whom require higher priority, you can apply the customized SIP profile to those users' phones.

Configure Flexible DSCP Marking and Video Promotion Policy

Follow these steps to configure a video promotion policy to handle the different types of video.

Procedure

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

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

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

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

Step 4 To configure a Video Promotion policy that promotes desktop video endpoints to immersive video endpoints, set the **Use Video BandwidthPool for Immersive Video Calls** parameter to **False** and set the **Video Call QoS Marking Policy** parameter to **Promote to Immersive**.

Step 5 To configure other parameters, scroll to the appropriate area of the **Service Parameter Configuration** window and update the parameter values. See Flexible DSCP Marking and Video Promotion Service Parameters, on page 516 for information about the service parameters and their configuration options.

Step 6 Click **Save**.

Flexible DSCP Marking and Video Promotion Service Parameters

Note For more information about the service parameters, click the parameter name or click the question mark (?) icon that displays in the **Service Parameter Configuration** window.

Table 79: Flexible DSCP Marking and Video Promotion Service Parameters

Parameter	Description
Clusterwide Parameters (System - QoS)	This section of service parameters includes clusterwide DSCP values for a wide range of audio and video call types, including DSCP for audio calls, video calls, the audio portion of a video call, TelePresence calls, and the audio portion of a TelePresence call. It is highly recommended that you keep these parameters set to the default value unless a Cisco support engineer instructs otherwise.
Clusterwide Parameters (Call Admission Control)	
Video Call QoS Marking Policy	This parameter allows you to configure a Promote to Immersive policy that reconciles bandwidth allocation inconsistencies between a desktop video endpoint and a Cisco TelePresence immersive video endpoint in favor of the immersive endpoint. When promotion is performed, the audio and video bandwidth are reserved from the immersive bandwidth pool allocation. The policy of Promote to Immersive takes effect only for calls between an immersive video device and a desktop video device that supports flexible DSCP marking.
Clusterwide Parameters (System - Location and Region)	
Default Intraregion Max Immersive Video Call Bit Rate (Includes Audio)	This parameter specifies the default maximum total bit rate for each immersive video call within a particular region, when the **Use System Default** option is selected as the **Max Immersive Video Call Bit Rate** in the **Region Configuration** window for the relationship of the region with itself.

Parameter	Description
Default Interregion Max Immersive Video Call Bit Rate (Includes Audio)	This parameter specifies the default maximum total bit rate for each immersive video call between a particular region and another region, when the **Use System Default** option is selected as the **Max Immersive Video Call Bit Rate** in the **Region Configuration** window for the relationship of the region with the other region.
Use Video BandwidthPool for Immersive Video Calls	This parameter specifies whether Unified Communications Manager reserves bandwidth from the desktop video bandwidth pool for immersive video calls.

Configure Custom QoS Policy for Users

Perform the following tasks to set up a custom Quality of Service (QoS) policy for users. You may want to apply a custom policy if a set of users within your company has different QoS requirements from the rest of the company such as telephone sales force or a CEO.

Procedure

	Command or Action	Purpose
Step 1	Configure Custom QoS Settings in SIP Profile, on page 517	Configure a SIP Profile with customized DSCP values and a UDP port range for audio and video streams.
Step 2	Apply Custom QoS Policy to a Phone, on page 518	Apply the SIP Profile to a phone. The DSCP settings in the SIP Profile override the DSCP clusterwide service parameter settings..

Configure Custom QoS Settings in SIP Profile

Configure custom DSCP values and UDP port ranges for the phones that use this SIP Profile. You can use these settings to configure a customized QoS policy that you can apply to specific phones and users within your network. You may want to do this if you want to apply specific QoS settings to specific users within your enterprise, such as a sales force, or a CEO.

Procedure

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

Step 2 Perform either of the following steps:

- Click **Find** and select an existing SIP Profile.
- Click **Add New** to create a new SIP Profile.

Step 3 From the **Media Port Ranges** field, select whether you want to assign a single UDP port range that handles both audio and video media, or separate port ranges for audio and video streams.

- If you want to configure a single port range for audio and video media, enter the range of ports in the **Start Media Port** and **Stop Media Port** fields. The possible port values are between 2048 and 65535.

- If you want separate port ranges for audio and video streams, enter the range of audio ports using the **Start Audio Port** and **Stop Audio Port** fields. Enter the range of video ports using the **Start Video Port** and **Stop Video Port** fields. The possible port values for each are between 2048 and 65535.The two port ranges must not overlap.

Step 4 In the following fields, configure customized DSCP values for audio and video streams.

- DSCP for Audio Calls
- DSCP for Video Calls
- DSCP for Audio Portion of Video Calls
- DSCP for TelePresence Calls
- DSCP for Audio Portion of TelePresence Calls

Note By default, each of the above fields is configured to use the value from a corresponding service parameter. If you assign new values, the new value overrides the service parameter setting.

Step 5 Complete the remaining fields in the **SIP Profile Configuration** window. For help with the fields and their settings, refer to the online help.

Step 6 Click **Save**.

Apply Custom QoS Policy to a Phone

Use this procedure to apply a SIP Profile that contains customized QoS settings, including DSCP values and a UDP port range for audio and video media. When you apply this SIP profile to a phone, the phone uses the custom settings from the SIP Profile.

Procedure

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

Step 2 Perform any one of the following steps:

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

Step 3 From the **SIP Profile** drop-down list, select the SIP profile that you set up with the custom DSCP values and UDP port range values.

Step 4 Complete the remaining fields in the **Phone Configuration** window. For more information on the fields and their configuration options, see the system Online Help.

Step 5 Click **Save**.

Flexible DSCP Marking and Video Promotion Interactions and Restrictions

You can perform:

- Flexible DSCP Marking and Video Promotion Interactions, on page 519

Flexible DSCP Marking and Video Promotion Interactions

Table 80: Flexible DSCP Marking and Video Promotion Interactions

Device	Interaction
SIP Intercluster Trunks	The Flexible DSCP Marking and Video Promotion feature is supported over SIP intercluster trunks.
Skinny Client Control Protocol (SCCP) Devices	The Flexible DSCP Marking and Video Promotion feature is supported for SCCP devices.
Pass-Through MTPs	If pass-through MTPs are inserted in a call, Unified Communications Manager signals the MTP to mark the packets with the DSCP marking that is expected from the endpoint device that originally emitted the packet for the video stream. If the two endpoints on a call use different DSCP markings (for example, a Cisco TelePresence immersive video endpoint and a desktop video endpoint without Video Promotion), the MTPs preserve the DSCP marking in each stream direction.

Flexible DSCP Marking and Video Promotion Restrictions

Table 81: Flexible DSCP Marking and Video Promotion Restrictions

Restriction	Description
Trunks and gateways	The Flexible DSCP Marking and Video Promotion feature is not supported over H.323 trunks and Media Gateway Control Protocol (MGCP) gateways.
Multilevel Precedence and Preemption	Cisco recommends that you do not use the Flexible DSCP Marking and Video Promotion feature with Multilevel Precedence and Preemption (MLPP) service calls. When you need MLPP service functionality, Cisco recommends that you set the Video Call QoS Marking Policy and Use Video BandwidthPool for Immersive Video Calls service parameters to their default values. With default values for the Video Call QoS Marking Policy and Use Video BandwidthPool for Immersive Video Calls service parameters, Unified Communications Manager and endpoints use MLPP DSCP markings for the media packets.
SIP video endpoints	The Flexible DSCP Marking and Video Promotion feature is dependent on desktop SIP video endpoint support. Currently, only Cisco DX650 series SIP phones provide the required endpoint support.

CHAPTER 67

Configure Transcoders and Media Termination Points

Transcoders and Media Termination Points Overview

Transcoders

A transcoder is a device that performs codec conversion, it converts an input stream from one codec into an output stream that uses a different codec. For example, a transcoder can take a G.711 stream and convert it to a G.729 stream in real time. During a call when the endpoints use different voice codecs, the Cisco Unified Communications Manager invokes a transcoder into the media path. The transcoder converts the data streams between the two incompatible codecs to allow communication between the devices. The transcoder is invisible to the user or the endpoints involved in a call.

Transcoder resources is managed by the Media Resource Manager (MRM).

Note The transcoder supports transcoding between G.711 and all codecs, including G.711, when functioning as a transcoder and when providing MTP/TRP functionality.

Transcoders and the Media Resource Manager

All Cisco Unified Communications Manager nodes can access transcoders through the Media Resource Manager (MRM). The MRM manages access to transcoders.

The MRM makes use of Cisco Unified Communications Manager media resource groups and media resource group lists. The media resource group list allows transcoders to communicate with other devices in the assigned media resource group, which in turn, provides management of resources within a cluster.

A transcoder control process gets created for each transcoder device that is defined in the database. The MRM keeps track of the transcoder resources and advertises their availability throughout the cluster.

Transcoders as Media Termination Points

Hardware-based transcoder resources also support Media Termination Point (MTP) and/or Trust Relay Point (TRP) functionality. In this capacity, when Cisco Unified Communications Manager determines that an endpoint in a call requires an MTP or TRP, it can allocate a transcoder resource and inserts it into the call, where it acts like an MTP transcoder.

Cisco Unified Communications Manager supports MTP and TRP and transcoding functionality simultaneously. For example, if a call originates from a Cisco Unified IP Phone (located in the G723 region) to NetMeeting (located in the G711 region), one transcoder resource supports MTP and transcoding functionality simultaneously.

If a software MTP resource is not available when it is needed, the call tries to connect without using an MTP resource and MTP/TRP services. If hardware transcoder functionality is required (to convert one codec to another) and a transcoder is not available, the call will fail.

Note The transcoder supports transcoding between G.711 and all codecs, including G.711, when functioning as a transcoder and when providing MTP/TRP functionality.

Transcoder Types

Transcoder types in Cisco Unified Communications Manager Administration are listed in the following table.

Note The transcoder supports transcoding between G.711 and all codecs, including G.711, when functioning as a transcoder and when providing MTP/TRP functionality.

Table 82: Transcoder Types

Transcoder Type	Description
Cisco Media Termination Point Hardware	This type, which supports the Cisco Catalyst 4000 WS-X4604-GWY and the Cisco Catalyst 6000 WS-6608-T1 or WS-6608-E1, provides the following number of transcoding sessions: For the Cisco Catalyst 4000 WS-X4604-GWY • For transcoding to G.711-16 MTP transcoding sessions For the Cisco Catalyst 6000 WS-6608-T1 or WS-6608-E1 • For transcoding from G.723 to G.711/For transcoding from G.729 to G.711-24 MTP transcoding sessions per physical port; 192 sessions per module

Transcoder Type	Description
Cisco IOS Media Termination Point (hardware)	This type, which supports the Cisco 2600XM, Cisco 2691, Cisco 3725, Cisco 3745, Cisco 3660, Cisco 3640, Cisco 3620, Cisco 2600, and Cisco VG200 gateways, provides the following number of transcoding sessions: Per NM-HDV • Transcoding from G.711 to G.729-60 • Transcoding from G.711 to GSM FR/GSM EFR- 45
Cisco IOS Enhanced Media Termination Point (hardware)	**Per NM-HD** This type, which supports Cisco 2600XM, Cisco 2691, Cisco 3660, Cisco 3725, Cisco 3745, and Cisco 3660 Access Routers, provides the following number of transcoding sessions: • Transcoding for G.711 to G.729a/G.729ab/GSMFR-24 • Transcoding for G.711 to G.729/G.729b/GSM EFR-18 **Per NM-HDV2** This type, which supports Cisco 2600XM, Cisco 2691, Cisco 3725, Cisco 3745, and Cisco 3660 Access Routers, provides the following number of transcoding sessions: • Transcoding for G.711 to G.729a/G.729ab/GSMFR-128 • Transcoding for G.711 to G.729/G.729b/GSM EFR-96 **PVDM4** • Onboard PVDM4 modules (PVDM4-32, PVDM4-64, PVDM4-128, PVDM4-256) • DSP module on T1/E1 modules (PVDM4-32, PVDM4-64, PVDM4-128, PVDM4-256) • DSP NIMs (NIM-PVDM4-32, NIM-PVDM4-64, NIM-PVDM4-128, NIM-PVDM4-256) These types support ISR4K (ISR44xx, ISR43xx), C83xx, and C82xx platforms provide the following number of transcoding sessions: • Transcoding for G.711 to G.729a/G.729ab/GSMFR-24 • Transcoding for G.711 to G.729/G.729b/GSM EFR-18 • Transcoding for G.711 to G.729a/G.729ab/GSMFR-128 • Transcoding for G.711 to G.729/G.729b/GSM EFR-96 • Transcoding for G.711/G.729/G.729ab/G.729a/G.729b to Opus

Transcoder Type	Description
Cisco Media Termination Point (WS-SVC-CMM)	This type provides 64 transcoding sessions per daughter card that is populated: 64 transcoding sessions with one daughter card, 128 transcoding sessions with two daughter cards, 192 transcoding sessions with three daughter cards, and 256 transcoding sessions with four daughter cards (maximum). This type provides transcoding between any combination of the following codecs: • G.711 a-law and G.711 mu-law • G.729 annex A and annex B • G.723.1 • GSM (FR) • GSM (EFR)

Transcoder Failover and Fallback

The following items describe the transcoder device recovery methods when the transcoder is registered to a Cisco Unified Communications Manager node that goes inactive:

- If the primary Cisco Unified Communications Manager node fails, the transcoder attempts to register with the next available node in the Cisco Unified Communications Manager Group that is specified for the device pool to which the transcoder belongs.
- The transcoder device reregisters with the primary Cisco Unified Communications Manager node as soon as it becomes available.
- A transcoder device unregisters with a Cisco Unified Communications Manager node that becomes unreachable. The calls that were on that node will register with the next Cisco Unified Communications Manager node in the list.
- If a transcoder attempts to register with a new Cisco Unified Communications Manager node and the register acknowledgment is never received, the transcoder registers with the next node in the list.

Transcoder devices will unregister and then disconnect after a hard or soft reset. After the reset completes, the devices reregister with the primary Cisco Unified Communications Manager node.

Media Termination Points

Media Termination Points (MTP) allow Unified Communications Manager to relay calls that are routed through SIP or H.323 endpoints or gateways. Media Termination Points extend supplementary services, such as call hold, call transfer, call park, and conferencing, that are normally not available when a call is routed to an H.323 endpoint. For H.323 supplementary services, MTPs are only required for endpoints that do not support EmptyCapability Set (ECS) or FastStart. All Cisco and other third party other endpoints that support ECS and FastStart do not require an MTP.

An MTP device always registers with its primary Unified Communications Manager if that Unified Communications Manager is available and informs the Unified Communications Manager about the number of MTP resources it supports. You can register multiple MTPs with the same Unified Communications

Manager. When more than one MTP is registered with a Unified Communications Manager, that Cisco Unified Communications Manager controls the set of resources for each MTP.

For example, consider MTP server 1 as configured for 48 MTP resources, and the MTP server 2 as configured for 24 resources. If both MTPs register with the same Unified Communications Manager, that Unified Communications Manager maintains both sets of resources for a total of 72 registered MTP resources.

When the Unified Communications Manager determines that a call endpoint requires an MTP, it allocates an MTP resource from the MTP that has the least active streams. That MTP resource gets inserted into the call on behalf of the endpoint. MTP resource use remains invisible to both the users of the system and to the endpoint on whose behalf it was inserted. If an MTP resource is not available when it is needed, the call connects without using an MTP resource, and that call does not have supplementary services.

MTP Failover and Fallback

This section describes how MTP devices failover and fallback when the Cisco Unified Communications Manager to which they are registered becomes unreachable:

- If the primary Cisco Unified Communications Manager fails, the MTP attempts to register with the next available Cisco Unified Communications Manager in the Cisco Unified Communications Manager Group that is specified for the device pool to which the MTP belongs.
- The MTP device reregisters with the primary Cisco Unified Communications Manager as soon as it becomes available after a failure and is currently not in use.
- The system maintains the calls or conferences that were active in call preservation mode until all parties disconnect. The system does not make supplementary services available.
- If an MTP attempts to register with a new Cisco Unified Communications Manager and the register acknowledgment is never received, the MTP registers with the next Cisco Unified Communications Manager.

The MTP devices unregister and then disconnect after a hard or soft reset. After the reset completes, the devices reregister with the Cisco Unified Communications Manager.

Software Media Termination Point Type

Software Media Termination Point type in Cisco Unified Communications Manager Administration is listed in the following table.

Software MTP Type	Description
Cisco Media Termination Point Software	A single MTP provides a default of 48 MTP (user configurable) resources, depending on the speed of the network and the network interface card (NIC). For example, a 100-MB Network/NIC card can support 48 MTP resources, while a 10-MB NIC card cannot. For a 10-MB Network/NIC card, approximately 24 MTP resources can be provided; however, the exact number of MTP resources that are available depends on the resources that other applications on that PC are consuming, the speed of the processor, network loading, and various other factors.

Transcoders and MTPs Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	To Configure Transcoders, on page 526,complete the following sub tasks: • Configure Transcoders, on page 527 • Add Transcoder to Media Resource Group, on page 527	If you need to configure a transcoder, follow this step. Transcoders convert an input stream from one codec into an output stream that uses a different codec.
Step 2	To Configure a Software MTP, on page 528, complete the following sub tasks: • Configure Media Termination Points, on page 529 • Add Software MTP to Media Resource Group, on page 529	If you need to configure a software MTP, follow this step. Software MTPs allow Cisco Unified Communications Manager to relay calls that are routed through SIP or H.323 endpoints or gateways.

Configure Transcoders

Procedure

	Command or Action	Purpose
Step 1	Determine the number of transcoder resources that are needed and the number of transcoder devices that are needed to provide these resources.	For a multi-site deployment, Cisco recommends placing a transcoder local at each site where it might be required. If multiple codecs are needed, it is necessary to know how many endpoints do not support all codecs, where those endpoints are located, what other groups will be accessing those resources, how many maximum simultaneous calls these device must support, and where those resources are located in the network.
Step 2	Configure Transcoders, on page 527	Configure transcoders to convert an input stream from one codec into an output stream that uses a different codec.
Step 3	Add Transcoder to Media Resource Group, on page 527	Add the new transcoders to the appropriate media resource groups.
Step 4	Restart the transcoder devices.	See the transcoder documentation for details.

Configure Transcoders

A transcoder is a device that converts an input stream from one codec into an output stream that uses a different codec.

Before you begin

The Cisco IP Voice Media Streaming service must be running for the IVR to be active.

Determine the number of transcoder resources that are needed and the number of transcoder devices that are needed to provide these resources.

Procedure

Step 1 Log into Cisco Unified CM Administration and choose **Media Resources** > **Transcoder**.

Step 2 Do either of the following:

- Click **Find** and select an existing transcoder.
- Click **Add New**.

Step 3 Select the **Transcoder Type**.

Step 4 Enter the **MAC Address** of the transcoder.

Step 5 Assign a **Device Pool** from the drop-down menu.

Step 6 Check the **Trusted Relay Point** check box if you want to make this transcoder available as a trusted relay point.

Step 7 Click **Save**.

Add Transcoder to Media Resource Group

Before you begin

Configure Transcoders, on page 527

Procedure

Step 1 Choose **Media Resources** > **Media Resource Group**.

Step 2 Click **Find** to display the list of configured Media Resource Groups.

Step 3 Click on the required Media Resource Group.
The **Media Resource Group Configuration** window displays.

Step 4 Select the transcoder from the list of available media resources and add it to the Selected Media Resources list.

Step 5 Click **Save**.

Step 6 Navigate to **Media Resources** > **Media Resource Group**.

Step 7 In the **Find and List Transcoders** window, 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 8 Click **Apply Config to Selected**.

The Apply Configuration Information dialog box displays.

Step 9 Click **OK**.

What to do next

Restart the transcoder device.

Synchronize Transcoder

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

Procedure

Step 1 Choose **Media Resources** > **Transcoder**.
The Find and List Transcoders window displays.

Step 2 Choose the search criteria to use.

Step 3 Click **Find**.

The window displays a list of transcoders that match the search criteria.

Step 4 Check the check boxes next to the transcoders that you want to synchronize. To choose all transcoders in the window, check the check box in the matching records title bar.

Step 5 Click **Apply Config to Selected**.
The Apply Configuration Information dialog box displays.

Step 6 Click **OK**.

Configure a Software MTP

This procedure describes the steps to configure a software MTP. For information about configuring a hardware MTP, see Configure Transcoders, on page 526.

Procedure

	Command or Action	Purpose
Step 1	Configure Media Termination Points, on page 529	Configure a media termination point to relay calls that are routed through SIP endpoints or gateways.
Step 2	Add Software MTP to Media Resource Group, on page 529	Add the new media termination point to the appropriate media resource groups.
Step 3	Restart the media termination point devices.	

Configure Media Termination Points

Use this procedure to configure a software Media Terminiation Point (MTP).

Before you begin

The Cisco IP Voice Media Streaming service must be running for the software Media Termination Point (MTP) to be active.

Determine the number of MTP resources that are needed and the number of MTP devices that are needed to provide these resources.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Media Resources** > **Media Termination Point**.

Step 2 Do either of the following:

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

Step 3 Assign a **Media Termination Point Name**.

Step 4 Assign a **Device Pool**.

Step 5 Check the **Trusted Relay Point** check box if you want to designate this MTP as a Trusted Relay Point (TRP).

Step 6 Click **Save**.

Add Software MTP to Media Resource Group

Before you begin

Configure Media Termination Points, on page 529

Procedure

Step 1 Choose **Media Resources** > **Media Resource Group**.

Step 2 Click **Find** to display the list of configured Media Resource Groups.

Step 3 Click on the required Media Resource Group.
The **Media Resource Group Configuration** window displays.

Step 4 Select the transcoder from the list of **Available Media Resources** and add it to the **Selected Media Resources** list.

Step 5 Click **Save**.

What to do next

Restart the media termination point device.

Transcoders and MTPs Interactions and Restrictions

Transcoder Interactions and Restrictions

Transcoder Interactions and Restrictions

Interactions or Restriction	Description
Transcoder Deletion	You cannot delete a transcoder that is assigned to a media resource group. To find out which media resource groups are using the transcoder, click **Dependency Records** from the **Related Links** drop-down list box on the **Transcoder Configuration** window and click **Go**. The Dependency Records Summary window displays information about media resource groups that are using the transcoder. To find out more information about the media resource group, click the media resource group, and the Dependency Records Details window displays. If the dependency records are not enabled for the system, the dependency records summary window displays a message. 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.
Failover and Fallback	Transcoder failover and fallback works as follows: • If the primary Unified Communications Manager node fails, the transcoder attempts to register with the next available node in the Unified Communications Manager Group that is specified for the device pool to which the transcoder belongs. • The transcoder device reregisters with the primary Cisco Unified Communications Manager node as soon as it becomes available. • A transcoder device unregisters with a Unified Communications Manager node that becomes unreachable. Calls that were using this transcoding profile for transcoding move to the preservation state and the transcoder attempts to register with the next available node. Gateway uses RTP/ RTCP timeout to inform to registered Unified Communications Manager of resource release. • If a transcoder attempts to register with a new Unified Communications Manager node and the register acknowledgment is never received, the transcoder registers with the next node in the list. Transcoder devices will unregister and then disconnect after a hard or soft reset. After the reset completes, the devices reregister with the primary Cisco Unified Communications Manager node.

Media Termination Points Interactions and Restrictions

Table 83: Media Termination Points Interactions and Restrictions

Restriction	Description
Cisco IP Voice Streaming Application	You can activate only one Cisco IP Voice Streaming Application per server. To provide more MTP resources, you can activate the Cisco IP Voice Streaming application on additional networked servers. Cisco strongly recommends that you do not activate the Cisco IP Voice Streaming Media Application on a Cisco Unified Communications Manager with a high call-processing load because it can adversely affect the performance of the Cisco Unified Communications Manager.
Registering with Cisco Unified Communoications Manager	Each MTP can register with only one Cisco Unified Communications Manager at a time. The system may have multiple MTPs, each of which may be registered to one Cisco Unified Communications Manager, depending on how your system is configured.
Failover and Fallback	This section describes how MTP devices failover and fallback when the Cisco Unified Communications Manager to which they are registered becomes unreachable: • If the primary Cisco Unified Communications Manager fails, the MTP attempts to register with the next available Cisco Unified Communications Manager in the Cisco Unified Communications Manager Group that is specified for the device pool to which the MTP belongs. • The MTP device reregisters with the primary Cisco Unified Communications Manager as soon as it becomes available after a failure and is currently not in use. • The system maintains the calls or conferences that were active in call preservation mode until all parties disconnect. The system does not make supplementary services available. • If an MTP attempts to register with a new Cisco Unified Communications Manager and the register acknowledgment is never received, the MTP registers with the next Cisco Unified Communications Manager. The MTP devices unregister and then disconnect after a hard or soft reset. After the reset completes, the devices reregister with the Cisco Unified Communications Manager.

PART IX

Register Devices

CHAPTER 68

Register Devices Overview

About Registering Devices

The chapters in this section describe the tasks that you perform to register new endpoint devices and to set up proxy TFTP servers for your endpoints and gateway devices.

You can choose to register new phones manually or use autoregistration. To register more than 100 phones, use the Bulk Administration Tool (BAT). For more information, see *Cisco Unified Communications Manager Bulk Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Note You cannot create new settings using BAT, but you can configure phone parameters when you use the BAT to register phones. Make sure that phone settings such as device pool, location, calling search space, button template, and softkey templates have already been configured using Cisco Unified Communications Manager Administration.

Registering Devices

Complete the following task flows to register devices for your system.

Procedure

	Command or Action	Purpose
Step 1	TFTP Server Configuration Task Flow, on page 540	Configure the proxy Trivial File Transfer Protocol (TFTP) server that provides the configuration files for endpoints in your network.

	Command or Action	Purpose
Step 2	(Optional) Update Device Defaults Task Flow, on page 545	Modify the device load, device pool, and the phone button template values that are applied to endpoints when they register.
Step 3	Configure Autoregistration Task Flow, on page 549	Enable autoregistration for your network. Because of the inherent security risk of allowing devices to register automatically on the network, we recommend that you disable autoregistration as soon as you have registered your new endpoints.
Step 4	Manual Device Registration Task Flow, on page 557	Manually register an IP phone and assign a new directory number.
Step 5	Self-Provisioning Configuration Task Flow, on page 562	Optional. If you want your end users to be able to provision their own phones without the aid of an administrator, configure self-provisioning.

CHAPTER 69

Configure TFTP Servers

Proxy TFTP Deployment Overview

Use a proxy Trivial File Transfer Protocol (TFTP) server to provide the configuration files that endpoints in your network need, such as: dial plans, ringer files, and device configuration files. A TFTP server can be installed in any cluster in your deployment and can service requests from endpoints on multiple clusters. The DHCP scope specifies the IP address of the proxy TFTP server to use to get the configuration files.

Redundant and Peer Proxy TFTP Servers

In a single cluster deployment, the cluster must have at least one proxy TFTP server. You can add another proxy TFTP server to the cluster for redundancy. The second proxy TFTP server is added in option 150 for IPv4. For IPv6, you add the second proxy TFTP server to TFTP Server Addresses sub-option type 1 in the DHCP scope.

In a multiple cluster deployment, you can specify up to three remote proxy TFTP servers as peer clusters of the primary proxy TFTP server. This is useful if you want to configure only one proxy TFTP server for many DHCP scopes, or have only one DHCP scope. The primary proxy TFTP server provides the configuration files for all phones and devices in the network.

You must create a peer relationship between each remote proxy TFTP server and the primary proxy TFTP server.

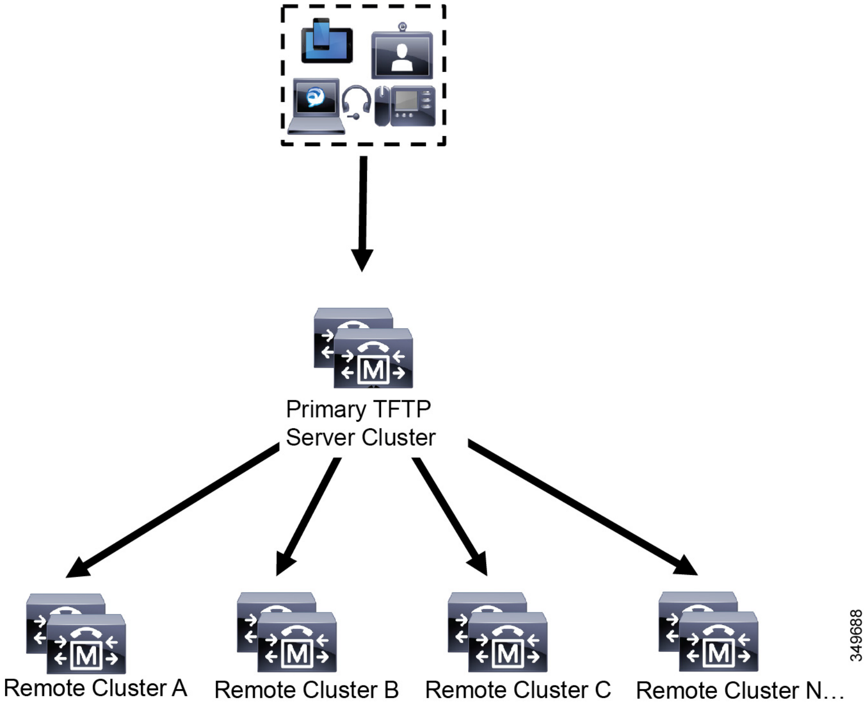
Tip When you configure peer relationships between the remote proxy TFTP servers in your network, keep the relationships hierarchical. Ensure that the peer proxy TFTP servers on the remote clusters do not point to each other to avoid possible looping. For example, if the primary node A has a peer relationship with nodes B and C. You should not create a peer relationship between nodes B and C. If you do, then you have created a loop.

Proxy TFTP

In multi-cluster systems, the proxy TFTP service is able provide TFTP files from multiple clusters via a single primary TFTP server. The proxy TFTP can serve as a single TFTP reference for scenarios where a single subnet or VLAN contains phones from multiple clusters or in any scenario where multiple clusters share the same DHCP TFTP option (150).

The Proxy TFTP service functions as a single-level hierarchy is as illustrated. More complicated multi-level hierarchies are not supported.

Figure 5: Proxy TFTP Single-Level Hierarchy



In the above illustration, a group of devices contacts the Primary TFTP server for their configuration files. When it receives a request for TFTP from a device, the primary TFTP looks into its own local cache for the configuration file as well as any other remotely configured clusters such as Remote Cluster A, B, C, or N (any other remote clusters configured).

It is possible to configure any number of remote clusters on the primary TFTP server; however, each remote cluster may contain only up to 3 TFTP IP addresses. The recommended design for redundancy is 2 TFTP servers per cluster, and thus 2 IP addresses per remote cluster on the Primary TFTP server for redundancy.

Use Cases and Best Practices

Consider the following scenarios that detail how Proxy TFTP can be used and the best practices for implementation.

1. The cluster can act as just a proxy TFTP cluster with no other purpose. In this case, the cluster has no relationship with the other clusters, and does not process calls. For this scenario, the Remote Cluster TFTP is manually defined and rollback to pre-8.0 is recommended.

Note Autoregistration will not work in this scenario.

2. The cluster is a remote cluster that is also acting as a Proxy TFTP server for remote clusters. The remote cluster is manually defined, and Autoregistration should not be enabled.

TFTP Support for IPv4 and IPv6 Devices

We recommend that you enable IPv4 phones and gateways to use the DHCP custom option 150 to discover the TFTP server IP address. Using option 150, gateways and phones discover the TFTP server IP address. For more information, see the documentation that came with your device.

In an IPv6 network, we recommend that you use the Cisco vendor-specific DHCPv6 information to pass the TFTP server IPv6 address to the endpoint. With this method, you configure the TFTP server IP address as the option value.

If you have some endpoints that use IPv4 and some that use IPv6, we recommend that you use DHCP custom option 150 for IPv4 and use the TFTP Server Addresses sub-option type 1, a Cisco vendor-specific information option, for IPv6. If the endpoint obtains an IPv6 address and sends a request to the TFTP server while the TFTP server is using IPv4 to process requests, the TFTP server does not receive the request because the TFTP server is not listening for the request on the IPv6 stack. In this case, the endpoint cannot register with Cisco Unified Communications Manager.

There are alternative methods that you could use for your IPv4 and IPv6 devices to discover the IP address of the TFTP server. For example, you could use DHCP option 066 or CiscoCM1 for your IPv4 devices. For your IPv6 devices, other methods include using TFTP Service sub-option type 2 or configuring the IP address of the TFTP server on the endpoint. These alternative methods are not recommended. Consult your Cisco service provider before using any alternative methods.

Endpoints and Configuration Files for TFTP Deployments

SCCP phones, SIP phones and gateways, request a configuration file when they initialize. An updated configuration file gets sent to the endpoint whenever you change the device configuration.

The configuration file contains information such as a prioritized list of Unified Communications Manager nodes, the TCP ports used to connect to those nodes, as well other executables. For some endpoints, the configuration file also contains locale information and URLs for phone buttons, such as: messages, directories, services, and information. Configuration files for gateways contain all the configuration information that the device requires.

Security Considerations for Proxy TFTP

Cisco Proxy TFTP servers handle both signed and unsigned requests and run in either nonsecure mode or mixed mode. The Proxy TFTP Server searches the local file system or database when a phone requests for a file and if not found, sends a request to remote clusters. When the phone requests the server for a common file with names such as `ringlist.xml.sgn, locale file`, and so on, the server sends a local copy of the file instead of the file itself from the home cluster of the phone.

When receiving files from Proxy TFTP, the phone rejects the file due to a signature verification failure because the file has the signature of the proxy server which doesn't match the Initial Trust List (ITL) of the phone. To resolve this issue, you can either disable Security By Default (SBD) for the Phone or import Proxy TFTP's callmanager certificate to new (remote/home) clusters phone-sast-trust. Then the phones can reachout to Trust Verification Service (TVS) and trust the Proxy TFTP certificats. Bulk certificate exchange is needed if EMCC is enabled on the deployment

To disable Security by Default, see "Update ITL File for Cisco Unified IP Phones" section the Security Guide for Cisco Unified Communications Manager.

Proxy TFTP in Mixed Mode

TFTP servers on remote clusters that are running in mixed mode must have the primary Proxy TFTP server certificates added to their Cisco Certificate Trust List (CTL) file. Otherwise, endpoints that are registered to a cluster where security is enabled will be unable to download the files that they need. To achieve this update CTL file after performing bulk import-export of certificates.

For more information, see "Bulk Certificate Export" section in the Security Guide for Cisco Unified Communications Manager when migrating IP phones between clusters to perform the bulk certificate export.

Moving Phones Between Clusters in Proxy TFTP Environment

When moving phones from one Remote Cluster to another in a Proxy TFTP environment, perform the following:

1. Add Phone details to Remote Cluster B (destination cluster).
2. Delete Phone details from Remote Cluster A (source cluster).

Note The phone's configuration in the Proxy TFTP takes 30 minutes to expire. To avoid any file not found response, you can restart Proxy Cluster's TFTP services.

3. Reset Phones to download configuration files from Remote Cluster B and register to Remote Cluster B.

TFTP Server Configuration Task Flow

You can let the system dynamically configure the proxy TFTP server if you have Extension Mobility Cross Cluster (EMCC) configured for your cluster. If you don't, then you can set up the TFTP server and set the security mode manually.

Procedure

	Command or Action	Purpose
Step 1	Set up the TFTP server using one of the following methods: • Configure TFTP Server Dynamically, on page 541 • Configure TFTP Server Manually, on page 541	If you have Intercluster Lookup Service (ILS) configured, you can set up your TFTP server dynamically. If you don't have EMCC configured, set up your TFTP server manually. You must indicate if the cluster is secured or non-secured. The cluster is treated as non-secure by default.
Step 2	(Optional) Update the CTL File for TFTP Servers, on page 542	Install the CTL client plug-in and add the primary proxy TFTP server to the Cisco Certificate Trust List (CTL) file of all proxy TFTP servers in all remote clusters that are operating in mixed-mode.

	Command or Action	Purpose
Step 3	(Optional) See the documentation that supports your endpoint device.	Add the proxy TFTP servers to the Trust Verification List (TVL) of all remote endpoints if your proxy TFTP deployment has remote clusters.
Step 4	(Optional) Modify Non-Configuration Files for the TFTP Server, on page 543	You can modify non-configuration files that the end points request from the proxy TFTP server.
Step 5	(Optional) Stop and Start the TFTP service, on page 543	Stop and restart the TFTP service on the proxy TFTP node if you have uploaded modified non-configuration files for your endpoints.
Step 6	(Optional) See the documentation that supports your DHCP server.	For multiple cluster deployments, modify the DHCP scope for individual remote nodes to include the IP address of the primary proxy TFTP server.

Configure TFTP Server Dynamically

You can configure a Cisco proxy TFTP server dynamically if you have Intercluster Lookup Service (ILS) configured for your network.

Before you begin

Configure EMCC for your network. For more information, see the *Features and Services Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Procedure

In Cisco Unified Communications Manager Administration, choose **Advanced Features** > **Cluster View** > **Update Remote Cluster Now**. The TFTP server is automatically configured for the cluster.

What to do next

You must add any remote proxy TFTP servers to the Trust Verification Lists (TVL) of the endpoints; otherwise, they will not accept the configuration files from the proxy TFTP server that is on a remote cluster. See the documentation that supports your endpoint device for instructions.

Configure TFTP Server Manually

To configure TFTP in your network when you don't have EMCC configured, you must use the manual procedure.

You set up peer relationships between the primary proxy TFTP server and other TFTP servers from the Cluster View. You can add up to three peer TFTP servers.

Each remote TFTP server in the proxy TFTP deployment must include a peer relationship to the primary proxy TFTP server. To avoid creating a loop, ensure that the peer TFTP servers on the remote clusters do not point to each other.

Procedure

Step 1 Create a remote cluster. Perform the following actions:

a) From Cisco Unified CM Administration, select **Advanced Features** > **Cluster View**.
b) Click **Add New**. The **Remote Cluster Configuration** window appears.
c) Enter a cluster ID and a Fully Qualified Domain Name (FQDN) of up to 50 characters for the TFTP server, then click **Save**.

   Valid values for the cluster ID include alphanumeric characters, period (.), and hyphen (-). Valid values for the FQDN include alphanumeric characters, period (.), dash (-), asterisk (*), and space.

d) (Optional) In the **Remote Cluster Service Configuration** window, enter a description of up to 128 characters for the remote cluster.

   Do not use quotes ("), closed or open angle brackets (> <), backslash (\), dash (-), ampersand (&), or the percent sign (%).

Step 2 Check the **TFTP** check box to enable TFTP for the remote cluster.

Step 3 Click **TFTP**.

Step 4 In the **Remote Cluster Service Manually Override Configuration** window, select **Manually configure remote service addresses**.

Step 5 Enter the IP addresses of the TFTP server to create a peer relationships to those TFTP servers.

You can enter up to three TFTP server IP addresses.

Step 6 (Optional) Check the **Cluster is Secure** check box if the proxy TFTP server is deployed in a secured cluster.

Step 7 Click **Save**.

What to do next

You must add any remote TFTP servers to the Trust Verification Lists (TVL) of the endpoints; otherwise, they will not accept the configuration files from the proxy TFTP server that is on a remote cluster. See the documentation that supports your endpoint device for instructions.

Update the CTL File for TFTP Servers

Update the CTL file from publisher node by running `utils ctl` in each cluster which is in mixed mode. Make sure that a complete security network is attained between the Proxy TFTP server and all the clusters, that is bulk import and export exchange of certificates between Proxy and remote clusters.

While using CTLClient, you must add the primary TFTP server or the IP address of the primary TFTP server to the Cisco Certificate Trust List (CTL) file of all TFTP servers in remote clusters that are running in mixed mode. This is necessary so that endpoints in security-enabled clusters can successfully download their configuration files.

For more information about security and using the Cisco CTL CLI, see the "About Cisco CTL Setup" section in the Security Guide for Cisco Unified Communications Manager.

Procedure

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

Step 2 Click **Find** to list of all the plug-ins that you can install.

Step 3 Click the **Download** link for the Cisco CTL Client.
The system installs the client that digitally signs certificates stored on the TFTP server.

Step 4 Reboot the TFTP server.

Modify Non-Configuration Files for the TFTP Server

You can modify a non-configuration file, such as a load file or `RingList.xml`, that the endpoints request from the proxy TFTP server. After you complete this procedure, upload the modified files to the TFTP directory of the proxy TFTP server.

Procedure

Step 1 In Cisco Unified Communications Operating System Administration, select **Software Upgrades** > **TFTP File Management**.
The **TFTP File Management** window appears.

Step 2 Click **Upload File**.
The **Upload File** pop-up appears.

Step 3 Perform one of the following actions:

- Click **Browse** to browse to the directory location of the file to upload.
- Paste the full directory path of the updated file in to the **Directory** field.

Step 4 Click **Upload File** or click **Close** to exit without uploading the file.

What to do next

Stop and restart the Cisco TFTP service on the proxy TFTP node using Cisco Unified Serviceability Administration.

Stop and Start the TFTP service

Use the following procedure to stop and restart the TFTP service on the proxy TFTP node.

For more information about service activation, deactivation, and restarts, see the *Cisco Unified Serviceability Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Procedure

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

Step 2 In the **Control Center–Feature Services** window, select the proxy TFTP node in the **Server** drop-down list.

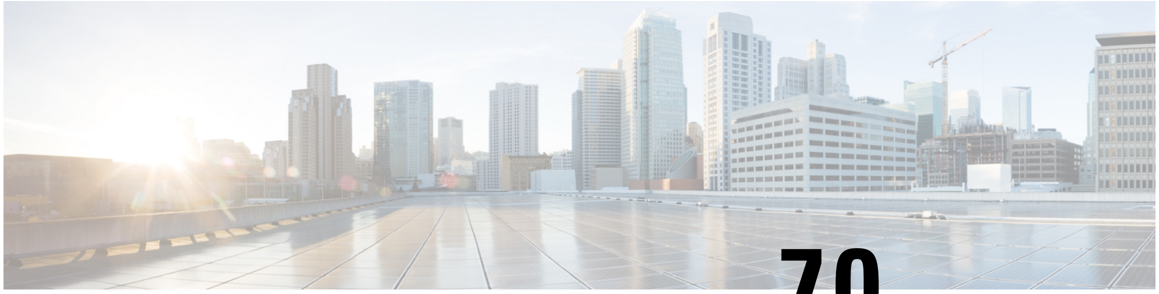
Step 3 Select the TFTP service in the **CM Services** area and click **Stop**.

The status changes to reflect the updated status.

Tip To see the latest status of services, click **Refresh**.

Step 4 Select the TFTP service in the **CM Services** area, then click **Start**.

The status changes to reflect the updated status.



CHAPTER 70

Update Device Defaults

Device Defaults Overview

Each device that registers with a Cisco Unified Communications Manager node is configured with the defaults for that type of device. Device defaults are applied to all auto-registering devices in the cluster. After registration, you can change the device's configuration.

You cannot create new device defaults or delete existing ones, but you can change the default settings that get applied to devices that auto-register.

These are the device default settings that you can change.

- Device load
- Device pool
- Phone button template

Installing a Cisco Unified Communications Manager automatically sets device defaults.

Update Device Defaults Task Flow

Procedure

	Command or Action	Purpose
Step 1	Update Device Default Settings, on page 546	You can change the default settings that are applied to devices that auto-register with a Cisco Unified Communications Manager node. Each type of device has a specific set of defaults.

Update Device Default Settings

Use this procedure to configure Device Default settings that allow you to assign default firmware loads, default device pools, softkey templates and the registration method: auto registration.

Before you begin

Before updating the device default settings, perform any of the following tasks that apply to your system.

- Add new firmware files for the devices to the TFTP server.
- If you use device defaults to assign a firmware load that does not exist in the directory, those devices will fail to load the assigned firmware.
- Configure new device pools. If the device is a phone, configure new phone templates.

Procedure

Step 1 In Cisco Unified CM Administration, select **Device** > **Device Settings** > **Device Defaults**.

Step 2 In the **Device Defaults Configuration** window, modify the applicable settings for the type of device that you want to update, then click **Save**. For field descriptions, see the online help.

- Load Information
- Device Pool
- Phone Template

Step 3 Click the **Reset** icon that appears to the left of the device name to reset all the devices of that type and load the new defaults to all devices of that type on all nodes in the cluster.

If you do not reset all devices, then only new devices that auto-register on the node are configured with the updated default values.

Device Defaults Settings

Table 84: Device Defaults Settings

Field Name	Description
Device Type	This field displays the type of device to which the defaults apply.
Protocol	This field displays the protocol that is used for this type of device.
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 to associate with each type of device. The device pool defines common characteristics for all devices in the pool.

Field Name	Description
Phone Template	Choose the phone button template that each type of Cisco IP Phone uses. The template defines the function of the keys on the phone.

CHAPTER 71

Configure Autoregistration

Autoregistration Overview

Autoregistration allows Unified Communications Manager to automatically assign directory numbers to new phones when you plug those phones in to your network.

Autoregistration is enabled on secure mode now. This enhancement provides greater security for your system because you can secure your cluster while provisioning new phones. It also simplifies the registration process because you don't have to disable cluster security to register new phones.

If you create a device pool that allows only 911 (emergency) and 0 (operator) calls, you can use that to prevent unauthorized endpoints from connecting to your network when autoregistration is enabled. New endpoints can register to this pool, but their access is limited. Unauthorized access by rogue devices that continuously boot in and attempt to register to your network is prevented. You can move a phone that has auto-registered to a new location and assign it to a different device pool without affecting its directory number.

The system doesn't know whether the new phones that are auto-registering are running SIP or SCCP, so you must specify this when you enable autoregistration. Devices that support both SIP and SCCP (such as Cisco IP Phones 7911, 7940, 7941, 7960, 7961) auto-register with the protocol that is specified in the enterprise parameter called Auto Registration Phone Protocol.

Devices that support only a single protocol will auto-register with that protocol. The Auto Registration Phone Protocol setting is ignored. For example, any Cisco IP Phones that support SCCP only will autoregister with SCCP even if the Auto Registration Phone Protocol parameter is set to SIP.

We recommend that you use autoregistration to add fewer than 100 phones to your network. To add more than 100 phones, use the Bulk Administration Tool (BAT). For more information, see *Cisco Unified Communications Manager Bulk Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Configure Autoregistration Task Flow

Enabling autoregistration carries a security risk. Enable autoregistration only for brief periods while you add new endpoints to the network.

Procedure

	Command or Action	Purpose
Step 1	Configure a Partition for Autoregistration, on page 550	Configure a route partition to use specifically for autoregistration to limit auto-registered phones to internal calls only.
Step 2	Configure a Calling Search Space for Autoregistration, on page 551	Configure a calling search space to use specifically for autoregistration to limit auto-registered phones to internal calls only.
Step 3	Configure a Device Pool for Autoregistration, on page 552	Create a device pool that uses the calling search space that is configured for autoregistration.
Step 4	Set the Device Protocol Type for Autoregistration, on page 553	Use this procedure to set the protocol to SCCP or SIP to match the type of phones you are auto-registering.
Step 5	Enable Autoregistration, on page 553	Enable autoregistration on the node to use for autoregistration and set the **Auto-registration Cisco Unified Communications Manager Group** parameter to enable autoregistration for the Cisco Unified Communications Manager group that is to be used for autoregistration.
Step 6	Disable Autoregistration, on page 555	Disable autoregistration for the node as soon as you are finished registering new devices.
Step 7	Reuse Autoregistration Numbers, on page 556	Optional. Autoregistration numbers for devices that have been disabled can be reused. When you reset the range of autoregistration directory numbers, you force the system to search again from the starting number. Available directory numbers are reused.

Configure a Partition for Autoregistration

Configure a route partition to use specifically for autoregistration to limit auto-registered phones to internal calls only.

Procedure

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

Step 2 Click **Add New** to create a new partition.

Step 3 In the **Partition Name, Description** field, enter a name for the partition that is unique to the route plan.

Partition names can contain alphanumeric characters, as well as spaces, hyphens (-), and underscore characters (_). See the online help for guidelines about partition names.

Step 4 Enter a comma (,) after the partition name and enter a description of the partition on the same line.

The description can contain up to 50 characters in any language, but it cannot include double quotes ("), percentage sign (%), ampersand (&), backslash (\), angle brackets (<>), or square brackets ([ ]).

If you do not enter a description, Cisco Unified Communications Manager automatically enters the partition name in this field.

Step 5 To create multiple partitions, use one line for each partition entry.

Step 6 From the **Time Schedule** drop-down list, choose a time schedule to associate with this partition.

The time schedule specifies when the partition is available to receive incoming calls. If you choose **None**, the partition remains active at all times.

Step 7 Select one of the following radio buttons to configure the **Time Zone**:

- **Originating Device**—When you select this radio button, the system compares the time zone of the calling device to the **Time Schedule** to determine whether the partition is available is available to receive an incoming call.
- **Specific Time Zone**—After you select this radio button, choose a time zone from the drop-down list. The system compares the chosen time zone to the **Time Schedule** to determine whether the partition is available is available to receive an incoming call.

Step 8 Click **Save**.

What to do next

Configure a Calling Search Space for Autoregistration, on page 551

Configure a Calling Search Space for Autoregistration

Configure a calling search space to use specifically for autoregistration to limit auto-registered phones to internal calls only.

Before you begin

Configure a Partition for Autoregistration, on page 550

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **Calling Search Space**.

Step 2 Click **Add New**.

Step 3 In the **Name** field, enter a name.

Ensure that each calling search space name is unique to the system. The name can include up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_).

Step 4 In the **Description** field, enter a description.

The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).

Step 5 From the **Available Partitions** drop-down list, perform one of the following steps:

- For a single partition, select that partition.

- For multiple partitions, hold down the **Control (CTRL)** key, then select the appropriate partitions.

Step 6 Select the down arrow between the boxes to move the partitions to the **Selected Partitions** field.

Step 7 (Optional) Change the priority of selected partitions by using the arrow keys to the right of the **Selected Partitions** box.

Step 8 Click **Save**.

What to do next

Configure a Device Pool for Autoregistration, on page 552

Related Topics

Class of Service, on page 118

Configure a Device Pool for Autoregistration

You can use the Default device pool for autoregistration or configure separate device pools for SIP and SCCP devices to use for autoregistration.

To configure the Default device pool for autoregistration, assign the Default Cisco Unified Communications Manager Group and the autoregistration calling search space (CSS) to the Default device pool. If you choose to configure a separate default device pool for SIP and SCCP devices, use the default device pool values.

Before you begin

Configure a Calling Search Space for Autoregistration, on page 551

Procedure

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

Step 2 To modify the Default device pool for autoregistration, perform the following actions:

a) Click **Find**, then select **Default** from the list of device pools.

b) In the **Device Pool Configuration** window, select the CSS to be used for autoregistration in the **Calling Search Space for Auto-registration** field, then click **Save**.

Step 3 To create a new device pool for autoregistration, perform the following actions:

a) Click **Add New**.

b) In the **Device Pool Configuration** window, enter a unique name for the device pool.

   You can enter up to 50 characters, which include alphanumeric characters, periods (.), hyphens (-), underscores (_), and blank spaces.

c) Set the following fields to match the Default device pool. See the online help for field descriptions.

   - In **Cisco Unified Communications Manager Group**, select **Default**.
   - In **Date/Time Group**, select **CMLocal**.
   - In **Region**, select **Default**.

d) Select the CSS to be used for autoregistration in the **Calling Search Space for Auto-registration** field, then click **Save**.

What to do next

Set the Device Protocol Type for Autoregistration, on page 553

Set the Device Protocol Type for Autoregistration

If you have SIP and SCCP devices to auto-register, you must first set the Auto Registration Phone Protocol parameter to SCCP and install all the devices that are running SCCP. Then change the Auto Registration Phone Protocol parameter to SIP and auto-register all the devices that are running SIP.

Before you begin

Configure a Device Pool for Autoregistration, on page 552

Procedure

Step 1 In Cisco Unified Communications Manager Administration, select **System** > **Enterprise Parameters**.

Step 2 In the **Enterprise Parameters Configuration** window, select either **SCCP** or **SIP** in the **Auto Registration Phone Protocol** drop-down list, then click **Save**.

What to do next

Enable Autoregistration, on page 553

Enable Autoregistration

When you enable autoregistration, you must specify a range of directory numbers that get assigned to the new endpoints as they connect to the network. As each new endpoint connects, the next available directory number is assigned. After all the available autoregistration directory numbers are used up, no more endpoints can auto-register.

New endpoints auto-register with the first Unified Communications Manager node in the group that has the **Auto-Registration Cisco Unified Communications Manager Group** setting enabled. That node then automatically assigns each auto-registered endpoint to a default device pool according to the device type.

Before you begin

Set the Device Protocol Type for Autoregistration, on page 553

- Create a device pool, calling search space, and route partition that restricts the access of devices that are auto-registering to allow only internal calls.
- Ensure that directory numbers are available in the autoregistration range.
- Ensure that there are enough license points available to register the new phones.

- Check that the correct phone image names for SIP and SCCP appear on the **Device Defaults Configuration** window. Although most of the common device configuration files should be available on the TFTP server, make sure that the configuration files for your devices are there.
- Ensure that the Cisco TFTP server is up and running and that the DHCP option for TFTP specifies the correct server.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, select **System** > **Cisco Unified CM**, then click **Find** in the **Find and List Cisco Unified Communications Managers** window.

Step 2 Select the Cisco Unified Communications Manager in the cluster to use for autoregistration.

appears.

Step 3 In the **Cisco Unified CM Configuration** widow, configure the autoregistration parameters for the node in the **Auto-registration Information** section, then click **Save**. For more information on the fields and their configuration options, see the system Online Help.

a) Select the universal device template to use for autoregistration from the drop-down list.

If no universal device template is created for autoregistration, you can select **Default Universal Device Template**. Make sure that the selected template specifies the device pool that is to be used for autoregistration from **User Management** > **User/Phone Add** > **Universal Device Template**.

b) Select the universal line template to use for autoregistration from the drop-down list.

If no universal line template is created for autoregistration, you can select **Default Universal Line Template**. Make sure that the selected template specifies the calling search space and the route partition that are to be used for autoregistration from **User Management** > **User/Phone Add** > **Universal Line Template**.

c) Enter the starting and ending directory numbers in to the **Starting Directory Number** and **Ending Directory Number** fields.

Setting the starting and ending directory numbers to the same value disables autoregistration.

d) Uncheck **Auto-registration Disabled on this Cisco Unified Communications Manager** to enable autoregistration for this node.

Always enable or disable autoregistration on only the selected Unified Communications Manager node. If you switch the autoregistration function to another node in the cluster, you must reconfigure the Unified Communications Manager nodes, the Default Unified Communications Manager group, and the default device pools that you used.

Step 4 Select **System** > **Cisco Unified CM Group**, then click **Find** in the **Find and List Cisco Unified Communications Manager Groups** window.

Step 5 Select the Unified Communications Manager group to enable for autoregistration.

In most cases, the name of this group is **Default**. You can choose a different Cisco Unified Communications Manager group. The group must have at least one node selected.

Step 6 In the **Cisco Unified CM Group Configuration** window for that group, select **Auto-registration Cisco Unified Communications Manager Group** to enable autoregistration for the group, then click **Save**.

Tip Ensure that the **Selected Cisco Unified Communications Managers** list contains the node that you configured for autoregistration. Use the arrows to move the node to appear in the list. The Unified Communications Manager nodes get selected in the order in which they are listed. **Save** your changes.

Step 7 Install the devices that you want to auto-register.

Note You can proceed to reconfigure the auto-registered phones and assign them to their permanent device pools. The directory number that is assigned to the phone does not change when you change the phone location.

Note To register phones of a different type, change the device protocol type and install those devices before disabling autoregistration.

Disable Autoregistration

Disable autoregistration for the node as soon as you are finished registering new devices.

Before you begin

Enable Autoregistration, on page 553

Procedure

Step 1 In Cisco Unified Communications Manager Administration, select **System** > **Cisco Unified CM**, then click **Find** in the **Find and List Cisco Unified CM** window.

Step 2 Select the **Cisco Unified Communications Manager** from the list of nodes.

Step 3 In the **Cisco Unified CM Configuration** widow for the selected node, check the **Auto-registration Disabled on this Cisco Unified Communications Manager** check box to disable autoregistration for this node, then click **Save**.

Tip Setting the same value in the **Starting Directory Number** and **Ending Directory Number** fields also disables autoregistration.

What to do next

Optional. If you manually changed the directory number of an auto-registered device, or if you delete that device from the database, you can reuse the directory number. For details, see Reuse Autoregistration Numbers, on page 556.

Reuse Autoregistration Numbers

When you connect a new device to the network, the system assigns the next available autoregistration directory number to that device. If you manually change the directory number of an auto-registered device, or if you delete that device from the database, the autoregistration directory number of that device can be reused.

When a device attempts to auto-register, the system 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, the system continues to search from the starting directory number in the range.

You can reset the range of autoregistration directory numbers and force the system to search from the starting number in the range.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, select **System** > **Cisco Unified Communications Manager**

Step 2 Select the Cisco Unified Communications Manager to reset for autoregistration.

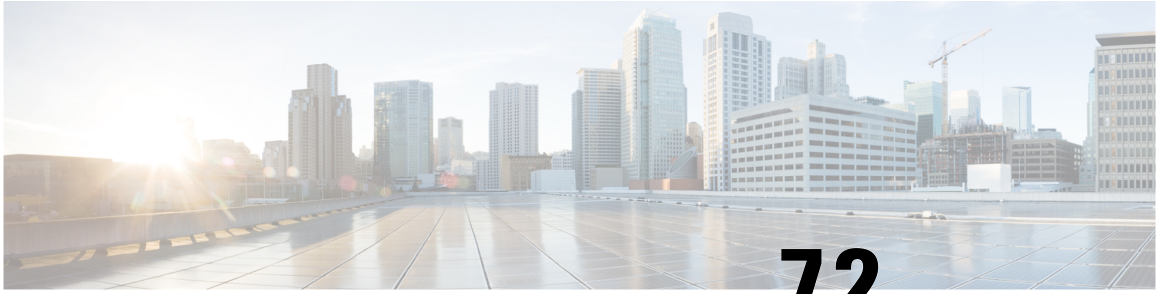
Step 3 Write down the current settings in the **Starting Directory Number** and **Ending Directory Number** fields.

Step 4 Click **Auto-registration Disabled on this Cisco Unified Communications Manager**, then click **Save**.

New phones cannot auto-register while autoregistration is disabled.

Step 5 Set the **Starting Directory Number** and **Ending Directory Number** fields to their previous values, then click **Save**.

Tip You could set the fields to new values.



CHAPTER 72

Manual Phone Registration

Manual Phone Registration Overview

To manually register a new Cisco IP Phone, you must add the phone to the Unified Communications Manager node using Unified Communications Manager, then configure the directory number for the phone.

You should have already set up the new phone with the proxy TFTP server IP address so that the new phone knows how to locate the Unified Communications Manager node. See the *Cisco IP Phone Administration Guide* for your phone series.

Manual Device Registration Task Flow

Procedure

	Command or Action	Purpose
Step 1	See the *Cisco IP Phone Administration Guide* for your phone series	Set up the new phone with the proxy TFTP server IP address so that the new phone knows how to locate the Unified Communications Manager node.
Step 2	Add a Phone to the System Manually, on page 557	Add the phone to the Unified Communications Manager node.
Step 3	Configure a Directory Number Manually for a Phone, on page 558	Add a directory number for the phone and configure some basic settings for the directory number.

Add a Phone to the System Manually

Manually add a new phone to the Cisco Unified Communications Manager node.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, select **Device** > **Phone**, then click **Add New**.

Step 2 In the **Add a New Phone** window, select your phone model in the **Phone Type** field, then click **Next**.

Step 3 In the **Phone Configuration** window, select the protocol type for your device in the **Select the device protocol** field, then click **Next**.

Step 4 In the **Device Information** area, perform the following actions.

a) Enter a name in the **Device Name** field.

   The name entered here must match the Device Name that is configured on your phone. See the documentation that supports your endpoint device for more information.

b) Select a device pool for the phone from the list of device pools.

c) Select the phone button template to use from the list of phone button templates.

Step 5 In the **Protocol Specific Information** area, select the non-secure profile for your type of phone in the **Device Security Profile** field.

Step 6 Click **Save**.

What to do next

Configure a Directory Number Manually for a Phone, on page 558

Configure a Directory Number Manually for a Phone

There are multiple ways to manually add and configure a directory number (DN) using Cisco Unified Communications Manager Administration.

- From the **Directory Number Configuration** window using **Call Routing** > **Directory Number**.
- From the **Phone Configuration** window using **Device** > **Phone** when you select either **Line [1] - Add a new DN** or **Line [2] - Add a new DN link** in the **Association Information** area.
- From the **Phone Configuration** window using **Call Routing** > **Phone** after you add the phone under call routing.
- From the **CTI Route Point Configuration** window when you configure a CTI route point using **Device** > **CTI Route Point**.

This procedure assumes that you are configuring a DN for a new phone using the **Phone Configuration** window that appeared after you added the new phone to the Unified Communications Manager node.

Only the settings that apply to your phone model display using this method.

Tip You can configure phone features at the same time that you add the new DN for the phone. To see all available DN settings, you must access the **Directory Number Configuration** window from call routing in the user interface.

Before you begin

The phone is added to the node. The **Phone Configuration** window should still be visible for the new phone that you are registering.

If your system uses partitions, collect the route partition and calling search space information to use for the new phone.

Procedure

Step 1 Click **Line [1] - Add a new DN** in the **Association** area of the **Phone Configuration** window.

Tip If the **Phone Configuration** window is not already visible, select **Device** > **Phone**, then click **Find** and select the phone from the list of phones.

Step 2 In the **Directory Number Configuration** window, enter a dialable phone number in the **Directory Number** field.

Step 3 (Optional) Select a partition in the **Route Partition** field.

Step 4 (Optional) Select a calling search space in the **Calling Search Space** field in the **Directory Number Settings** area.

Step 5 (Optional) Configure other directory number features as applicable for the new phone, then click **Save**.

For example, if you already know the user name for the new phone, you can enter that in the **Display (Caller ID)** field. See the online help for field descriptions.

CHAPTER 73

Configure Self-Provisioning

Self-Provisioning Overview

The Self-Provisioning feature helps you provision phones for your network by giving end users the ability to provision their own phones without contacting an administrator. If the system is configured for self-provisioning, and an individual end user is enabled for self-provisioning, then end user can provision a new phone by plugging the phone into the network and follow the specified few prompts. Cisco Unified Communications Manager configures the phone and the phone line by applying pre-configured templates.

Self-provisioning can be used either by administrators to provision phones on behalf of their end users, or end users can use self-provisioning to provision their own phones.

Self-provisioning is supported whether the cluster security setting is nonsecure or mixed mode.

Security Modes

You can configure self-provisioning in one of two modes:

- Secure mode—In secure mode, users or administrators must be authenticated in order to access self-provisioning. End users can be authenticated against their password or PIN. Administrators can enter a pre-configured authentication code.
- Non-secure mode—In non-secure mode, users or administrators can enter their user ID, or a self-provisioning ID, in order to associate the phone to a user account. Non-secure mode is not recommended for day-to-day use.

Configuration through Universal Line and Device Templates

Self-provisioning uses the universal line template and universal device template configurations to configure provisioned phones and phone lines for an end user. When a user provisions their own phone, the system references the user profile for that user and applies the associated universal line template to the provisioned phone line and the universal device template to the provisioned phone.

Self-Provisioning Phones

When the feature is configured, you can provision a phone by doing the following:

- Plug the phone into the network.
- Dial the self-provisioning IVR extension.
- Follow the prompts to configure the phone, and associate the phone to an end user. Depending on how you have configured self-provisioning, the end user may to enter the user password, PIN, or an administrative authentication code.

Tip If you are provisioning a large number of phones on behalf of your end users, configure a speed dial on the universal device template that forwards to the self-provisioning IVR extension.

Self-Provisioning Prerequisites

Before your end users can use self-provisioning, your end users be configured with the following items:

- Your end users must have a primary extension.
- Your end users must be associated to a user profile or feature group template that includes a universal line template, universal device template. The user profile must be enabled for self-provisioning.

Self-Provisioning Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Activate Services for Self-Provisioning, on page 563	In Cisco Unified Serviceability, activate the **Self-Provisioning IVR** and **CTI Manager** services.
Step 2	Enable Autoregistration for Self-Provisioning, on page 563	Enable autoregistration parameter for self-provisioning
Step 3	Configure CTI Route Point, on page 563	Configure a CTI route point to handle the self-provisioning IVR service.
Step 4	Assign a Directory Number to the CTI Route Point, on page 564	Configure the extension that users will dial in order to access the self-provisioning IVR and associate that extension to the CTI route point.
Step 5	Configure Application User for Self-Provisioning, on page 564	Configure an application user for the self-provisioning IVR. Associate the CTI route point to the application user.

	Command or Action	Purpose
Step 6	Configure the System for Self-Provisioning, on page 565	Configure self-provisioning settings for your system, including associating the application user and CTI route point to the self-provisioning IVR.

Activate Services for Self-Provisioning

Use this procedure to activate the services that support the Self-Provisioning feature. Ensure that both the Self-Provisioning IVR and Cisco CTI Manager services are running.

Procedure

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

Step 2 From the **Server** drop-down list, select the publisher node and click **Go**.

Step 3 Under **CM Services**, check **Cisco CTI Manager**.

Step 4 Under **CTI Services**, check **Self Provisioning IVR**.

Step 5 Click **Save**.

Enable Autoregistration for Self-Provisioning

Use this procedure for self-provisioning, you must configure the auto-registration parameters on the publisher.

Procedure

Step 1 In Cisco Unified CM Administration, choose **System** > **Cisco Unified CM**.

Step 2 Click on the publisher node.

Step 3 Select the **Universal Device Template** that you want to be applied to provisioned phones.

Step 4 Select the **Universal Line Template** that you want to be applied to the phone lines for provisioned phones.

Step 5 Use the **Starting Directory Number** and **Ending Directory Number** fields to enter a range of directory numbers to apply to provisioned phones.

Step 6 Uncheck the **Auto-registration Disabled on the Cisco Unified Communications Manager** check box.

Step 7 Confirm the ports that will be used for SIP registrations. In most cases, there is no need to change the ports from their default settings.

Step 8 Click **Save**.

Configure CTI Route Point

Us this procedure to configure a CTI Route Point for the Self-Provisioning IVR.

Procedure

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

Step 2 Complete either of the following steps:

a) Click **Find** and select an existing CTI route point.
b) Click **Add New** to create a new CTI route point.

Step 3 In the **Device Name** field, enter a unique name to identify the route point.

Step 4 From the **Device Pool** drop-down list, select the device pool that specifies the properties for this device.

Step 5 From the **Location** drop-down list, select the appropriate location for this CTI route point.

Step 6 From the **Use Trusted Relay Point** drop-down list, enable or disable whether Unified Communications Manager inserts a trusted relay point (TRP) device with this media endpoint. The default setting is to use the Common Device Configuration setting that is associated to this device.

Step 7 Complete the remaining fields in the **CTI Route Point Configuration** window. For more information on the fields and their settings, see the online help.

Step 8 Click **Save**.

Assign a Directory Number to the CTI Route Point

Use this procedure to set up the extension that users will dial in to access the self-provisioning IVR. You must associate this extension to the CTI route point that you want to use for self-provisioning.

Procedure

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

Step 2 Click **Find** and select the CTI route point that you set up for self-provisioning.

Step 3 Under **Association** click **Line [1] - Add a new DN**.
The **Directory Number Configuration** window displays.

Step 4 In the **Directory Number** field, enter the extension that you want users to dial to access the Self-Provisioning IVR service.

Step 5 Click **Save**.

Step 6 Complete the remaining fields in the **Directory Number Configuration** window. For more information with the fields and their settings, see the online help.

Step 7 Click **Save**.

Configure Application User for Self-Provisioning

You must set up an application user for the self-provisioning IVR and associate the CTI route point that you created to the application user.

Procedure

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

Step 2 Perform either of the following steps:

a) To select an existing application user, click **Find** and select the application user.
b) To create a new application user, click **Add New**.

Step 3 In the **User ID** text box, enter a unique ID for the application user.

Step 4 Select a **BLF Presence Group** for the application user.

Step 5 Associate the CTI route point that you created to the application user by performing the following steps:

a) If the CTI route point that you created does not appear in the **Available Devices** list box, click **Find More Route Points**.
The CTI route point that you created displays as an available device.
b) In the **Available Devices** list, select the CTI route point that you created for self-provisioning and click the down arrow.
The CTI route point displays in the **Controlled Devices** list.

Step 6 Complete the remaining fields in the **Application User Configuration** window. For help with the fields and their settings, see the online help.

Step 7 Click **Save**.

Configure the System for Self-Provisioning

Use this procedure to configure your system for self-provisioning. Self-provisioning provides users in your network with the ability to add their own desk phone through an IVR system, without contacting an administrator.

Note In order to use the self-provisioning feature, your end users must also have the feature enabled in their user profiles.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **Self-Provisioning**.

Step 2 Configure whether you want the self-provisioning IVR to authenticate end users by clicking one of the following radio buttons:

- **Require Authentication**—In order to use the self-provisioning IVR, end users must enter their password, PIN, or a system authentication code.
- **No Authentication Required**—End users can access the self-provisioning IVR without authenticating.

Step 3 If the self-provisioning IVR is configured to require authentication, click one of the following radio buttons to configure the method whereby the IVR authenticates end users:

- **Allow authentication for end users only**—End users must enter their password or PIN.

- **Allow authentication for users (via Password/PIN) and Administrators (via Authentication Code)**—End Users must enter an authentication code. If you choose this option, configure the authentication code by entering an integer between 0 and 20 digits in the **Authentication Code** text box.

Step 4 In the **IVR Settings** list boxes, use the arrows to select the Language that you prefer to use for IVR prompts. The list of available languages depends on the language packs that you have installed on your system. Refer to the Downloads section of cisco.com if you want to download additional language packs.

Step 5 From the **CTI Route Points** drop-down list, choose the CTI route point that you have configured for your self-provisioning IVR.

Step 6 From the **Application User** drop-down list, choose the application user that you have configured for self-provisioning.

Step 7 Click **Save**.

Enable Self-Provisioning in a User Profile

In order for users to be able to Self-Provision phones, the feature must be enabled in the user profile to which they are assigned.

Note If you don’t know which user profile your users are using, you can open a user’s settings in the End User Configuration window and view the **User Profile** field to get the correct profile.

Procedure

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

Step 2 Click **Find and select the user profile** to which the user is assigned.

Step 3 Assign **Universal Line Templates** and **Universal Device Templates** to the user profile.

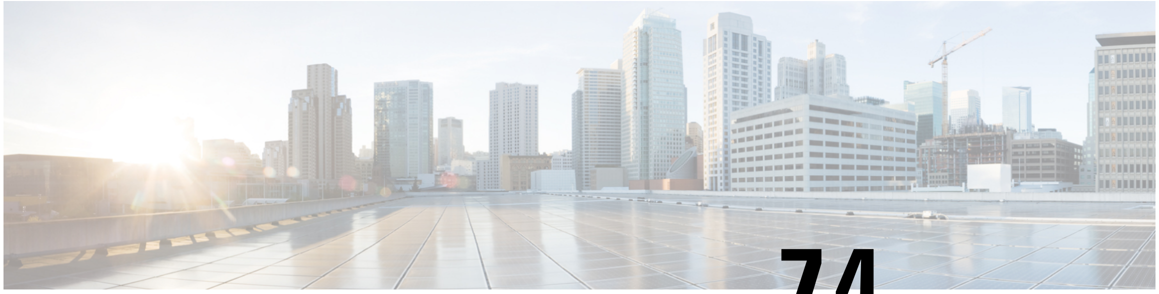
Step 4 Configure user settings for Self-Provisioning:

- Check the **Allow End User to Provision their own phones** check box.
- Enter a limit for the number of phones a user can provision. The default is 10.

Step 5 Click **Save**.

PART X

Configure Advanced Call Handling



CHAPTER 74

Advanced Call Handling Overview

About Advanced Call Handling

The chapters in this part describe different ways to configure advanced call handling in your system. With the functions outlined in this part, you can configure how your system handles a call at any point in the call flow at a more granular level than basic call handling features such as call forwarding. The task flow in this part lists each call handling function, describes the purpose for configuring it, and links to the applicable chapter that provides further details.

Advanced Call Handling Configuration

Complete the following task flows to configure advanced call handling for your system.

Procedure

	Command or Action	Purpose
Step 1	APIC-EM Controller Configuration Task Flow, on page 574	In order to manage network quality of service (QoS) for SIP calls, deploy a Cisco Application Policy Infrastructure controller Enterprise module (APIC-EM). APIC-EM applies DSCP markings to media flows created by communication sessions among Cisco Unified Communications Manager-managed SIP endpoints and trunks. Applying DSCP markings to media flows ensures that audio and video media will not be blocked by other lower priority network traffic such as email, print jobs, and software downloads.
Step 2	Call Control Discovery Configuration Task Flow, on page 579	Configure call control discovery to advertise the Cisco Unified Communications Manager to other call control entities that use the Service

	Command or Action	Purpose
		Advertisement Framework (SAF) network. These call control entities can use the advertised information to dynamically configure their routing operations for the call.
Step 3	External Call Control Configuration Task Flow, on page 590	Configure external call control to have an adjunct route server make call-routing decisions for your system. Unified Communications Manager issues a route request to an adjunct route server, which provides instructions about how to route the call, along with any additional call treatment to apply.
Step 4	Call Queuing Task Flow, on page 600	Configure call queueing to place callers in a queue until hunt members are available to answer them.
Step 5	Call Throttling Configuration, on page 612	Configure call throttling to automatically throttle or deny new call attempts when system conditions can cause users to experience a delay in the interval between going off hook and receiving a dial tone. We recommend that you not modify call throttling parameters unless advised to do so by Cisco customer support.
Step 6	Calling Party Normalization Configuration Task Flow, on page 616	Configure calling party normalization to reformat incoming phone numbers so that they display on the recipient's phone as globalized or localized phone numbers. Use this feature to improve callback functionality when a call is routed to multiple geographic locations, and to map a global calling party number to its localized variant so that a phone can return a call without modifying the directory number in the call log directories on the phone.
Step 7	Logical Partitioning Configuration Task Flow, on page 631	Configure logical partitioning to satisfy regulatory requirements in markets where toll bypass is forbidden. For example, you can configur ea policy prevent users from initiating restricted calls by using midcall features such as conference join and redirect.
Step 8	Geolocation and Location Conveyance Task Flow, on page 641	Specify a geolocation for every device and communicate geolocation information across clusters. Geolocations assign a civic address to devices so that communication between devices can be controlled based on legal requirements in certain countries.

	Command or Action	Purpose
Step 9	Location Awareness Configuration Task Flow, on page 649	Location Awareness allows administrators to determine the physical location from which a phone connects to the company network.
Step 10	AAR Configuration Task Flow, on page 655	Configure your system to automatically reroute calls through the PSTN or other networks when your system 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.
Step 11	Multilevel Precendence and Preemption Task Flow, on page 669	Configure Multilevel Precedence and Preemption (MLPP) if you want to allow validated users to place priority calls. If necessary, these users can preempt lower priority phone calls.
Step 12	Two Stacks (IPv4 and IPv6) Configuration Task Flow, on page 690	If you want your endpoints to be able to support both IPv4 and IPv6 addressing, complete these tasks to configure two stack support for endpoints.

CHAPTER 75

Configure QoS with APIC-EM Controller

APIC-EM Controller Overview

The APIC-EM Controller provides a centralized system for managing network traffic so that you always have the bandwidth to maintain communications, even in congested networks. You can configure Cisco Unified Communications Manager to use the APIC-EM Controller to manage SIP media flows thereby providing the following benefits:

- Centralizes QoS management, thereby eliminating the need for endpoints to assign DSCP values.
- Applies differential QoS treatment for different media flows. For example, you can prioritize audio over video to ensure that basic audio communication is always maintained, even when network bandwidth is low.
- External QoS setting in the SIP Profile allows you to target which users will use the APIC-EM. For example, you may have Cisco Jabber users use the APIC-EM to manage media flows, while Cisco Unified IP Phone users use the DSCP settings in Cisco Unified Communications Manager.

SIP Media Flow Management

For SIP calls that use APIC-EM, Cisco Unified Communications Manger sends the policy request to the APIC-EM Controller at the call outset notifying the APIC-EM of the media flow that is being set up. The policy request contains information about the call, including the IP address and ports for source and destination devices, the media type for the flow and the protocol.

The APIC-EM notifies the switch at the beginning of the call flow of the DSCP values for the associated media flows. The switch inserts those DSCP values into individual media packets, overwriting any values that the endpoint inserts. If a gateway in the call flow experiences congestion, that gateway sends through the packets with the higher DSCP values first. This ensures that high priority audio and video streams are not blocked by lower-priority network traffic such as email, print jobs, or software downloads. When the call ends, Cisco Unified Communications Manager notifies the APIC-EM and the APIC-EM notifies the switch to delete the flow.

External QoS Support

In order for Cisco Unified Communications Manager to use the APIC-EM to manage media flows, the External QoS parameter must be enabled at both the system level, via a clusterwide service parameter, and at the device level, via the SIP Profile.

APIC-EM Controller Prerequisites

Before using APIC-EM, you must do the following:

- Configure DSCP priority for different SIP media flows in Cisco Unified Communications Manager. For details, see DSCP Settings Configuration Task Flow, on page 515.
- Configure the APIC-EM controller hardware within your network. For details, see the hardware documentation that comes with the APIC-EM controller.

APIC-EM Controller Configuration Task Flow

Complete these tasks on Cisco Unified Communications Manager to enable APIC-EM Controller to manage SIP media flows.

Before you begin

- Review APIC-EM Controller Prerequisites, on page 574.

Procedure

	Command or Action	Purpose
Step 1	Upload APIC-EM Controller Certificate, on page 575	Upload the APIC-EM certificate into Cisco Unified OS Administration.
Step 2	Configure HTTPS Connection to APIC-EM Controller, on page 576	Configure an HTTP Profile that points to the APIC-EM service.
Step 3	Enable External QoS Service for System, on page 576	Enable the **External QoS Enable** service parameter to configure the system to use the APIC-EM to manage media flows. The service parameter must be enabled for devices to use the APIC-EM for SIP media flow management. **Note** You must also enable external QoS within the SIP Profile for devices that will use the APIC-EM for SIP media flow management.
Step 4	Configure External QoS Service at SIP Profile Level, on page 577	Enable external QoS within a SIP Profile. All devices that use this SIP Profile will be able to use the APIC-EM to manage SIP media flows

	Command or Action	Purpose
		You can use the SIP Profile setting to configure which devices and device types you want the APIC-EM to manage media flows.
Step 5	Assign SIP Profile to Phones, on page 578	Associate the external QoS-enabled SIP Profile to a phone.

Configure the APIC-EM Controller

Use this procedure on the APIC-EM Controller to add Cisco Unified Communications Manager as a user. APIC-EM's role-based access control feature provides Cisco Unified Communications Manager with access to APIC-EM resources.

Procedure

Step 1 On the APIC-EM Controller, choose **Settings** > **Internal Users**.

Step 2 Create a new user with the following role: **ROLE_POLICY_ADMIN**. Keep track of the username and password that you enter because you must enter identical credentials in Cisco Unified Communications Manager's **HTTP Profile** window.

Step 3 Go to the **Discovery** tab and add a discovery with CDP or the IP address range of the available devices.

Step 4 Select the **Device Inventory** tab and select the reachable devices.

Step 5 Click on **Set Policy Tag**.

Step 6 Create a policy tag and set it for the devices.

Step 7 On the **EasyQoS** tab, select the policy that you created and enable **DynamicQoS**.

What to do next

Upload APIC-EM Controller Certificate, on page 575

Upload APIC-EM Controller Certificate

Use this procedure to upload the APIC-EM controller certificate into Cisco Unified Communications Manager.

Procedure

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

Step 2 Click **Upload Certificate/Certificate Chain**.
The **Upload Certificate/Certificate Chain** popup window appears.

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

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

Step 5 Click **Browse** to search for, and select, the certificate.

Step 6 Click **Upload**.

What to do next

Configure HTTPS Connection to APIC-EM Controller, on page 576

Configure HTTPS Connection to APIC-EM Controller

Use this procedure to set up an HTTP Profile to connect Cisco Unified Communications Manager to the APIC-EM Controller. In this connection, Cisco Unified Communications Manager acts as an HTTP user and the APIC-EM acts as the HTTP server.

Before you begin

Upload APIC-EM Controller Certificate, on page 575

Procedure

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

Step 2 Enter a **Name** for the service.

Step 3 Enter the **User Name** and **Password** for this HTTP connection. The user name does not have to be a configured end user in Cisco Unified Communications Manager, but the user name and password must match the values that are configured in the APIC-EM Controller.

Step 4 In the **Web Service Root URI** text box, enter the IP address or fully qualified domain name of the APIC-EM service.

Step 5 Configure any remaining fields in the HTTP Profile window. For help with the fields and their options, refer to the online help.

Step 6 Click **Save**.

What to do next

Enable External QoS Service for System, on page 576

Enable External QoS Service for System

Use this procedure to configure Cisco Unified Communications Manager to use an external service for QoS management. You must enable this service parameter in order to use an APIC-EM controller for QoS.

Before you begin

Configure HTTPS Connection to APIC-EM Controller, on page 576

Procedure

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

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

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

Step 4 Set the value of the **External QoS Enabled** service parameter to **True**.

Step 5 Click **Save**.

Note To use the APIC-EM to manage call flows for devices, you must also enable external QoS within the SIP Profile for the device.

What to do next

Configure External QoS Service at SIP Profile Level, on page 577

Configure External QoS Service at SIP Profile Level

If you have enabled the **External QoS Enabled** clusterwide service parameter, use this procedure to enable external QoS for SIP devices that use this SIP Profile.

Note External QoS must be enabled at both the system level and in the SIP Profile to use the APIC-EM to manage QoS.

Before you begin

Enable External QoS Service for System, on page 576

Procedure

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

Step 2 Do one of the following:

- Click **Find** and select an existing SIP Profile.
- Click **Add New** to create a new SIP Profile.

Step 3 Check the **Enable External QoS** check box. This check box must be checked for phones that use this SIP Profile to use the APIC-EM Controller to manage QoS.

Step 4 Complete the remaining fields in the **SIP Profile Configuration** window. For help with the fields and their settings, see the online help.

Step 5 Click **Save**.

What to do next

Assign SIP Profile to Phones, on page 578

Assign SIP Profile to Phones

Use this procedure if you want to assign the external QoS-enabled SIP Profile that you created to a phone.

Tip Use the Bulk Administration Tool to update the SIP Profile for a large selection of phones in a single operation. For details, see the *Bulk Administration Guide for Cisco Unified Communications Manager.*

Before you begin

Assign SIP Profile to Phones, on page 578

Procedure

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

Step 2 Click **Find** and select an existing phone.

Step 3 From the **SIP Profile** drop-down list box, select the SIP Profile that you updated for phones that will use the APIC-EM Controller to manage traffic.

Step 4 Complete any remaining fields in the **Phone Configuration** window. For help with the fields and their settings, see the online help.

Step 5 Click **Save**.

CHAPTER 76

Configure Call Control Discovery

Call Control Discovery Overview

Use Call Control Discovery (CCD) to advertise Unified Communications Manager information along with other key attributes, such as directory number patterns. Other call control entities that use the Service Advertisement Framework (SAF) network can use the advertised information to dynamically configure and adapt their routing operations. All entities that use SAF advertise their directory number patterns along with other key information. Other remote call control entities can learn the information from this broadcast and adapt the routing operations of the call.

Call Control Discovery Prerequisites

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

Call Control Discovery Configuration Task Flow

Before you begin

- Review Call Control Discovery Prerequisites, on page 579.

Procedure

	Command or Action	Purpose
Step 1	See the documentation that supports your Cisco IOS router. Cisco Feature Navigator (http://www.cisco.com/go/cfn) allows you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform.	Configure a Cisco IOS router as the SAF forwarder.
Step 2	Configure SAF Security Profile, on page 581	Configure the SAF security profile for the SAF forwarder to provide a secure connection between the SAF forwarder and Unified Communications Manager.
Step 3	Configure SAF Forwarders, on page 582	Configure the SAF forwarders, which are Cisco IOS routers configured for SAF. They notify the local cluster when remote call-control entities advertise their hosted DNs patterns. In addition, the SAF forwarder receives publishing requests from the local cluster for each configured and registered trunk that is configured; the publishing request contains the Hosted DN patterns for the Cisco Unified Communications Manager, the PSTN failover configuration, the listening port for the trunk, and, for SIP trunks, the SIP route header field, which contains a URI for the trunk.
Step 4	Configure SIP or H.323 Intercluster Trunks, on page 582	Configure SIP or H.323 intercluster (non-gatekeeper controlled) trunks for SAF support. The local cluster uses SAF-enabled trunks that are assigned to the CCD requesting service to route outbound calls to remote call-control entities that use the SAF network.
Step 5	Configure Hosted DN Groups, on page 583	Configure hosted DN groups, which are collections of hosted DN patterns. After you assign a hosted DN group to the CCD advertising service, the CCD advertising service advertises all the hosted DN patterns that are a part of the hosted DN group. You can assign only one hosted DN group per CCD advertising service.
Step 6	Configure Hosted DN Patterns, on page 583	Configure hosted DN patterns, which are directory number patterns that belong to Unified Communications Manager; the CCD advertising service advertises these patterns to other remote call-control entities that use the SAF network. You associate these patterns

	Command or Action	Purpose
		with hosted DN groups, which allow you to easily associate multiple patterns to a CCD advertising service.
Step 7	Configure the Advertising Service, on page 584	Configure the call control discovery advertising service, which allows Unified Communications Manager to advertise the hosted DNs for the cluster and the PSTN failover configuration to remote call-control entities that use the SAF network.
Step 8	Configure the Partition for Call Control Discovery, on page 584	Configure a call control discovery partition to ensure that the learned patterns are inserted into digit analysis under this partition.
Step 9	Configure the Requesting Service, on page 584	To ensure that your local cluster can detect advertisements from the SAF network, configure one call control discovery requesting service to listen for advertisements from remote call control entities that use the SAF network. In addition, the CCD requesting service ensures that learned patterns are inserted into the digit analysis.
Step 10	Block Learned Patterns, on page 585	Block learned patterns that remote call control entities send to the local Unified Communications Manager. Perform this procedure on learned patterns that you no longer want to use.

Configure SAF Security Profile

Configure the SAF security profile for the SAF forwarder to provide a secure connection between the SAF forwarder and Unified Communications Manager.

Tip Use the same username and password that you entered on the router (SAF forwarder).

Before you begin

Configure a Cisco IOS router as the SAF forwarder. (See the Cisco Feature Navigator at http://www.cisco.com/go/cfn.)

Procedure

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

Step 2 Configure the fields on the **SAF Security Profile Configuration** window. For more information on the fields and their configuration options, see the system Online Help.

Step 3 Click **Save**.

Configure SAF Forwarders

Configure the SAF forwarders, which are Cisco IOS routers configured for SAF. They notify the local cluster when remote call-control entities advertise their hosted DNs patterns. In addition, the SAF forwarder receives publishing requests from the local cluster for each configured and registered trunk that is configured; the publishing request contains the Hosted DN patterns for the Cisco Unified Communications Manager, the PSTN failover configuration, the listening port for the trunk, and, for SIP trunks, the SIP route header field, which contains a URI for the trunk.

Tip If more than one node appears in the **Selected Cisco Unified Communications Managers** pane, append @ to the client label value; otherwise, errors can occur if each node uses the same client label to register with the SAF forwarder.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Advanced Features** > **SAF** > **SAF Forwarder**.

Step 2 Configure the fields on the **SAF Forwarder Configuration** window. See the online help for more information about the fields and their configuration options.

Step 3 Click **Save**.

Configure SIP or H.323 Intercluster Trunks

Configure SIP or H.323 intercluster (non-gatekeeper controlled) trunks for SAF support. The local cluster uses SAF-enabled trunks that are assigned to the CCD requesting service to route outbound calls to remote call-control entities that use the SAF network.

Procedure

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

Step 2 Click **Add New**.

Step 3 Perform one of the following tasks:

- For SIP trunks:

  a. From the **Trunk Service Type** Type drop-down list, choose **Call Control Discovery**. You cannot change the trunk service type after you select it from the drop-down list.

  b. Click **Next**.

c. Configure the fields on the **Trunk Configuration** window. See the online help for more information about the fields and their configuration options.

- For intercluster (non-gatekeeper controlled) trunks:

  a. Click **Next**.

  b. Check the **Enable SAF** check box.

  c. Configure the other fields on the **Trunk Configuration** window. See the online help for more information about the fields and their configuration options.

Step 4 Click **Save**.

Configure Hosted DN Groups

Configure hosted DN groups, which are collections of hosted DN patterns. After you assign a hosted DN group to the CCD advertising service, the CCD advertising service advertises all the hosted DN patterns that are a part of the hosted DN group. You can assign only one hosted DN group per CCD advertising service.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Call Control Discovery** > **Hosted DN Group**.

Step 2 Configure the fields on the Hosted DN Groups Configuration window. See the online help for more information about the fields and their configuration options.

Step 3 Click **Save**.

Configure Hosted DN Patterns

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

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Call Control Discovery** > **Hosted DN Patterns**.

Step 2 Configure the fields on the **Hosted DN Patterns Configuration** window. For more information on the fields and their configuration options, see the system Online Help.

Step 3 Click **Save**.

Configure the Advertising Service

Configure the call control discovery advertising service, which allows Unified Communications Manager to advertise the hosted DNs for the cluster and the PSTN failover configuration to remote call-control entities that use the SAF network.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Call Control Discovery** > **Advertising Service**.

Step 2 Configure the fields in the **Advertising Service Configuration** window. For more information on the fields and their configuration options, see the system Online Help.

Step 3 Click **Save**.

Configure the Partition for Call Control Discovery

Configure a call control discovery partition to ensure that the learned patterns are inserted into digit analysis under this partition.

Note The CCD partition does not appear under **Call Routing** > **Class of Control** > **Partition** in Cisco Unified Communications Manager Administration.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Call Control Discovery** > **Partition**.

Step 2 Configure the fields in the **Call Control Discovery Partition Configuration** window. For more information on the fields and their configuration options, see the system Online Help.

Step 3 Click **Save**.

Configure the Requesting Service

Caution Updating the **Learned Pattern Prefix** or **Route Partition** fields can affect system performance. To avoid system performance issues, we recommend that you update these fields during off-peak hours.

To ensure that your local cluster can detect advertisements from the SAF network, configure one call control discovery requesting service to listen for advertisements from remote call control entities that use the SAF network. In addition, the CCD requesting service ensures that learned patterns are inserted into the digit analysis.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Call Control Discovery** > **Requesting Service**.

Step 2 Configure the fields in the **Requesting Service Configuration** window. For more information on the fields and their configuration options, see the system Online Help.

Step 3 Click **Save**.

Configure your remote call control entity to use the SAF network. (See the documentation for your remote call control entity.)

Block Learned Patterns

Block learned patterns that remote call control entities send to the local Unified Communications Manager. Perform this procedure on learned patterns that you no longer want to use.

Before you begin

Configure your remote call control entity to use the SAF network. See the documentation that supports your remote call control entity.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Call Control Discovery** > **Block Learned Patterns**.

Step 2 Click **Add New**.

Step 3 Configure one of the following fields:

- In the **Learned Pattern** field, enter the exact learned pattern that you want to block. You must enter the exact pattern that you want Cisco Unified Communications Manager to block.
- In the **Learned Pattern Prefix** field, enter the prefix to block a learned pattern based on the prefix that is prepended to the pattern.

Example:

For **Learned Pattern**, enter 235XX to block 235XX patterns.

Example:

For **Learned Pattern Prefix**, enter +1 to block patterns that use +1.

Step 4 In the **Remote Call Control Entity** field, enter the name of the remote call control entity that advertises the pattern that you want to block.

Step 5 In the **Remote IP** field, enter the IP address for the remote call control entity where you want to block the learned pattern.

Step 6 Click **Save**.

Call Control Discovery Interactions and Restrictions

Call Control Discovery Interactions

Table 85: Call Control Discovery Interactions

Feature	Interaction
Alarms	Cisco Unified Serviceability provides alarms to support the call control discovery feature. For information about how to configure alarms, see the *Cisco Unified Serviceability Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.
BLF Subscriptions	For a user to subscribe BLF status of a SAF learned pattern, Unified Communications Manager sends a SIP subscribe message over a SIP trunk to the remote cluster. This functionality is supported with only SAF-enabled SIP trunks.
Bulk Administration Tool	In the Bulk Administration Tool, you can import and export the configuration for SAF security profiles, SAF forwarder, CCD advertising service, CCD requesting service, hosted DN groups, and hosted DN patterns.
Call Detail Records	Unified Communications Manager supports redirecting onBehalfOf as SAFCCDRequestingService with a redirection reason as SS_RFR_SAF_CCD_PSTNFAILOVER, which indicates that the call is redirected to a PSTN failover number.
Incoming Called Party Settings	The H.323 protocol does not support the international escape character +. To ensure that the correct DN patterns are used with SAF and call control discovery for inbound calls over H.323 gateways or trunks, you must configure the incoming called party settings in the service parameter, device pool, H.323 gateway, or H.323 trunk windows; that is, configure the incoming called party settings to ensure that when a inbound call comes from a H.323 gateway or trunk, Unified Communications Manager transforms the called party number back to the value that was originally sent over the trunk or gateway. For example, a caller places a call to +19721230000 to Unified Communications Manager A. Unified Communications Manager A receives +19721230000 and transforms the number to 55519721230000 before sending the call to the H.323 trunk. In this case, your configuration indicates that the international escape character + should be stripped and 555 should be prepended for calls of International type. For this inbound call from the trunk, Unified Communications Manager B receives 55519721230000 and transforms the number back to +19721230000 so that digit analysis can use the value as it was sent by the caller. In this case, your configuration for the incoming called party settings indicates that you want 555 to be stripped and +1 to be prepended to called party numbers of International type.

Feature	Interaction
Digest Authentication	Unified Communications Manager uses digest authentication (without TLS) to authenticate to the SAF forwarder. When Unified Communications Manager sends a message to the SAF forwarder, Unified Communications Manager computes the SHA1 checksum and includes it in the MESSAGE-INTEGRITY field in the message.
QSIG	The QSIG Variant and ASN.1 ROSE OID Encoding settings in the **H.323 Configuration** window are advertised by the CCD advertising service. These settings affect decoding of QSIG messages for inbound tunneled calls; for call control discovery, they do not affect outgoing calls. The remote call-control entity determines whether QSIG tunneling is required for outgoing calls over H.323 trunks. If the remote call-control entity advertises that QSIG tunneling is required, the QSIG message is tunneled in the message of the outgoing call, even if the **H.323 Configuration** window in Cisco Unified CM Administration indicates that QSIG support is not required.

Call Control Discovery Restrictions

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

CHAPTER 77

Configure External Call Control

External Call Control Overview

External call control lets an adjunct route server make call routing decisions for Unified Communications Manager by using the Cisco Unified Routing Rules Interface. When you configure external call control, Unified Communications Manager issues a route request that contains the calling party and called party information to the adjunct route server. That server receives the request, applies appropriate business logic, and returns a route response that instructs your system on how to route the call and any additional call treatment to apply.

The adjunct router influences how your system allows, diverts, or denies calls; modifies calling and called party information; plays announcements to callers; resets call history so that adjunct voicemail and IVR servers can properly interpret calling and called party information; and logs reason codes that indicate why calls were diverted or denied.

External call control provides the following functions:

- Best Quality Voice Routing—The adjunct route server monitors network link availability, bandwidth usage, latency, jitter, and MOS scores to ensure that calls are routed through voice gateways that deliver the best voice quality to all call participants.
- Least Cost Routing—The adjunct route server is configured with carrier contract information such as local access and transport area (LATA) and inter-LATA rate plans, trunking costs, and burst utilization costs to ensure that calls are routed over the most cost effective links.
- Ethical Wall—The adjunct route server is configured with corporate policies that determine reachability, for example, whether user 1 is allowed to call user 2.

External Call Control Prerequisites

This feature requires the Cisco Unified Routing Rules XML Interface, which directs your system on how to handle calls.

For more information, see the *Cisco Unified Routing Rules Interface Developers Guide* (CURRI documentation) at https://developer.cisco.com.

External Call Control Configuration Task Flow

Before you begin

- Review External Call Control Prerequisites, on page 589.

Procedure

	Command or Action	Purpose
Step 1	Configure a Calling Search Space for External Call Control, on page 591	Configure a calling search space for your system to use when the route server sends a divert obligation. A calling search space comprises an ordered list of route partitions that you assign to devices. Calling search spaces determine the partitions that calling devices search when they attempt to complete a call.
Step 2	Configure an External Call Control Profile, on page 592	Configure an external call control profile to provide the URIs for the adjunct route server, a calling search space that is used for diverting calls, a timer that indicates how long your system waits for a response from the adjunct route server, and so on.
Step 3	Assign a Profile to a Translation Pattern, on page 592	For the translated patterns that you want to use with external call control, assign an external call control profile to the pattern. When a call occurs that matches the translation pattern, your system immediately sends a call routing query to an adjunct route server, and the adjunct route server directs your system on how to handle the call.
Step 4	(Optional) Import the Route Server Certificate into the Trusted Store, on page 593	If the route server uses HTTPS, import the certificate for the route server into the trusted store on your system node. You must perform this task on each node in the cluster that can send routing queries to the route server. If you use HTTPS for the primary or secondary web service URIs in the external call control profile, your system uses certificates to mutually authenticate through a TLS connection to the configured adjunct route servers.
Step 5	(Optional) Export the Self-Signed Certificate to the Route Server, on page 594	If the route server uses HTTPS, export the Cisco Unified Communications Manager self-signed

	Command or Action	Purpose
		certificate to the route server. You must perform this task for each node in the cluster that can send routing queries to the route server. To ensure that the primary and redundant route servers can authenticate with Cisco Unified Communications Manager through HTTPS, you must generate a self-signed certificate that you can import to each adjunct route server that sends directives to your system. Perform this procedure for each node in the cluster that can contact the primary and redundant adjunct route server.
Step 6	(Optional) Configure the Chaperone Function, on page 594	Configure chaperone functionality if your routing rules from the route server state that a chaperone must monitor or record a call. A chaperone is a designated phone user who can announce company policies in the call, monitor the call, and record the call.
Step 7	(Optional) Configure Customized Announcements, on page 595	Follow this procedure if your routing rules require that an announcement is played for some calls and you do not want to use the Cisco-provided announcements.

Configure a Calling Search Space for External Call Control

Configure a calling search space for your system to use when the route server sends a divert obligation. A calling search space comprises an ordered list of route partitions that you assign to devices. Calling search spaces determine the partitions that calling devices search when they attempt to complete a call.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **Calling Search Space**.

Step 2 Click **Add New**.

Step 3 In the **Name** field, enter a name.

Ensure that each calling search space name is unique to the system. The name can include up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_).

Step 4 In the **Description** field, enter a description.

The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).

Step 5 From the **Available Partitions** drop-down list, perform one of the following steps:

- For a single partition, select that partition.
- For multiple partitions, hold down the **Control (CTRL)** key, then select the appropriate partitions.

Step 6 Select the down arrow between the boxes to move the partitions to the **Selected Partitions** field.

Step 7 (Optional) Change the priority of selected partitions by using the arrow keys to the right of the **Selected Partitions** box.

Step 8 Click **Save**.

What to do next

Configure an External Call Control Profile, on page 592

Configure an External Call Control Profile

Configure an external call control profile to provide the URIs for the adjunct route server, a calling search space that is used for diverting calls, a timer that indicates how long your system waits for a response from the adjunct route server, and so on.

Before you begin

Configure a Calling Search Space for External Call Control, on page 591

Procedure

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

Step 2 Perform one of the following tasks:

- To modify the settings for an an existing external call control profile, enter search criteria, click **Find**, and then choose an existing external call control profile from the resulting list.
- To add a new external call control profile, click **Add New**.

Step 3 Configure the fields on the **External Call Control Profile Configuration** window. See the online help for more information about the fields and their configuration options.

Step 4 Click **Save**.

What to do next

Assign a Profile to a Translation Pattern, on page 592

Assign a Profile to a Translation Pattern

Configure an external call control profile to provide the URIs for the adjunct route server, a calling search space that is used for diverting calls, a timer that indicates how long your system waits for a response from the adjunct route server, and so on.

Before you begin

Configure an External Call Control Profile, on page 592

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Translation Pattern**.

Step 2 Perform one of the following tasks:

- To modify the settings for an existing translated pattern, enter search criteria, click **Find**, and then choose an existing translated pattern from the resulting list.
- To add a new translated pattern, click **Add New**.

Step 3 From the **External Call Control Profile** drop-down list, choose the external call control profile that you want to assign to the pattern.

Step 4 Configure other fields as needed in the **Translation Pattern Configuration** window. See the online help for more information about the fields and their configuration options.

Step 5 Click **Save**.

What to do next

(Optional) Import the Route Server Certificate into the Trusted Store, on page 593

Import the Route Server Certificate into the Trusted Store

If the route server uses HTTPS, import the certificate for the route server into the trusted store on your system node. You must perform this task on each node in the cluster that can send routing queries to the route server. If you use HTTPS for the primary or secondary web service URIs in the external call control profile, your system uses certificates to mutually authenticate through a TLS connection to the configured adjunct route servers.

Before you begin

Assign a Profile to a Translation Pattern, on page 592

Procedure

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

Step 2 Click **Upload Certificate**.

Step 3 In the **Upload Certificate** popup window, click **CallManager-trust** from the **Certificate Name** drop-down list, and browse to the certificate for the adjunct route server.

Step 4 After the certificate appears in the **Upload File** field, click **Upload**.

Step 5 (Optional) Perform this procedure again if your system can contact a redundant adjunct route server.

What to do next

Export the Self-Signed Certificate to the Route Server, on page 594

Export the Self-Signed Certificate to the Route Server

If the route server uses HTTPS, export the Cisco Unified Communications Manager self-signed certificate to the route server. You must perform this task for each node in the cluster that can send routing queries to the route server. To ensure that the primary and redundant route servers can authenticate with Cisco Unified Communications Manager through HTTPS, you must generate a self-signed certificate that you can import to each adjunct route server that sends directives to your system.

Perform this procedure for each node in the cluster that can contact the primary and redundant adjunct route server.

Before you begin

Import the Route Server Certificate into the Trusted Store, on page 593

Procedure

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

Step 2 In the **Certificate List** window, click **Generate New**.

Step 3 From the **Certificate Name** drop-down list, choose **CallManager**.

Step 4 Click **Generate New**.

Step 5 From the **Find and List Certificates** window, choose the **CallManager.pem** certificate that you just created.

Step 6 After the certificate file data appears, click **Download** to download the certificate to a location that you can use for exporting the certificate to the adjunct route server.

Step 7 Export the certificate to each adjunct route server that sends directives.

What to do next

(Optional) Configure the Chaperone Function, on page 594

Configure the Chaperone Function

Configure chaperone functionality if your routing rules from the route server state that a chaperone must monitor or record a call. A chaperone is a designated phone user who can announce company policies in the call, monitor the call, and record the call.

Cisco Unified Communications Manager provides the following capabilities to support chaperone functionality, as directed by the adjunct route server:

- Redirect an incoming call to a chaperone, hunt group, or a list of chaperones.
- Provide a chaperone with the ability to record a call.

When the chaperone is connected to the caller or when the chaperoned conference is established, the **Record** softkey or programmable line key (PLK) (depending on the phone model) is active on the phone so that the chaperone can invoke call recording. Call recording occurs for only the current call, and call recording stops when the current call ends. Messages that indicate the status of recording may display on the phone when the chaperone presses the recording softkey or PLK.

Before you begin

(Optional) Export the Self-Signed Certificate to the Route Server, on page 594

Procedure

Step 1 For phones on which you want to enable recording, set the Built-in-Bridge to **On** in the **Phone Configuration** window.

Step 2 Create a recording profile:

a) Choose **Device** > **Device Settings** > **Recording Profile**.

b) Create a Call Recording Profile for the phones that can record chaperoned conferences.

Step 3 Apply the recording profile to the line appearance.

Step 4 Add a SIP trunk to point to the recorder.

Step 5 Create a route pattern that points to the SIP trunk.

Step 6 Configure the following service parameters:

a) Play Recording Notification Tone to Observed Target

b) Play Recording Notification Tone to Observed Connected Target

Step 7 Assign the Standard Chaperone Phone softkey template to the phone that the chaperone uses.

Step 8 Perform the following steps from **Call Routing** > **Directory Number** for a new phone or from **Device** > **Phone** if the phone is already configured:

a) Configure only one directory number (DN) for the chaperone phone.

b) For the DN on the chaperone phone, choose **Device Invoked Call Recording Enabled** from the **Recording Option** drop-down list.

c) For the DN on the chaperone phone, enter `2` for the **Maximum Number of Calls** setting, and enter `1` for the **Busy Trigger** setting.

Step 9 For Cisco Unified IP Phones that support the **Record** softkey, configure the Standard Chaperone Phone softkey template so that only the **Conference**, **Record**, and **End Call** softkeys display on the phone in a connected state.

Step 10 For Cisco Unified IP Phones that support the record programmable line key (PLK), configure the PLK in the **Phone Button Template Configuration** window.

Step 11 (Optional) If you have more than one chaperone in your cluster, add the chaperone DN to the chaperone line group that you plan to assign to the chaperone hunt list.

This step ensures that an available chaperone monitors the call.

What to do next

(Optional) Configure Customized Announcements, on page 595

Configure Customized Announcements

Follow this procedure if your routing rules require that an announcement is played for some calls and you do not want to use the Cisco-provided announcements.

Tip: Do not use embedded spaces for the announcement identifier.

If other language locales are installed, you can upload other .wav files for this announcement to use with those locales.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Media Resources** > **Announcement**.

Step 2 Perform one of the following tasks:

- To add a new announcement:

a) Click **Add New**.
b) In the **Announcement Identifier** field, enter an announcement identifier.
c) In the **Description**, enter a description of the announcement.
d) From the **Default Announcement** drop-down list, choose a default Cisco-provided announcement if desired.
e) Click **Save**.

- To upload a custom .wav file for the announcement:

a) Click **Upload File**.
b) From the **Locale** drop-down list, choose the locale language for the announcement.
c) Click **Choose File**, and then choose a .wav file to upload.
d) Click **Upload File**.
e) When the upload finishes, click **Close** to refresh the window and show the uploaded announcement.

External Call Control Interactions and Restrictions

External Call Control Interactions

Table 86: External Call Control Interactions

Feature	Interaction
Best Call Quality Routing	You can set up routing rules on the adjunct route server that determine which gateway to use for a call, taking voice quality into consideration. For example, gateway A provides the best voice quality, so it is used for the call. In this case, the adjunct route server monitors network link availability, bandwidth usage, latency, jitter, and mean opinion scores (MOS) to ensure that calls are routed through voice gateways that deliver the best voice quality to all call participants.

Feature	Interaction
Call Detail Records	External Call Control functions can be displayed in call detail records; for example, the call detail record can indicate whether the adjunct route server permitted or rejected a call. In addition, the call detail record can indicate whether Cisco Unified Communications Manager blocked or allowed calls during which it did not receive a decision from the adjunct route server.
Call Forward	External Call Control intercepts calls at the translation pattern level, while Call Forward intercepts calls at the directory number level. External Call Control has a higher priority than Call Forward; for calls that invoke Call Forward, Cisco Unified Communications Manager sends a routing query to the adjunct route server if the translation pattern is assigned to an External Call Control profile. Call Forward is triggered only when the adjunct route server sends a Permit decision with a Continue obligation to the Cisco Unified Communications Manager. **Note** The **Call Diversion Hop Count** service parameter that supports External Call Control and the **Call Forward Call Hop Count** service parameter that supports Call Forward are independent of each other.
Call Pickup	When a phone user tries to pick up a call by using the Call Pickup feature, External Call Control is not invoked; Cisco Unified Communications Manager does not send a routing query to the adjunct route server for that portion of the call.
Chaperones	A chaperone is a designated phone user who can announce company policies to the call, monitor the call, and record the call, if required. Chaperone restrictions exist so that the parties that are involved in the call cannot converse without the presence of the chaperone.
Cisco Unified Mobility	Cisco Unified Communications Manager allows the route decision from the adjunct route server for the following Cisco Unified Mobility features: • Mobile Voice Access • Enterprise Feature Access • Dial-via-Office Reverse Callback Cisco Unified Communications Manager does not send a routing query for the following Cisco Unified Mobility features: • Cell pickup • Desk pickup • Session handoff
Conferences	When a phone user creates a conference, External Call Control may be invoked for the primary call and consultative call.

Feature	Interaction
Directory Numbers	When you configure directory numbers as four- or five-digit extensions (enterprise extensions), you need to configure two translation patterns if on-net dialing supports four or five digits. One translation pattern supports globalizing the calling and called numbers, and a second translation pattern supports localizing the calling and called numbers.
Do Not Disturb	By default, the DND setting for the user takes effect when the user rule on the adjunct route server indicates that the adjunct route server sent a continue obligation. For example, if the adjunct route server sends a continue obligation, and the user has DND-R enabled, Cisco Unified Communications Manager rejects the call.
Emergency Call Handling	**Caution** We strongly recommend that you configure a very explicit set of patterns for emergency calls (for example, 911 or 9.11) so that the calls route to their proper destination (for example, to Cisco Emergency Responder or a gateway) without having to contact the route server for instructions on how to handle the call.
Transfer	When a phone user transfers a call, External Call Control may be invoked for both the primary call and consultative call. However, Cisco Unified Communications Manager cannot enforce any routing rules from the adjunct route server between the party that transfers and the target of the transfer.

External Call Control Restrictions

Table 87: External Call Control Restrictions

Restriction	Description
Adding Parties	The chaperone cannot use the phone to add parties to a conference after the conference begins, because the call must be put on hold for the chaperone to add parties. The other parties on the conference may add additional parties to the conference. The configuration for the **Advanced Ad Hoc Conference Enabled** service parameter, which supports the Cisco CallManager service, determines whether other parties can add participants to the conference. If the service parameter is set to **True**, other parties can add participants to the conference.
Call Transfer	The chaperone cannot use the phone to transfer the conference call to another party.
Conference Log Out	When the chaperone leaves the conference, the entire conference ends.
Conference Softkey	After the chaperone creates a conference, the **Conference** softkey, if available, is disabled on the phone.
Hold	The chaperone cannot use the phone to put the conference call on hold.
Recording	If the chaperone starts recording before the feature makes a consultative call to the party that will join the conference, Cisco Unified Communications Manager suspends recording while the chaperone makes the consultative call; recording resumes after the conference is established.

CHAPTER 78

Configure Call Queuing

Call Queuing Overview

Cisco Unified Communications Manager provides Call Queuing to place callers in a queue until hunt members are available to answer them. An administrator can set the default so callers receive an initial greeting announcement before the call is extended to an agent or the default can be changed so the initial announcement plays only after the caller is put in the queue followed by Music On Hold or Tone On Hold. If the caller remains in queue for a specified period of time, a secondary announcement is played at a configured interval until the call can be answered or until the maximum wait timer expires.

When an incoming call reaches the hunt pilot, the following functions are provided:

- A caller may be connected to an initial customizable greeting announcement before proceeding.
- If one or more line members are logged in to the hunt pilot and are in an idle state, and if no calls are queued, the call is extended to the line member that has been idle for the longest period of time.
- If no line members answer a call, that caller is not placed in queue. The call is routed to a new destination or disconnected, based on the setting When no hunt members answer, are logged in, or registered.
- If a line member does not answer a queue-enabled call, that line member is logged off the hunt group only if the setting **Automatically Logout Hunt Member on No Answer** is selected in the Line Group setting window.
- Calls are placed in queue only if all members are busy.
- A caller who is waiting in queue may hear Music On Hold and a repeating (customizable) periodic announcement.
- After a line member becomes idle, the caller with the longest wait time across multiple hunt groups is extended to the idle line member. If the idle line member does not answer the call, the caller is returned to the previous position in the queue.
- If a queued call exceeds its maximum wait time or the maximum number of callers allowed in queue is exceeded, the call can be routed to an alternate number or it can be disconnected, depending on how the hunt pilot is configured. The alternate number can be one of the following:
  - A hunt pilot DN with queuing either enabled or disabled
  - A voicemail DN

  - A line DN
  - A shared DN

- Line members can display the queue status of their queue-enabled hunt pilots. The queue status display provides the following types of information:
  - Hunt pilot pattern
  - Number of queued callers on each hunt pilot
  - Longest waiting time

Call queuing works in conjunction with existing hunt pilots, but there are no changes in the behavior of the hunting operation for either queuing or nonqueuing hunt pilots. Hunt pilots that have call queuing enabled provide the following features:

- Queuing-enabled hunt pilot calls can only be received by line members one call at a time. Two queuing-enabled hunt pilot calls cannot be offered to a line member. A line member can receive calls directly to the DN or from non-queuing hunt pilots.
- Line members who do not answer calls that are routed by hunt pilots are automatically logged out. A line member is automatically logged out of a device if the line member receives a queuing-enabled hunt pilot call and does not answer the call before timeout occurs. In the case of a shared-line deployment, all devices configured with the same shared line are logged out. You can configure this behavior from the Line Group setting window by selecting Automatically Logout Hunt Member on No Answer. Line members are logged out only if this check box is checked.

For information about Call Queuing monitoring or announcements monitoring, see *Cisco Unified Real Time Monitoring Tool Administration Guide*.

You can configure the inbound calls to change to the connected call state before playing the queuing announcement while the call is extended to a hunt member in the queuing-enabled hunt pilot.

Call Queuing Prerequisites

- Cisco IP Voice Media Streaming (IPVMS) Application, which should be activated on at least one node in the cluster
- Cisco CallManager service that is running on at least one server in the cluster
- Cisco RIS Data Collector service that is running on the same server as the Cisco CallManager service
- Cisco Unified Communications Manager Locale Installer, if you want to use non-English phone locales or country-specific tones

Call Queuing Task Flow

Before you begin

Configure Announcements

Cisco Unified Communications Manager allows you to:

- use the existing Cisco-provided announcements,
- change the message or tone that you want an announcement to play,
- insert custom announcement .wav files,
- assign the locale for the announcement,
- change the description for the announcement,
- change the message or tone that you want an announcement to play.

Feature announcements are used by specific features such as Music On Hold (MoH) in association with Hunt Pilot call queuing or External Call Control.

There are up to 50 feature announcements available. These announcements can be Cisco-provided audio files or uploaded custom .wav files.

All custom announcement .wav files must be uploaded to all servers in the cluster.

Procedure

Step 1 In Cisco Unified Communications Manager, select **Media Resources** > **Announcements**.

The **Find and List Announcements** window displays.

Step 2 Select a hyperlink to the announcement you want to use.

Example:

Hyperlink—Wait_In_Queue_Sample
You can edit the announcement description or choose a customized announcement if uploaded.

Step 3 To upload a .wav file to use as a custom announcement, click **Upload File**.
The **Upload File** window opens.

Step 4 In the **Upload File** window, choose the locale, enter the filename or browse to select the .wav file, and click **Upload File**.

The upload process begins, and may take a few minutes depending on the file. The Status is updated after processing is complete.

Step 5 Click **Close** to close the upload window.
The **Announcement Configuration** window refreshes to update the uploaded file status.

Step 6 To play the customized announcement, ensure that the **Enable** check box is checked in the Announcement by Locale pane in the **Announcements Configuration** window.

Step 7 After you make the changes in the **Announcements Configuration** window, click **Save**.

What to do next

You must upload the announcement on each node in the cluster, because the announcement files are not propagated between servers in a cluster. Browse to Cisco Unified Communications Manager Administration on each server in the cluster and repeat the upload process.

Configure Music On Hold

You can configure Music On Hold (MoH) to play an optional initial greeting announcement when a caller is first put on hold and also to play a periodic repeating announcement. These announcements can use one of the Cisco-provided audio files or a file that is uploaded into the system.

Perform the following procedure to add or update a Music On Hold audio source, to associate an existing audio source with an audio stream number, or to upload a new custom audio source.

Procedure

Step 1 From the Cisco Unified Communications Manager, choose **Media Resources** > **Music On Hold Audio Source**.

The **Find and List Music On Hold Audio Sources** window appears.

Step 2 To add a new Music On Hold audio source, click **Add New**. To update a Music On Hold audio source, locate a specific Music On Hold audio source. Based on the search criteria you specify, the system displays search results for the record that matches all the criteria.

Step 3 Enter the appropriate settings, as described in Audio Source Fields for Music On Hold, on page 602.

Step 4 Click **Save.**
The list box at the bottom of the window shows the new Music On Hold audio source. The MOH Audio Source File Status pane shows the MOH audio translation status for the added source.

Audio Source Fields for Music On Hold

Table 88: Music On Hold Audio Source Information

Field	Description
MOH Audio Stream Number	Use this field to choose the stream number for this MOH audio source. Click the drop-down arrow and choose a value from the list. For existing MOH audio sources, the value appears in the MOH Audio Source title.
MOH Audio Source File	Use this field to choose the file for this MOH audio source. Click the drop-down arrow and choose a value from the list.
MOH Audio Source Name	Enter a unique name in this field for the MOH audio source. This name includes up to 50 valid characters, such as letters, numbers, spaces, dashes, dots (periods), and underscores.
Allow Multicasting	Check this check box to specify that the selected MOH audio source allows multicasting.

Field	Description
MOH Audio Source File Status	This pane displays the following information about the source file for the selected MOH audio source: • InputFileName • ErrorCode • ErrorText • DurationSeconds • DiskSpaceKB • LowDateTime • HighDateTime • OutputFileList • MOH Audio Translation completion date **Note** OutputFileList includes information on ULAW, ALAW, G.729, and Wideband wav files and status options.

Table 89: Announcement Settings

Field	Description
Initial Announcement	Choose an initial announcement from the drop- **Note** To select MoH with no initial anno Click the **View Details** link to view the followi • Announcement Identifier • Description • Default Announcement **Note** • Played by MOH server only v and "Initial Announcement P • Played by ANN if "Allow Mu is set to 'Always.'
Initial Announcement Played	Choose one of the following to determine whe • Play announcement before routing to Hun • Play announcement if call is queued

Field	Description
Periodic Announcement	Choose a periodic announcement from the drop-do **Note** To select MoH with no periodic annou Click the **View Details** link to view the following • Announcement Identifier • Description • Default Announcement **Note** The MOH server always plays the per
Periodic Announcement Interval	Enter a value (in seconds) that specifies the period default value is 30.
Locale Announcement	Locale Announcement depends upon the locale ins **Note** • Prompts played by MOH will use • Prompts played by ANN will use

Table 90: Music On Hold Audio Sources

Field	Description
(list of MoH audio sources)	This list box shows the MOH audio source that yo source to configure that MoH audio source. Audio source ID is an ID that represents an audio s include either a file on a disk or a fixed device fron streaming data. An MOH server can support up to audio source ID, can stream as unicast and multica **Note** If you select **<None>** , the system defau **Hold MoH Audio Source ID**) is used
Upload File	To upload an MOH audio source file that does not **Upload File** window, either enter the path of an au After you locate the audio source file, click the **Up** file gets uploaded, the Upload Result window disp window. **Note** When you upload a file, the file is upl server and performs audio conversions on the size of the original file, process **Note** Uploading an audio source file to an M must upload an audio source file to ea Communications Manager Administra automatically propagate to other MOH

Configure Hunt Pilot Queuing

When a hunt pilot has more calls distributed through the call distribution feature than its hunt members can handle at any given time, call queuing holds these calls in a queue until they can be answered.

When queuing is enabled, both Forward Hunt No Answer and Forward Hunt Busy are automatically disabled. Conversely, if Forward Hunt No Answer or Forward Hunt Busy is enabled, queuing is automatically disabled.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, select **Call Routing** > **Route/Hunt** > **Hunt Pilot** to configure hunt pilots.

Step 2 Select the hunt pilot that you need to configure for Queuing.

Step 3 Navigate to the Queuing section of the **Hunt Pilot Configuration** window.

Step 4 Check the **Queue Calls** check box to enable queuing.

Step 5 Choose a Music On Hold (MoH) source from the drop-down list box to be used to play announcements and provide queue hold treatments.

The MoH source can be configured as unicast or multicast. The caller-side Media Resource Group List (MRGL) takes precedence for multicast or unicast.

If you do not select a source, the default Network Hold MoH/MoH Source and Announcements is used.

The MoH source announcement locale is used to determine the language used for the announcement. Only one type of language announcement can be played per hunt pilot.

Step 6 In the **Maximum Number of Callers Allowed in Queue** field, enter an integer value for the number of callers allowed in the queue for this hunt pilot.

The default value is 32. The field range is from 1 to 100.

Step 7 Choose one of the following options when the maximum number of callers in the queue is reached:

- If you want subsequent calls to be disconnected, select **Disconnect the call**.
- If you want subsequent calls to be routed to a secondary destination, select **Route the call to this destination**. Provide a specific device DN, shared line DN, or another hunt pilot DN.
- (Optional) You may also select **Full Queue Calling Search Space** from the drop-down list. Used to determine which partition to search when attempting to complete a call.

Step 8 In the Maximum Wait Time in Queue field, enter an integer value to set the maximum wait time, in seconds, in a queue.

The default value is 900 seconds. The field range is from 10 to 3600 seconds.

Step 9 Choose one of the following options when the maximum wait time is reached:

- If you want that call to be disconnected, select **Disconnect the call**.
- If you want that call to be routed to a secondary destination, select **Route the call to this destination**. Provide a specific device DN, shared line DN, or another hunt pilot DN.
- (Optional) You may also select **Maximum Wait Time Calling Search Space** from the drop-down list. Used to determine which partition to search when attempting to complete a call.

Step 10 When no line members are logged in or registered at the time of an incoming call, choose one of the following options:

- If you need that call to be disconnected, select **Disconnect the call**.
- If you need that call to be routed to a secondary destination, select **Route the call to this destination**. Provide a specific device DN, shared line DN, or another hunt pilot DN.
- (Optional) You may also select **No hunt members logged in or registered Calling Search Space** from the drop-down list. Used to determine which partition to search when attempting to complete a call.

Step 11 Click **Save**.

Automatically Logout Hunt Member on No Answer

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Call Routing** > **Route/Hunt > Line Group** to configure line groups.

Step 2 Choose the line group that you need to configure from the **Find and List Line Groups** window.

Step 3 Navigate to the Hunt Options section of the **Line Group Configuration** window.

Step 4 Ensure that the **Automatically Logout Hunt Member on No Answer** check box is checked.

Step 5 Click **Save**.

Call Queuing Interactions and Restrictions

Call Queuing Interactions

Feature	Interaction
SIP Rel1XX Options	If a call is routed to a queuing-enabled hunt pilot through SIP ICT, the SIP ICT uses the SIP profile that has SIP Rel1XX Options set to **Send PRACK if 1XX contains SDP**. As a result, the initial announcement is played to every call before the call is extended to the line member. The above existing interaction for SIP ICT does not apply if **Connect Inbound Call before Playing Queuing Announcement** checkbox is checked under **DeviceDevice Settings SIP Profile** > **Trunk Specific Configuration** in Cisco Unified CM Administration. If **Connect Inbound Call before Playing Queuing Announcement** checkbox is not checked the interaction for SIP ICT remains the same. However, it does not guarantee the initial announcement can always be heard by a caller from the PSTN side. The initial announcement will not be heard by a caller from the PSTN side if the PSTN provider doesn't open the voice path until a Connect message is received on the call.
Hunt Pilots and Hunt Groups	• The logoff notification functionality for hunt groups changes when Call Queuing is enabled for a hunt pilot. If Call Queuing is enabled for a hunt pilot, the Hunt Group Logoff Notification does not play when users log out of a hunt group or are logged off because they missed their turn in the queue. • If the hunt list has multiple line groups, these line groups must have the same setting for **Automatically Logout Hunt Member on No Answer**. • Hunt Pilot still queues calls, even when all hunt members are logged out.The line group members should not be added in more than one line group and even if they are added in second line groups, those second line groups should not be in the same Hunt list. • All hunt options must be set to Try Next Member, then Try Next Group in the hunt list.

Call Queuing Restrictions

The following general restrictions apply to call queuing:

- H.323 Fast Start does not support Call Queuing.
- Queue status PLK is supported only with the following LCD display phones for both SCCP and SIP: 6921, 6941, 6945, 6961, 7911G, 7931G, 7942G, 7945G, 7962G, 7965G, 7975G, 8961, 8945, 8941, 9951, 9971, 7800 and 8800 series.
- Log Out of Hunt Groups (HLog) is not compatible with Cisco Extension Mobility Cross Cluster (EMCC); Call Queuing should not be deployed with EMCC.
- Unified Communications Manager does not support Unified Mobility with Call Queuing.
- In a H323 to SIP interworking scenario, the user may not hear initial announcement, MoH, periodic announcement or observe call failure in a native call queuing flow due to interworking delays. In such a scenario it is advised to use only SIP protocol.

Performance and Scalability for Hunt Pilots with Call Queuing

The following performance and scalability restrictions apply:

- A single Unified CM Cluster supports a maximum of 15,000 hunt list devices.
- A single Unified CM Subscriber supports a maximum of 100 hunt pilots with call queuing enabled per node
- Hunt list devices may be a combination of 1500 hunt lists with ten IP phones in each hunt list, 750 hunt lists with twenty IP phones in each hunt list, or similar combinations

Note When using the broadcast algorithm for call coverage, the number of hunt list devices is limited by the number of busy hour call attempts (BHCA). Note that a BHCA of 10 on a hunt pilot pointing to a hunt list or hunt group containing 10 phones and using the broadcast algorithm is equivalent to 10 phones with a BHCA of 10.

- The maximum number of hunt pilots is 100 per Unified CM subscriber node with call queue enabled when configured with 32 callers which is allowed in the queue. The total number of queue slots per node (the value of "Maximum Number of Callers Allowed in Queue" for all Call Queuing Enabled Hunt Pilots on the node combined) is limited to 3200. The maximum number of simultaneous callers in a queue for each hunt pilot is 100, meaning 100 callers per hunt pilot is allowed in a queue and the maximum number of hunt pilots is reduced to 32. The maximum number of members across all hunt lists does not change when call queuing is enabled.
- The maximum wait time in queue for each hunt pilot that you can configure ranges from 0 to 3600 seconds (default 900). An increase in the number of hunt lists can require you to increase the dial plan initialization timer that is specified in the Unified Communications Manager service parameters. We recommend that you set the dial plan initialization timer to 600 seconds if you have 1500 hunt lists configured.

- We recommend having no more than 35 directory numbers for a single line group when using broadcast algorithms with call queuing. Additionally, the number of broadcast line groups depends on the busy hour call completion rate (BHCC). If there are multiple broadcast line groups in a Unified CM system, the number of maximum directory numbers in a line group must be less than 35. The number of busy hour call attempts (BHCA) for all the broadcast line groups should not exceed 35 calls set up per second.

CHAPTER 79

Configure Call Throttling

Call Throttling Overview

Call Throttling allows your system to automatically throttle or deny new call attempts. The system takes this action when conditions cause users to experience a delay in the interval between going off hook and receiving a dial tone.

Some factors that can result in this delay are as follows:

- Heavy call activity
- Low CPU availability
- Routing loops
- Disk I/O limitations
- Disk fragmentation

The system uses the values that are specified in the call throttling parameters to determine a possible delay to dialtone and also to determine when conditions no longer require call throttling.

When throttling is necessary to prevent excessive delay to dialtone, the system enters a Code Yellow state and new call attempts are throttled (denied).

When the system calculates the delay to dialtone as being over the threshold that is configured in the call throttling service parameters, Unified Communications Manager rejects new calls. When call throttling activates, a user who attempts a new call receives a reorder tone and, depending on the phone model, may also receive a prompt on the phone display.

Call throttling effectively prevents the type of excessive delays that can cause a user to complain to the system administrator or question whether the system is down or the phone is broken. Your system constantly monitor the system to anticipate when such latency could occur.

When the delay to dialtone is within the guidelines of the call throttling service parameters, Unified Communications Manager stops throttling calls by exiting the Code Yellow state and new calls are again allowed.

Call Throttling Configuration

⚠

Caution We recommend that you not modify call throttling parameters unless advised to do so by customer support.

Call throttling occurs automatically when your system detects conditions such as heavy call activity, low CPU availability, and disk fragmentation. The system automatically exits throttling when these conditions are fixed.

Configure Call Throttling

Call throttling occurs automatically when your system detects conditions such as heavy call activity, low CPU availability, and disk fragmentation. The system automatically exits throttling when these conditions are fixed. Call Throttling is configured via advanced service parameters. For many deployments, the default settings are sufficient.

⚠

Caution We recommend that you not modify call throttling parameters unless advised to do so by customer support.

Procedure

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

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

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

Step 4 Click **Advanced**.

Step 5 Under **Call Throttling**, configure values for the cll throttling service parameters. For parameter help descriptions, click the parameter name in the GUI.

- Code Yellow Entry Latency
- Code Yellow Exit Latency Calendar
- Code Yellow Duration
- Max Events Allowed
- System Throttle Sample Size

Step 6 Click **Save**.

Configure Memory Throttling

Use this procedure to configure memory throttling for your system.

Procedure

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

Step 2 From the **Server** drop-down list, select a Unified Communications Manager server.

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

Step 4 Click **Advanced**.

Step 5 Set the **Enable Memory Throttling** parameter to **True**.

Step 6 Configure values for the additional service parameters in the **Memory Throttling** area. For parameter help, click the parameter name in the GUI.

Step 7 Click **Save**.

CHAPTER 80

Calling Party Normalization

Calling Party Normalization Overview

Calling Party Normalization allows you to globalize and localize phone numbers so that the appropriate calling presentation displays on the phone. Calling Party Normalization enhances the dialing capabilities of some phones and improves callback functionality when a call is routed to multiple geographic locations. The feature allows you to map a global calling party number to its localized variant such that a phone can return a call without modifying the directory number in the call log directories on the phone.

Globalization of the Calling Party Number

By configuring a Calling Party Number Type and prefixes in Cisco Unified CM Administration, you can set Cisco Unified Communications Manager to reformat the calling party number that displays on the called phone to a globalized version that includes prefixes such as international country codes, thereby allowing the number to be dialed from anywhere in the world.

Cisco Unified Communications Manager uses various number patterns, such as route patterns or translation patterns, along with the value for the Calling Party Number Type to globalize a phone number. For example, you can configure Cisco Unified Communications Manager to take a localized German phone number of 069XXXXXXX with a Subscriber calling party number type and globalize it to +49 40 69XXXXXXX, which includes the German country code and city code.

For calls that are routed to multiple geographic locations, the different translation settings that are applied for each routing path can globalize the calling party number uniquely for each call path. Cisco Unified Communications Manager can also be configured such that the phone displays a localized calling party number on the phone screen and the globalized number in the call log directories on the phone. To ensure that the phone user does not need to edit the call log directory entry on the phone before placing a call, map the global calling party number to its local variant.

Localization of the Calling Party Number

For the final presentation of the calling party number, you can configure calling party transformation patterns for each calling party number type (National, International, Subscriber, and Unknown), and apply strip digits and prefix instructions specific to the calling party number type for that call. This allows Cisco Unified Communications Manager to reformat the calling party number such that the calling party number that displays on the called phone is a localized number that does not include unnecessary country codes and international access codes.

For example, assume an incoming number arrives from the PSTN with a globalized number of +49 40 69XXXXXXX where +49 represents the country code, 40 represents the city code, and the calling party number type is Subscriber. Cisco Unified Communications Manager can be configured with a calling party transformation pattern, along with instructions to strip the country code, city code, and add a prefix of 0. After the instructions are applied, the calling party number displays in the dialed phone as 069XXXXXXX.

Map Globalized Calling Party Number to a Localized Version

To ensure that the phone user does not need to edit the call log directory entry on the phone before placing a call, use route patterns and called party transformation patterns to map the global calling party number to a localized version. This ensures that when the called party returns the call, Cisco Unified Communications Manager can route the call to the correct gateway.

Mapping the global calling party number improves callback functionality so that the called party can return a call without having to modify the directory number in the call log directories on the phone.

Calling Party Normalization Prerequisites

Make sure to activate the **Cisco CallManager** service in Cisco Unified Serviceability before you configure Calling Party Normalization. For more information, see the *Cisco Unified Serviceability Administration Guide*.

If you want Cisco Unified Communications Manager to determine the Calling Party Number Type, configure patterns that assign the **Calling Party Number Type** value that matches the calls that you expect. You can create and apply patterns in the following configuration windows:

- Route patterns
- Hunt pilots
- Translation patterns
- Calling party number transformation patterns

Note Calling Party Transformation works only with the original calling party. Any modifications done for redirecting numbers affect only the diversion header. Review your configuration from the SIP trunk chapter, and add a diversion header on the SIP trunk itself.

Calling Party Normalization Configuration Task Flow

Calling Party Normalization prefixes and strip digits rules can be applied in a variety of ways in Unified Communications Manager. For example, you can apply digit transformations to device pools, route patterns, translation patterns, hunt pilots, gateways, and trunks. The manner in which you apply digit transformations depends on how you deploy your dial plan, devices, and trunks. For details, review topics relating to dial plans, route patterns, translation patterns, and transformation patterns.

Procedure

	Command or Action	Purpose
Step 1	If you want Unified Communications Manager to determine the calling party number type, create a pattern and configure the Calling Party Number Type that matches the calls that you expect. You can create and apply patterns in the following configuration windows: • Route patterns • Hunt pilots • Translation patterns • Calling party number transformation patterns	
Step 2	Globalize Calling Party Numbers, on page 617	For incoming calls that arrive through the PSTN, configure settings that will globalize calling party numbers.
Step 3	Set up Calling Search Spaces, on page 618	Set up your partitions and calling search spaces.
Step 4	Create Calling Party Transformation Patterns, on page 618	Create calling party transformation patterns that transform the calling party number to a globalized or localized version and assign each pattern to a partition.
Step 5	Apply Calling Party Transformation Patterns to a Calling Search Space, on page 619	Apply the incoming Calling Party Transformation CSS to your devices such as device pools, gateways, and trunks

Globalize Calling Party Numbers

For incoming calls that arrive via the PSTN, configure settings that will globalize calling party numbers. You can apply settings that will globalize calling party numbers and apply them to a device pool, or to individual devices. Alternatively, you can configure service parameters that will apply calling party normalization settings on a clusterwide basis.

To globalize calling party numbers, perform the following steps:

Procedure

Step 1 If you want to apply calling party normalization settings to particular devices, perform the following steps:

a) Open the configuration window for the device on which you want to apply settings. For example, device pools, gateways, phones, and trunks.

b) In the Incoming Calling Party Settings section for the configuration window, apply prefix and strip digit instructions for each calling party number type.

Note Cisco Unified Communications Manager includes the prefix in the calling party number field for all additional actions, such as supplementary services including call forwarding, call park, voice messaging, and CDR data that pertain to the call.

Step 2 If you want to use service parameters to globalize calling party numbers on all devices clusterwide, perform the following steps:

a) From Cisco Unified CM Administration, choose **System** > **Service Parameters**.
b) From the **Server** drop-down list, select the server on which you want the service to run.
c) From the **Service** drop-down list, select Cisco CallManager.
d) Click **Advanced**.
e) Configure values for the following parameters, which can be applied on a clusterwide basis to phones, MGCP gateways, or H.323 gateways:

- Incoming Calling Party National Number Prefix
- Incoming Calling Party International Number Prefix
- Incoming Calling Party Unknown Number Prefix
- Incoming Calling Party Subscriber Number Prefix

Note In order for Cisco Unified Communications Manager to apply the clusterwide service parameter settings on a particular phone, the prefix setting for that phone must be set to the default option at both the device and device pool levels.

Set up Calling Search Spaces

Use this procedure if you are setting up calling search spaces to handle the calling party normalization feature.

Procedure

Step 1 In Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **Partitions**.

Step 2 Create partitions for your network.

Step 3 In Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **Calling Search Space**.

Step 4 Create calling search spaces for your calling party transformation patterns.

Step 5 For each calling search space, assign partitions to the calling search spaces

Create Calling Party Transformation Patterns

Use this procedure if you are setting up calling party transformation patterns to handle the calling party normalization feature.

Procedure

Step 1 In Cisco Unified CM Administration, choose **Call Routing** > **Transformation Pattern** > **Calling Party Transformation Pattern**.

Step 2 Create transformation patterns.

Step 3 For each calling party transformation pattern that you create, assign prefixes or strip digits commands that will globalize or localize the calling party number.

Step 4 For each calling party transformation pattern, assign a partition that is associated to one of your calling search spaces.

Apply Calling Party Transformation Patterns to a Calling Search Space

For your devices, assign the incoming Calling Party Transformation CSS to your devices such as device pools, gateways, and trunks.

Procedure

Step 1 In Cisco Unified CM Administration, choose the configuration window that applies to the device on which you want to apply calling party transformations.

- Gateways
- Trunks
- Device Pools

Step 2 To localize calling party numbers, in the Calling Search Space drop-down list box, choose the CSS that contains the calling party transformation pattern that you want to apply.

Note If you configure the CSS against the Device Pool, you must also apply that device pool to your phones.

Step 3 To globalize calling party numbers, in the Incoming Calling Party Settings section, choose the calling search space that contains the calling party transformation pattern that you want to apply.

Calling Party Normalization Service Parameter Examples

The following service parameters can be applied on a clusterwide basis to phones, MGCP gateways, or H.323 gateways. In order for a particular device to use the clusterwide parameter, the prefix in the device configuration must be set to Default.:

- Incoming Calling Party National Number Prefix
- Incoming Calling Party International Number Prefix
- Incoming Calling Party Unknown Number Prefix
- Incoming Calling Party Subscriber Number Prefix

The following table provides examples of prefix and strip digits configurations and how these values can be used to transform the display of the calling party number. For the service parameter configurations, the numbers after the colon represent the number of digits to strip from the beginning of the calling party number while the digits after the colon represent the prefix to add to the beginning of the calling party number.

Table 91: Calling Party Number Normalization Service Parameter Examples

Original Calling Number	Service Parameter Value	Description	Final Calling Number
04423452345	+:1	Strip the first digit then add a prefix of +	+4423452345
04423452345	:2	Strip the first two digits	423452345
552345	+1:6	Strip the first 6 digits and then add a prefix of +1	+1
552345	+1:8	Final number is blank because more digits are stripped than are available	
552345	123	Add a prefix of 123	123552345
blank	+1:2	If calling number is blank no prefix is applied	blank
0442345	:26	Calling Party Normalization allows only 24 digits to be stripped	Cisco Unified Communications Manager does not allow this configuration

Calling Party Normalization Interactions and Restrictions

Calling Party Normalization Interactions

The following table describes feature interactions with the Calling Party Normalization feature.

Feature	Interaction
Transferred Calls	Calling Party Normalization may not be supported for some transferred call scenarios because the transfer feature relies on midcall updates and calling party normalization occurs during initial call setup for each call hop. Following is one example of how calling party normalization can work for transfer. Phone A with extension 12345 and phone number of 972 500 2345 calls Phone B with extension 54321 and phone number 972 500 4321. On Phone B, the calling party number 12345 displays, but Phone B transfers the call through a San Jose gateway to Phone C. During the initial transfer, Phone C displays a calling party number of 972 500 4321, but after the transfer completes, Phone C displays the calling party number for Phone A as 12345.

Feature	Interaction
Forwarded Calls	Forwarded calls support globalization and localization of calling party numbers. For example, a caller with Phone F calls Phone G in Dallas through the PSTN, but Phone G has forwarded calls to Phone H in San Jose. On the incoming Dallas gateway the calling party number displays as 555-5555/Subscriber, but the call is forwarded to a San Jose gateway. The outgoing call from Dallas displays as 972 555 5555. On the incoming San Jose gateway the +1 is prefixed and Phone F displays a calling number of +1 972 555 5555.
Call Detail Records	For details of how calling party normalization works with CDR records, see the *Cisco Unified Communications Manager Call Detail Records Administration Guide*.
Cisco Unified Communications Manager Assistant	Cisco Unified Communications Manager Assistant automatically supports localized and globalized calls if you configure the Calling Party Normalization feature. Cisco Unified Communications Manager Assistant can display localized calling party numbers on the user interfaces. In addition, for an incoming call to the manager, Cisco Unified Communications Manager Assistant can display localized and globalized calling party numbers when filter pattern matching occurs. For information on configuring Cisco Unified Communications Manager Assistant, see the *Feature Configuration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.
Cisco Unity Connection	Cisco Unity Connection does not support the international escape character (+). Therefore, you must ensure that calls to Cisco Unity Connection do not contain the +, so that voice-messaging features work as expected. For Cisco Unity Connection to work as expected, treat this application as a device and configure calling party transformations that ensure that the + does not get sent to this voice-messaging application. If the Cisco Unity Connection server uses a North American-based dial plan, localize the calling party number to NANP format before Cisco Unity Connection receives the calling party number. Because no calling party transformation options exist in Cisco Unified Communications Manager Administration for voice-messaging ports, make sure that you configure the calling party number transformations in the device pool that is associated with the voice-messaging ports. To localize the calling party number, also consider adding prefixes for access codes so that the voice-messaging application easily can redial the number for certain features, such as Live Reply. For example, you can convert +12225551234 to 912225551234, and you can convert international number, +4423453456, to include the international escape code, 90114423453456.

Feature	Interaction
Device Mobility	The Calling Party Transformation CSS of the roaming device pool overrides the device-level configuration of the phone roaming within same Device Mobility Group, even when the Use Device Pool Calling Party Transformation CSS check box in the phone configuration window remains unchecked. The following examples demonstrate how calling party normalization works with device mobility for a phone with a home location of Dallas which is currently roaming in San Jose. When the phone is roaming in San Jose, a call comes through the PSTN from 972 500 1212 <National> in Dallas. On the incoming San Jose gateway, the calling party number gets converted to the global format of + 1 408 500 1212. On the phone that currently is in San Jose, the calling party number displays as 1 972 500 1212. When the phone is roaming in San Jose, a call comes through the PSTN from 500 1212 <Subscriber> from a seven-digit dialing area in San Jose. On the incoming San Jose gateway, the calling party number gets converted to the global format of + 1 408 500 1212. On the phone that currently is in San Jose, the calling party number displays as 9 500 1212.

Calling Party Normalization Restrictions

The following table displays restrictions that the Calling Party Normalization feature has with certain features and system components of Cisco Unified Communications Manager.

Table 92: Restrictions with Calling Party Normalization

Feature	Restriction
Share lines	The calling party number that displays for a shared line depends on the sequence of call control events in Cisco Unified Communications Manager. To avoid displaying an incorrect localized calling party number on a shared line, especially when the shared line occurs in different geographical locations, make sure that you configure the same Calling Party Transformation CSS for different devices that share the same line.
SIP trunks and MGCP gateways	SIP trunks and MGCP gateways can support sending the international escape character, (+) for calls. H.323 gateways do not support the +. QSIG trunks do not attempt to send the +. For outgoing calls through a gateway that supports +, Cisco Unified Communications Manager can send the + with the dialed digits to the gateway. For outgoing calls through a gateway that does not support +, the international escape character + gets stripped when Cisco Unified Communications Manager sends the call information to the gateway.
SIP	SIP does not support the number type, so calls through SIP trunks support only the Incoming Number settings for calling party number types of Unknown.

Feature	Restriction
QSIG	A QSIG configuration usually supports a uniform dial plan. Transformation of numbers and prefixes may cause feature interaction issues if you use QSIG.
Calling Party Transformation CSS	For localizing the calling party number, the device must apply the transformation by using digit analysis. If you configure the Calling Party Transformation CSS as **None**, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.
T1-CAS and FXO ports	The Calling Party Transformation CSS settings do not apply to T1-CAS and FXO ports on the gateway.
Cisco Unity Connection	CiscoUnity Connection does not support the international escape character (+). Therefore, you must ensure that calls to CiscoUnity Connection do not contain the +, so that voice-messaging features work as expected. For detailed information on Cisco Unity Connection, go to http://www.cisco.com/c/en/us/products/unified-communications/unity-connection/index.html.

CHAPTER 81

Configure Push Notifications

Push Notifications Overview

When your cluster is enabled for Push Notifications, Unified Communications Manager and the IM and Presence Service use Google and Apple's cloud-based Push Notification service to push notifications for voice and video calls, instant message notification to Cisco Jabber or Cisco Webex on Android and iOS clients that are running in suspended mode (also known as background mode). Push Notifications allows your system to maintain a persistent communication with Cisco Jabber or Cisco Webex. Push Notifications is required both for Cisco Jabber and Cisco Webex on Android and iOS clients that connect from within the enterprise network, and for clients that register to an on-premise deployment through Expressway's Mobile and Remote Access feature.

How Push Notifications Work

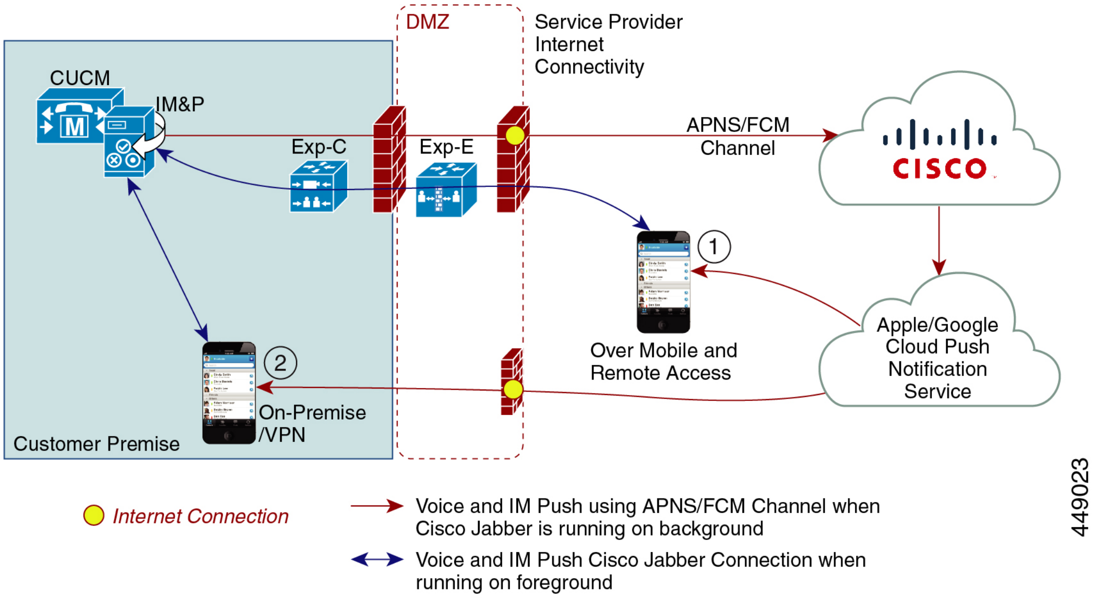
At startup, clients that are installed on Android and iOS platform devices register to Unified Communications Manager, the IM and Presence Service and to the Google and Apple cloud. With Mobile and Remote Access deployments, the clients registers to the on-premises servers through Expressway. So as long as the Cisco Jabber and Cisco Webex client remains in foreground mode,Unified Communications Manager and the IM and Presence Service can send calls and instant messages to the clients directly.

However, once the Cisco Jabber or Cisco Webex clients moves to suspended mode (for example, to maintain battery life), the standard communication channel is unavailable, preventing Unified Communications Manager and IM and Presence Service from communicating directly with the clients. Push Notifications provides another channel to reach the clients through the partner clouds.

Note Cisco Jabber and Cisco Webex is considered to be running in suspended mode if any of the following conditions are true:

- the Cisco Jabber or Cisco Webex application is running off-screen (in the background)
- the Android or iOS device is locked
- the Android or iOS device screen is turned off

Figure 6: Push Notifications Architecture


DMZ
Service Provider Internet Connectivity
CUCM
IM&P
Exp-C
Exp-E
APNS/FCM Channel
1
Over Mobile and Remote Access
Apple/Google Cloud Push Notification Service
2
On-Premise /VPN
Customer Premise
449023
Internet Connection
Voice and IM Push using APNS/FCM Channel when Cisco Jabber is running on background
Voice and IM Push Cisco Jabber Connection when running on foreground

The above diagram displays what happens when Cisco Jabber or Cisco Webex for Android and iOS clients run in the background or are stopped. The figure illustrates: (1) an Mobile and Remote Access deployment where the clients that connects with an on-premises Cisco Unified Communications Manager and IM and Presence Service deployment through Expressway, and (2) a Cisco Jabber or Cisco Webex for Android and iOS clients that connects directly to the on-premises deployment from within the enterprise network.

Note As of iOS13 for Apple clients and supported Android clients, voice calls and messages use separate Push Notifications channels ('VoIP' and 'Message') to reach a client that is running in background mode. However, the general flow is the same for both channels. With iOS 12, voice calls and messages are delivered using the same channel.

Push Notifications Behavior for Cisco Jabber and Cisco Webex

The following table describes the behavior under iOS 12 and iOS 13 for Cisco Jabber or Cisco Webex iOS clients that are registered to Unified Communications Manager and the IM and Presence Service.

Cisco Jabber or Cisco Webex client is running in...	Cisco Jabber is running on an iOS12 Device	Cisco Jabber is running on an iOS13 Device or Android Device
Foreground Mode	**Voice and Video Calls** Unified Communications Manager sends voice and video calls to Cisco Jabber or Cisco Webex clients directly using the standard SIP communications channel. For calls, Unified Communications Manager also sends Push Notifications to Cisco Jabber or Cisco Webex clients that are in foreground mode. However, the standard SIP channel gets used to establish the call, rather than the Push Notifications channel. **Messages** The IM and Presence Service sends messages to the client directly using the standard SIP communication channel. For messages, Push Notifications are not sent to clients that are in foreground mode.	The behaviour is the same as with iOS12.

Cisco Jabber or Cisco Webex client is running in...	Cisco Jabber is running on an iOS12 Device	Cisco Jabber is running on an iOS13 Device or Android Device
Suspended Mode (Background mode)	**Voice or Video Calls** Standard communication channel is unavailable. Unified CM uses the Push Notifications channel. Upon receiving the notification, the Cisco Jabber or Cisco Webex client re-enters foreground mode automatically, and the client rings. **Messaging** Standard communication channel is unavailable. IM and Presence Service uses the Push Notifications channel to send IM notifications as follows: **1.** IM and Presence Service sends the IM notification to the Push REST service in the Cisco cloud, which forwards the notification to the Apple cloud. **2.** The Apple cloud pushes the IM notification to the Cisco Jabber or Cisco Webex client and a notification appears on the Cisco Jabber or Cisco Webex client. **3.** When the user clicks the notification, the Cisco Jabber or Cisco Webex client moves back the foreground. The Cisco Jabber or Cisco Webex client resumes the session with the IM and Presence Service and downloads the instant message. **Note** While the Cisco Jabber or Cisco Webex client is in suspended mode, the user's Presence status displays as **Away**.	With iOS13, call traffic and message traffic is split into separate Push Notifications channels: a 'VoIP' channel for calls, and a "Message" channel for messaging. **Voice or Video Calls** Standard communication channel is unavailable. Unified CM uses Push Notifications 'VoIP' channel. Upon receiving the VoIP notification, Jabber launches CallKit with Caller ID. This behavior holds for Cisco Jabber or Cisco Webex iOS clients. **Messaging** Standard communication channel is unavailable. IM and Presence Service uses Push Notifications 'Message' channel. **1.** IM and Presence Service sends the IM notification to the Push REST service in the Cisco cloud, which forwards the notification to the Apple cloud. **2.** The Apple cloud pushes the IM notification to the Cisco Jabber or Cisco Webex client. **3.** When the user clicks the notification, Cisco Jabber or Cisco Webex client moves to foreground mode. Cisco Jabber or Cisco Webex client resumes the session with the IM and Presence Service and downloads the message. **Note** While Cisco Jabber or Cisco Webex client is in suspended mode, the user Presence displays as **Away**.

Supported Clients for Push Notifications

Client	OS	Platform Cloud	Cloud Service
Cisco Jabber on iPhone and iPad	iOS	Apple	Apple Push Notification Service (APNS)
Cisco Jabber on Android	Android	Google	Android PNS Service
Webex on iOS	iOS	Apple	Apple Push Notification Service (APNS)

Client	OS	Platform Cloud	Cloud Service
Webex on Android	Android	Google	Android PNS Service

Push Notifications Configuration

For details on how to configure and deploy Push Notifications, refer to *Deploying Push Notifications for Cisco Jabber on iPhone and iPad* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

CHAPTER 82

Configure Logical Partitioning

Logical Partitioning Overview

With logical partitioning, you can support PSTN and VoIP calls on a single system while meeting regulatory requirements for call separation. For example, under regulatory constraints in India, all calls that are received from or sent to an external phone must be handed off to and carried by a local or long-distance service provider over the full length of the connection, with the applicable toll charges. You can create a single Unified Communications Manager cluster that routes calls appropriately to the PSTN or the VoIP network according to the caller's location and the phone number being called.

logical partitioning defines which sets of VoIP devices are allowed to communicate with each other. Users do not have to remember to use one line for PSTN and one line for VoIP. Phones making off-net calls are only allowed to talk to a PSTN gateway. It's like having two networks to separately handle your VoIP and PSTN calls, but without the expense of dual infrastructure.

Logical Partitioning Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Enable Logical Partitioning, on page 632	Enable Logical Partitioning.
Step 2	To Configure Geolocations, on page 632, perform the following subtasks: • Create Geolocations, on page 633 • Assign Geolocations, on page 633 • Set the Default Geolocation, on page 634	Configuring geolocations is a two-step process: defining locations and assigning them to devices. You also can set the default location to be used by all devices in the cluster.
Step 3	Configure a Logical Partitioning Default Policy, on page 634	Set up a default policy for devices that are not associated with a geolocation or geolocation

	Command or Action	Purpose
		filter. The policy allows or denies PSTN calls between these devices.
Step 4	Configure Devices to Avoid Logical Partitioning Checks, on page 634	You can specifically exempt devices and device pools from the partitioning checks.
Step 5	To Configure Geolocation Filters, on page 635, perform the following subtasks: • Create Geolocation Filter Rules, on page 635 • Assign Geolocation Filters, on page 636 • Set the Default Geolocation Filter, on page 636	Logical partitioning assigns a unique identifier to each device based on its location. When one device calls another, these identifiers are used to determine whether the call is allowed and what routing is appropriate. You can choose which fields are used to create this identifier. For example, you can apply different policies based on the room or floor within a building.
Step 6	Define a Set of Logical Partitioning Policy Records, on page 637	Define a set of logical partitioning policies for allowing or denying calls between geolocations. Before calls between geolocations are allowed to proceed, the system checks to be sure that calls are allowed between the specified geolocations based on these policies.
Step 7	(Optional) Enable Location Conveyance, on page 637	Configure location conveyance if you want to communicate geolocation information about devices across clusters.

Enable Logical Partitioning

Use this procedure to turn on the Logical Partitioning feature.

Procedure

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

Step 2 For the **Enable Logical Parititioning** enterprise parameter, choose **True** from the drop-down list.

Step 3 Click **Save**.

Configure Geolocations

Configuring geolocations is a two-step process: defining locations and assigning them to devices. You also can set the default location to be used by all devices in the cluster.

Procedure

	Command or Action	Purpose
Step 1	Create Geolocations, on page 633	Configure geolocations to specify geographic locations. These are used to associate devices with regulatory features such as logical partitioning. Geolocations are used in policy decisions, such as in-country regulations.
Step 2	Assign Geolocations, on page 633	Assign a geolocation to a device or device pool.
Step 3	Set the Default Geolocation, on page 634	Specify a default geolocation for all devices and device pools in this cluster.

Create Geolocations

Use this procedure to create geolocations that you can assign to the devices in your system. You can use the geolocations for logical partitioning.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Geolocation Configuration**.

Step 2 Click **Add New**.

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

Step 4 Configure the fields on the **Geolocation Configuration** window. For more information on the fields and their configuration options, see the system Online Help.

Step 5 Click **Save**.

Step 6 Repeat this procedure to create additional geolocations.

Assign Geolocations

Assign a geolocation to a device or device pool.

Procedure

Step 1 From Cisco Unified CM Administration, choose one of the following menu items:

- **Device** > **Phone**
- **Device** > **Trunk**
- **Device** > **Gateway**
- **System** > **Device Pool**

Step 2 Perform one of the following tasks:

- Click **Find** to modify the settings for an existing device or device pool. Enter search criteria, and then choose an existing device or device pool from the resulting list.

- Click **Add New** to add a new device or device pool. For devices, choose device types and protocols as needed and click **Next**.

Step 3 From the Geolocation drop-down list, choose a geolocation that you configured.

Step 4 Click **Save**.

Set the Default Geolocation

Specify a default geolocation for all devices and device pools in this cluster.

Procedure

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

Step 2 From the **Default Geolocation** drop-down list, choose a Geolocation that you configured. The default value is **Unspecified**.

Step 3 Click **Save**.

Step 4 Click **Apply Config**.

Step 5 (Optional) If you need to override this default for a specific device or device pool, enter the value on either the **Device Configuration** or **Device Pool Configuration** window, and then click **Save**.

Configure a Logical Partitioning Default Policy

Set up a default policy for devices that are not associated with a geolocation or geolocation filter. The policy allows or denies PSTN calls between these devices.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Logical Partitioning Policy Configuration**

Step 2 Click **Add New**.

Step 3 Configure the fields on the **Logical Partition Policy Configuration** window. For more information on the fields and their configuration options, see the system Online Help.

Step 4 Click **Save**.

Note If a policy that contained the value Allow is then later changed to Deny, then it remains Deny. The opposite is also true. A policy previously set to Deny, later changed to Allow is an Allow. The **Cisco Unified Reporting** > **Geolocation Policy Report** can help you identify policies that overlap.

Configure Devices to Avoid Logical Partitioning Checks

You can specifically exempt devices and device pools from the partitioning checks.

Procedure

Step 1 From Cisco Unified CM Administration, choose one of the following menu items:

- **Device** > **Phone**
- **Device** > **Trunk**
- **Device** > **Gateway**
- **System** > **Device Pool**

Step 2 Perform one of the following tasks:

- Click **Find** to modify the settings for an existing device or device pool. Enter search criteria and then choose an existing device or device pool from the resulting list.
- Click **Add New** to add a new device or device pool. For devices, choose device types and protocols as needed and click **Next**.

Step 3 From the **Geolocation** drop-down list, choose **Unspecified**.

Step 4 Click **Save**.

Configure Geolocation Filters

Logical partitioning assigns a unique identifier to each device based on its location. When one device calls another, these identifiers are used to determine whether the call is allowed and what routing is appropriate. You can choose which fields are used to create this identifier. For example, you can apply different policies based on the room or floor within a building.

Procedure

	Command or Action	Purpose
Step 1	Create Geolocation Filter Rules, on page 635	Geolocation filters allow you to specify which fields are used to create a geolocation identifier. This feature is used to make policy decisions on a subset of the geolocation objects.
Step 2	Assign Geolocation Filters, on page 636	
Step 3	Set the Default Geolocation Filter, on page 636	Configure the Default Geolocation Filter enterprise parameter to specify a default geolocation filter for a cluster. This parameter determines the default geolocation filter setting for all devices and device pools that are not associated with a geolocation filter.

Create Geolocation Filter Rules

Use this procedure to create geolocation filters that you can use for logical partitioning decisions.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Geolocation Filter**.

Step 2 Click **Add New**.

Step 3 Enter a **Name** and **Description** for the filter.

Step 4 Check the check boxes that correspond to the items you want to use for logical partitioning decisions.

Step 5 Configure the fields on the **Geolocation Filter Configuration** window. For more information on the fields and their configuration options, see the system Online Help.

Step 6 Click **Save**.

Step 7 Repeat these steps to create additional geolocation filters.

Assign Geolocation Filters

Procedure

Step 1 From Cisco Unified CM Administration, choose one of the following menu items:

- **Device** > **Phone**
- **Device** > **Trunk**
- **Device** > **Gateway**
- **System** > **Device Pool**

Step 2 Perform one of the following tasks:

- Click **Find** to modify the settings for an existing device or device pool. Enter search criteria and then choose an existing device or device pool from the resulting list.
- Click **Add New** to add a new device or device pool. For devices, choose device types and protocols as needed and click **Next**.

Step 3 From the **Geolocation Filter** drop-down list, choose a geolocation filter that you configured.

Step 4 Click **Save**.

Set the Default Geolocation Filter

Procedure

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

Step 2 From the **Default Geolocation** drop-down list, choose a Geolocation that you configured. The default value is **Unspecified**.

Step 3 Click **Save**.

Step 4 Click **Apply Config**.

Step 5 (Optional) If you need to override this default for a specific device or device pool, specify the default geolocation filter value on either the **Device Configuration** or **Device Pool Configuration** window, and then click **Save**.

Define a Set of Logical Partitioning Policy Records

Define a set of logical partitioning policies for allowing or denying calls between geolocations. Before calls between geolocations are allowed to proceed, the system checks to be sure that calls are allowed between the specified geolocations based on these policies.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Logical Partitioning Policy Configuration**.

Step 2 Perform one of the following tasks:

- Click **Find** to modify the settings for an existing logical partitioning policy. Enter search criteria and then choose an existing logical partitioning policy from the resulting list.
- Click **Add New** to add a new logical partitioning policy.

Step 3 Configure the fields on the **Logical Partitioning Policy Configuration** window. For more information on the fields and their configuration options, see the system Online Help.

Note If any policy is left blank without any configuration values, it will become a blank geolocation policy and configuring a Logical Policy for a specific Device Type with the blank Logical Partitioning configurations makes Unified Communications Manager add the policy value (Allow or Deny) in the configured device type.

Step 4 Click **Save**.

Enable Location Conveyance

Location Conveyance is an optional configuration that lets you share geolocation information across clusters.

Procedure

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

Step 2 Do one of the following:

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

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

Step 4 In the **Geolocation Information** area, select a **Geolocation** and **Geolocation Filter**.

Step 5 To enable Location Conveyance, check the **Send Geolocation Information** check box.

Step 6 Click **Save**.

Logical Partitioning Interactions and Restrictions

Logical Partitioning Interactions

Table 93: Logical Partitioning Interactions

Feature	Interaction
Ad Hoc Conference, Join, Join Across Lines, Call Forwarding, Call Transfer	Logical partitioning handling does not take place in the following circumstances: • When all participants are VoIP phones. • When the geolocation or geolocation filter does not associate with a device.
Barge, cBarge, and Remote Resume	Logical partitioning handling does not take place in the following circumstances: • When both the caller and the callee devices are VoIP phones, logical partitioning policy checks are ignored. • For the participants in cBarge/Barge, no logical partitioning policy checking exists, and you cannot prevent logical-partitioning-denied scenarios.
Cisco Unified Mobility	Logical partitioning handling does not take place in the following circumstances: • Geolocation or geolocation filter does not associate with the involved devices. • No logical partitioning support exists when a dual-mode phone is used.
CTI Handling	Logical partitioning handling does not take place in the following circumstances: • When a geolocation or geolocation filter does not associate with any device, handling does not occur. • When all the involved devices specify VoIP phones, handling does not occur.
Extension Mobility	Logical partitioning handling does not take place in the following circumstances: • A geolocation or geolocation filter does not associate with a VoIP phone that is logged on to Cisco Extension Mobility, nor does it associate with the calling party or called party device. • The VoIP phone that is logged on to Cisco Extension Mobility calls or receives a call from a VoIP phone.

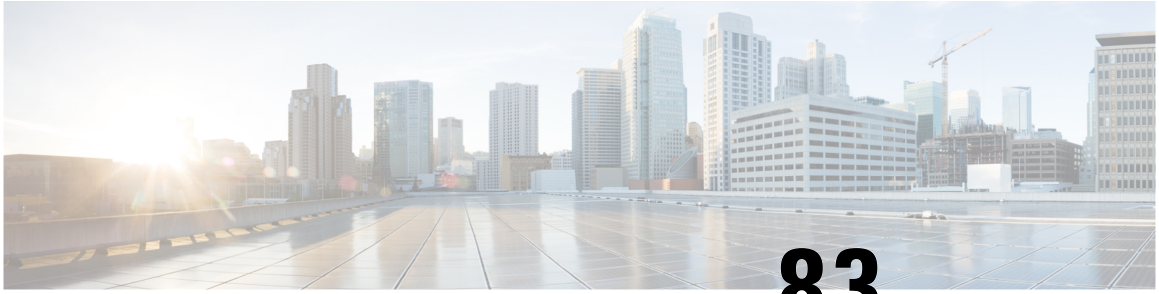
Feature	Interaction
Meet-Me Conference	Logical partitioning handling does not take place in the following circumstances: • When all participants are VoIP phones, handling does not occur. • When geolocation or geolocation filter does not associate with a device, no policy check takes place for that device.
Route Lists and Hunt Pilots	Logical partitioning handling does not take place in the following circumstances: • When both the calling party and called party devices are VoIP phones, handling does not occur. • All devices must associate with both a geolocation and geolocation filter. If any device does not associate with both geolocation and geolocation filter, handling does not occur.
Shared Line	Logical partitioning handling does not take place in the following circumstances: • When both the caller and the callee devices are VoIP phones, no handling occurs. • When geolocation or geolocation filter does not associate with any device, no handling occurs.

Logical Partitioning Restrictions

Table 94: Logical Partitioning Restrictions

Restriction	Description
Barge/cBarge	Barge/cBarge does not occur; the call instance is dropped. For the participants in cBarge/Barge, no logical partitioning policy checking exists, and you cannot prevent logical-partitioning-denied scenarios.
BLF Presence	BLF Presence notifications are not checked for a logical partitioning policy.
Cisco Extension Mobility	When Cisco Extension Mobility logs in to a phone in a different geolocation, outgoing PSTN calls can occur when Local Route Groups are configured. Incoming PSTN calls are not placed to the phone but receive a reorder tone.
Cisco Unified MeetingPlace	The system does not support the logical partitioning feature for calls that involve Cisco Unified MeetingPlace or Cisco Unified MeetingPlace Express.
Conferences	The logical partitioning checks are not supported for participants across conferences in conference chaining. For example, meet-me and adhoc chained conferences can have participants that are logical partitioning denied.

Restriction	Description
H.225 gatekeeper-controlled trunk	Cisco Unified Communications Manager does not communicate geolocation information over a H.225 gatekeeper-controlled trunk.
H.323 and MGCP Gateways	Cisco Unified Communications Manager does not communicate geolocation info to H.323 or MGCP gateways. Communication to a SIP gateway can be disabled through the SIP trunk check box.
Mobility Cell Pickup	Logical partitioning deny handling takes place after call is answered on the mobile phone. The logical partitioning policy check does not occur before the call is placed to the mobile phone (as it happens for a basic SNR call). The system checks the logical partitioning policy after the mobile phone answers the call.
Q.SIG intercluster trunk	Intercluster trunks (ICT) with the Q.SIG protocol are not allowed to communicate geolocation inforomation for the caller or receiving device. The ICT configuration for “Send Geolocation Information” is disabled when the Q.SIG tunneled protocol is selected.
Reorder Tones	No reorder tone (fast busy tone) is provided on IOS H.323 and SIP gateways upon release of connected calls due to logical partitioning policies.
Shared Line Active Call	For a restricted logical partitioning scenario, the shared line drops the active call information for the duration of the call, even if a feature moves the shared-line call to the allowed category.
User Agent Server	The logical partitioning policy checks in the logical partitioning-aware cluster that receives this geolocation may cancel the call if the policy is denied.



CHAPTER 83

Configure Geolocation and Location Conveyance

Geolocation and Location Conveyance Overview

Use Geolocations to define the geographical location (or civic address) of devices that is used in policy decisions, such as whether a call from one phone to another is allowed. The Request for Comments (RFC) 4119 standard provides the basis for geolocations.

Use Location Conveyance to allow communication of geolocation information from one cluster to another, when a call is established and during a call.

Geolocation and Location Conveyance Task Flow

Procedure

	Command or Action	Purpose
Step 1	To Configure Geolocations, on page 642, perform the following subtasks: • Configure a Geolocation, on page 642 • Assign a Geolocation, on page 642 • Set the Default Geolocation, on page 643 • Configure Location Conveyance, on page 644	Configure geolocations to specify geographic locations. These are used to associate devices with regulatory features such as logical partitioning. Geolocations are used in policy decisions, such as in-country regulations.
Step 2	To Configure Geolocation Filters, on page 644, configure the following subtasks: • Configure a Geolocation Filter, on page 645 • Assign a Geolocation Filter, on page 645 • Set the Default Geolocation Filter, on page 646	Configure geolocation filters to choose which fields are used to create a geolocation identifier. This feature is used to make policy decisions on a subset of the geolocation objects. Geolocation filters define which of the geolocation objects should be used when comparing the geolocations of different devices. For example, a group of phones may be

	Command or Action	Purpose
		assigned identical geolocations, except for the room and floor in which they are located. Even though the actual geolocations of each phone differ, the filtered geolocation is the same.

Configure Geolocations

Procedure

	Command or Action	Purpose
Step 1	Configure a Geolocation, on page 642	Configure geolocations to specify geographic locations. These are used to associate devices with regulatory features such as logical partitioning. Geolocations are used in policy decisions, such as in-country regulations.
Step 2	Assign a Geolocation, on page 642	Assign a geolocation to a device or device pool.
Step 3	Set the Default Geolocation, on page 643	Specify a default geolocation for all devices and device pools in this cluster.
Step 4	(Optional) Configure Location Conveyance, on page 644	Configure location conveyance if you want to communicate geolocation information about devices across clusters.

Configure a Geolocation

Configure geolocations to specify geographic locations. These are used to associate devices with regulatory features such as logical partitioning. Geolocations are used in policy decisions, such as in-country regulations.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Geolocation Configuration**.

Step 2 Click **Add New**.

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

Step 4 Configure the fields on the **Geolocation Configuration** window. For more information on the fields and their configuration options, see the system Online Help.

Step 5 Click **Save**.

Step 6 Repeat this procedure to create additional geolocations.

Assign a Geolocation

Assign a geolocation to a device or device pool.

Procedure

Step 1 From Cisco Unified CM Administration, choose one of the following menu items:

- **Device** > **Phone**
- **Device** > **Trunk**
- **Device** > **Gateway**
- **System** > **Device Pool**

Step 2 Perform one of the following tasks:

- Click **Find** to modify the settings for an existing device or device pool. Enter search criteria, and then choose an existing device or device pool from the resulting list.
- Click **Add New** to add a new device or device pool. For devices, choose device types and protocols as needed and click **Next**.

Step 3 From the Geolocation drop-down list, choose a geolocation that you configured.

Step 4 Click **Save**.

Set the Default Geolocation

Specify a default geolocation for all devices and device pools in this cluster.

Before you begin

Assign a Geolocation, on page 642

Procedure

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

Step 2 From the **Default Geolocation** drop-down list, choose a Geolocation that you configured. The default value is **Unspecified**.

Step 3 Click **Save**.

Step 4 Click **Apply Config**.

Step 5 (Optional) If you need to override this default for a specific device or device pool, enter the value on either the **Device Configuration** or **Device Pool Configuration** window, and then click **Save**.

What to do next

- (Optional) Configure Location Conveyance, on page 644
- Configure Geolocation Filters, on page 644

Configure Location Conveyance

Configure location conveyance if you want to communicate geolocation information about devices across clusters.

Before you begin

- Configure a Geolocation, on page 642
- Assign a Geolocation, on page 642
- Set the Default Geolocation, on page 643

Procedure

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

Step 2 Do one of the following:

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

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

Step 4 In the **Geolocation Information** area, select a **Geolocation** and **Geolocation Filter**.

Step 5 To enable Location Conveyance, check the **Send Geolocation Information** check box.

Step 6 Click **Save**.

Configure Geolocation Filters

Configure geolocation filters to choose which fields are used to create a geolocation identifier. This feature is used to make policy decisions on a subset of the geolocation objects. Geolocation filters define which of the geolocation objects should be used when comparing the geolocations of different devices. For example, a group of phones may be assigned identical geolocations, except for the room and floor in which they are located. Even though the actual geolocations of each phone differ, the filtered geolocation is the same.

Procedure

	Command or Action	Purpose
Step 1	Configure a Geolocation Filter, on page 645	Geolocation filters allow you to specify which fields are used to create a geolocation identifier. This feature is used to make policy decisions on a subset of the geolocation objects.
Step 2	Assign a Geolocation Filter, on page 645	
Step 3	Set the Default Geolocation Filter, on page 646	Configure the Default Geolocation Filter enterprise parameter to specify a default geolocation filter for a cluster. This parameter

	Command or Action	Purpose
		determines the default geolocation filter setting for all devices and device pools that are not associated with a geolocation filter.

Configure a Geolocation Filter

Geolocation filters allow you to specify which fields are used to create a geolocation identifier. This feature is used to make policy decisions on a subset of the geolocation objects.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Geolocation Filter**.

Step 2 Click **Add New**.

Step 3 Enter a **Name** and **Description** for the filter.

Step 4 Check the check boxes that correspond to the items you want to use for logical partitioning decisions.

Step 5 Configure the fields on the **Geolocation Filter Configuration** window. For more information on the fields and their configuration options, see the system Online Help.

Step 6 Click **Save**.

Step 7 Repeat these steps to create additional geolocation filters.

Assign a Geolocation Filter

Procedure

Step 1 From Cisco Unified CM Administration, choose one of the following menu items:

- **Device** > **Phone**
- **Device** > **Trunk**
- **Device** > **Gateway**
- **System** > **Device Pool**

Step 2 Perform one of the following tasks:

- Click **Find** to modify the settings for an existing device or device pool. Enter search criteria and then choose an existing device or device pool from the resulting list.
- Click **Add New** to add a new device or device pool. For devices, choose device types and protocols as needed and click **Next**.

Step 3 From the **Geolocation Filter** drop-down list, choose a geolocation filter that you configured.

Step 4 Click **Save**.

Set the Default Geolocation Filter

Configure the Default Geolocation Filter enterprise parameter to specify a default geolocation filter for a cluster. This parameter determines the default geolocation filter setting for all devices and device pools that are not associated with a geolocation filter.

Before you begin

Assign a Geolocation Filter, on page 645

Procedure

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

Step 2 From the **Default Geolocation** drop-down list, choose a Geolocation that you configured. The default value is **Unspecified**.

Step 3 Click **Save**.

Step 4 Click **Apply Config**.

Step 5 (Optional) If you need to override this default for a specific device or device pool, specify the default geolocation filter value on either the **Device Configuration** or **Device Pool Configuration** window, and then click **Save**.

CHAPTER 84

Configure Location Awareness

Location Awareness Overview

Important Meraki Access Points support for Location Awareness is applicable only from Release 12.5(1)SU6 onwards and Release 14SU1 onwards.

Location Awareness allows administrators to determine the physical location from which a phone connects to the company network. For wireless networks, you can view the wireless access point infrastructure, and which mobile devices currently associate to those access points. For wired networks, you can view the Ethernet switch infrastructure and see which devices are currently connected to those switches. This allows you to determine the building, floor, and cube from which a call was placed.

Note Currently, wired phones do not support Location Awareness.

You can view your network infrastructure from **Cisco Unified CM Administration** > **Advanced Features** > **Device Location Tracking Services** > **Switches and Access Points** > **Find and List Switches and Access Points** window.

This feature updates the Unified Communications Manager database dynamically with the following information:

- Network infrastructure devices such as switches and wireless access points, including IP addresses, hostnames, and BSSID info (where applicable) for each infrastructure device.
- Associated endpoints for each infrastructure device, including:
    - For wireless networks, the list of devices that are currently associated to a wireless access point.
    - For wired networks, the list of devices and device types that are currently connected to an ethernet switch.

Cisco Emergency Responder Integration

Location Awareness helps integrated applications such as Cisco Emergency Responder to determine the physical location of a user who places an emergency call. When Location Awareness is enabled, Cisco Emergency Responder learns of a new device to infrastructure association within minutes of a mobile device associating with a new wireless access point, or a desk phone being connected to a new ethernet switch.

When Cisco Emergency Responder first starts up, it queries the Unified Communications Manager Database for the current device to network infrastructure associations. Every two minutes following, the Cisco Emergency Responder checks for updates to the existing associations. As a result, even if a mobile caller places an emergency call while in a roaming situation, Cisco Emergency Responder can quickly determine the physical location of the caller and send emergency services to the appropriate building, floor, or cube.

Wireless Network Updates

To enable Location Awareness for your wireless infrastructure, you can configure Unified Communications Manager to synchronize with a Cisco Wireless LAN Controller. You can synchronize Unified Communications Manager with up to fifty controllers. During the synchronization process, Unified Communications Manager updates its database with the access point infrastructure that the controller manages. In Cisco Unified CM Administration, you can view the status for your wireless access points, including the list of mobile clients that are associated to each access point.

As mobile clients roam between access points, SIP and SCCP signaling from the endpoint communicates the new device to access point association to Unified Communications Manager, which updates its database. Cisco Emergency Responder also learns of the new association by querying the Unified Communications Manager database every few minutes for new endpoints that have changed their association. As a result, if a mobile client places an emergency call, Cisco Emergency Responder has accurate information on the physical location of the user whom placed the call.

If you have a regular synchronization schedule for your Wireless Access Point controllers, Unified Communications Manager adds and updates access points from the database dynamically following each synchronization.

Using Bulk Administration to insert Access Points

If you are using a third-party wireless access point controller, or if you want to export your access points from Cisco Prime Infrastructure, you can use the Bulk Administration Tool to bulk insert your wireless access point infrastructure from a CSV file into the Unified Communications Manager database. Following the bulk insert, the next location update from the mobile device updates the database with the current access point association.

However, Bulk Administration does not allow you to update your access point infrastructure dynamically as new access points get added to your wireless network. If a mobile call gets placed through an access point that was added after the bulk insert, that access point will not have a record in the database, Unified Communications Manager will not be able to match the BSSID of the new access point, and will mark the infrastructure for the wireless device as UNIDENTIFIED AP.

For detailed information on the Bulk Administration Tool, refer to the "Manage Infrastructure Devices" chapter of the *Bulk Administration Guide for Cisco Unified Communications Manager*.

Supported Endpoints for Location Awareness

The following endpoints support tracking via Location Awareness:

- Cisco Uniifed Wireless IP Phone 7925G

- Cisco Unified Wireless IP Phone 7925G-EX
- Cisco Unified Wireless IP Phone 7926G
- Cisco Jabber clients—supported as of 12.5(1)SU1
- Cisco Wireless IP Phone 8821—supported as of 12.5(1)SU1
- Webex App—supported as of 12.5(1)SU1

These endpoints provide upstream infrastructure information, such as BSSID, through Station Info messages to Cisco Unified Communications Manager. Cisco Emergency Responder uses AXL Change Notifications to track these devices through the associated access point.

For device tracking to work, wireless access points must be defined in Cisco Unified Communications Manager. You can do this by syncing a wireless access point controller or using Bulk Administration to import wireless access point infrastructure.

Location Awareness Prerequisites

This feature allows you to synchronize the Cisco Unified Communications Manager database with multiple Cisco Wireless LAN Controllers. You must also set up your Cisco Wireless LAN Controller hardware and your infrastructure of access points. For details, see your controller documentation.

Location Awareness Configuration Task Flow

Complete the following tasks to set up Location Awareness in Cisco Unified Communications Manager.

Before you begin

Procedure

	Command or Action	Purpose
Step 1	Start Services for Wireless Infrastructure Synchronization, on page 650	In Cisco Unified Serviceability, start services that support the Location Awareness feature.
Step 2	Configure Wireless Access Point Controller, on page 650	Synchronize the database with a Cisco wireless access point controller. The sync imports the wireless infrastructure into the database. **Tip** Set up a sync schedule for automatic updates.
Step 3	Insert Infrastructure Devices, on page 651	Optional. If you want to add your wireless infrastructure from Cisco Prime Infrastructure, or if you are using a third-party wireless LAN controller, use Bulk Administration to update the database from a CSV file.

	Command or Action	Purpose
		Note This method does not allow you to set up automatic updates.
Step 4	Deactivate Infrastructure Device from Tracking, on page 652	Optional. If your synchronization includes access points that you do not want to track (for example, if the synchronization pulls in access points from a lab), you can deactivate the access point and Cisco Unified Communications Manager will not track updates to the access point.

Start Services for Wireless Infrastructure Synchronization

Use this procedure to start services that support synchronization with a Cisco Wireless LAN Controller in support of the Location Awareness feature.

Procedure

Step 1 Log in to Cisco Unified Serviceability and choose **Tools** > **Service Activation**.

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

Step 3 Make sure that the following services are checked:

- **Cisco CallManager**
- **Cisco AXL Web Service**
- **Cisco Wireless Controller Synchronization Service**

Step 4 Optional. If you want to use Bulk Administration to import your network infrastructure from a CSV file, make sure that **Bulk Provisioning Service** is checked.

Step 5 Click **Save**.

Configure Wireless Access Point Controller

Use this procedure to synchronize the database with a Cisco wireless access point controller. During the sync, Unified Communications Manager updates its database with the wireless access point infrastructure that the controller manages. You can add up to fifty wireless access point controllers.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Advanced Features** > **Device Location Tracking Services** > **Wireless Access Point Controllers**.

Step 2 Select the controller that you want to configure:

- Click **Find** and select the controller to edit an existing controller.
- Click **Add New** to add a new controller.

Step 3 In the **Name** field, enter the IP address or hostname for the controller.

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

Step 5 Complete the SNMP settings that will be used for SNMP messaging to the controller:

a) From the **SNMP Version** drop-down list, select the SNMP version protocol that the controller uses.
b) Complete the remaining SNMP authentication fields.For more information on the fields and their configuration options, see Online Help.
c) Click the **Test SNMP Settings** to confirm that you entered valid SNMP settings.

Step 6 If you want to configure scheduled syncs to regularly update the database:

a) Check the **Enable scheduled synchronization to discover Infrastructure Devices** check box.
b) In the **Perform a Re-sync Every** fields, create the synchronization schedule.

Step 7 Click **Save**.

Step 8 (Optional) To update the database immediately, click **Synchronize**.

Optional. If the synchronization pulls in access points that you do not want to track (for example, lab equipment or access points that are not in use) you can remove the access point from tracking.

Insert Infrastructure Devices

Use this procedure to complete a bulk import of your wireless Access Point infrastructure from a CSV file into the Unified Communications Manager database. You can use this procedure to import a CSV file that was exported from Cisco Prime Infrastructure or if you want to import access points from a third-party wireless Access Point controller.

Before you begin

You must have a data file in comma separated value (CSV) format with the following delineated columns:

- AccessPoint or Switch Name
- IPv4 Address
- IPv6 Address
- BSSID—Required for Wireless Access Protocol (WAP) infrastructure devices
- Description—A location identifier, a combination of switch type and location, or another meaningful identifier

Note You can define both an IPv4 and IPv6 address, or you can define an IPv4 or an IPv6 address.

Note For the BSSID value, enter the BSSID mask, ending in 0, that uniquely identifies the access point as opposed to the BSSIDs for the individual channels on the access point.

Procedure

Step 1 Choose **Bulk Administration** > **Infrastructure Device** > **Insert Infrastructure Device**.
The **Insert Infrastructure Device Configuration** window displays.

Step 2 In the **File Name** field, choose the CSV data file that you created for this transaction.

Step 3 In the **Job Information** area, enter the Job description.

The default description is **Insert Infrastructure Device**.

Step 4 Select when you want to run the job:

- Select the **Run Immediately** radio button, if you want to run the job immediately.
- Select the **Run Later** radio button, if you want to schedule the job for later.

Step 5 Click **Submit**.
If you chose to run the job immediately, the job runs.

Step 6 If you chose to run the job later, schedule when the job runs:

a) Choose **Bulk Administration** > **Job Scheduler**.
b) Click **Find** and select the job that you just created.
c) In the **Job Scheduler** window, schedule when you want to run the job.
d) Click **Save**.
At the scheduled time, the job runs.

Deactivate Infrastructure Device from Tracking

If the synchronization includes access points or switches that you do not want to track (for example, if the sync pulls in lab equipment or access points that are not in use), you can deactivate the access point or switch from tracking. Unified Communications Manager will not update the status for the access point or switch.

Procedure

Step 1 In Cisco Unified CM Administration, choose **Advanced Features** > **Device Location Tracking Services** > **Switches and Access Points**.

Step 2 Click **Find** and select the switch or access point that you want to stop tracking.

Step 3 Click **Deactivate Selected**.

Related Documentation

After you complete your system configuration, and your system is up and running, you can use tasks in the following chapter to manage your infrastructure on an ongoing basis:

"Manage Infrastructure", Administration Guide for Cisco Unified Communications Manager and IM and Presence Service

Location Awareness Restrictions

Feature	Interactions and Restrictions
Meraki Access Points	The Location Awareness feature does not support Meraki access points.

CHAPTER 85

Configure Automated Alternate Routing

Automated Alternate Routing Overview

Configure automated alternate routing (AAR) to automatically reroute calls through the PSTN or other networks when the system 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.

AAR Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Enable Clusterwide Automated Alternate Routing, on page 655	Enable automated alternate routing for the cluster.
Step 2	Configure AAR Group, on page 656	Configure automated alternate routing (AAR) 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.

Enable Clusterwide Automated Alternate Routing

Enable Automated Alternate Routing (AAR) for the cluster.

Procedure

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

Step 2 Select a node in the **Server** drop-down box.

Step 3 From the **Service** drop-down list, select Cisco Call Manager.

Step 4 In the Clusterwide Parameters (System - CCM Automated Alternate Routing) area, set the **Automated Alternate Routing Enable** parameter to **True**.

Configure AAR Group

Configure Automated Alternate Routing (AAR) to automatically reroute calls through the PSTN or other networks when the system blocks a call due to insufficient location bandwidth. With AAR, the caller does not need to hang up and redial the called party.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **AAR Group**.

Step 2 Choose one of the following options:

- Click **Add New**, to add a new AAR group.
- Click **Find** and choose an AAR group from the resulting list, to modify the settings for an existing AAR group.

The **AAR Group Configuration** window appears.

Step 3 In the **Name** field, 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 (_).

The window refreshes and displays additional fields.

Step 4 Configure the fields on the **AAR Group Configuration** window. For more information on the fields and their configuration options, see the system Online Help.

Step 5 Click **Save**.

Note **Optional**. To enable AAR to work with hunt pilots, see Hunt Pilot Configuration Task Flow, on page 151.

CHAPTER 86

Configure AS-SIP Endpoints

AS-SIP Overview

Assured Services SIP (AS-SIP) endpoints are compliant with MLPP, DSCP, TLS/SRTP, and IPv6 requirements. AS-SIP provides for multiple endpoint interfaces on the Unified Communications Manager.

Many Cisco IP phones support AS-SIP. In addition, the Third-Party AS-SIP Endpoint device type allows a third-party AS-SIP compliant endpoint to be configured and used with Cisco Unified Communications Manager. In addition, the Third-Party AS-SIP Endpoint device type allows a third-party AS-SIP-compliant generic endpoint to be configured and used with Cisco Unified Communications Manager

AS-SIP Capabilities

The following capabilities are implemented or made available for AS-SIP endpoints:

- MLPP
- TLS
- SRTP
- DSCP for precedence levels
- Error responses
- V.150.1 MER
- Conference Factory flow support
- AS-SIP Line Early Offer

Third-Party AS-SIP Phones

Third-party phones can be provisioned in Cisoc Unified Communications Manager using the Third-Party AS-SIP Endpoint device type.

Third-party phones that are running AS-SIP do not get configured through the Cisco Unified Communications Manager TFTP server. The customer must configure 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). Also, if the directory number of a line is changed, the customer must ensure that it gets changed in both Cisco Unified CM Administration and in the native phone configuration mechanism.

Identification of Third-Party Phones

The 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 a user that is configured in the **End User Configuration** window of Cisco Unified CM Administration. The administrator configures the SIP third-party phone with the user; for example, **`swhite`**, in the **Digest User** field of **Phone Configuration** window.

Note You can assign each user ID to only one third-party phone. If the same user ID is assigned as the Digest User for multiple phones, the third-party phones to which they are assigned will not successfully register.

Configuration of Third Party AS-SIP Phones and Cisco IP Phones

The following table provides a comparison overview of the configuration differences between Cisco Unified IP Phones and third-party phones that are running AS-SIP.

Table 95: Comparison of the Configuration Differences Between Cisco IP Phones and Third-Party Phones

Phone Running AS-SIP	Integrated with Centralized TFTP	Sends MAC Address	Downloads Softkey File	Downloads Dial Plan File	Supports Unified Communications Manager Failover and Fallback	Supports Reset and Restart
Cisco IP Phone	Yes	Yes	Yes	Yes	Yes	Yes
Third-party AS-SIP device	No	No	No	No	No	No

Note Not all Cisco IP Phones support AS-SIP. See the phone administration guide for your phone model for support information

Use Cisco Unified CM Administration to configure third-party phones that are running SIP (see the Configure SIP Profile, on page 348). The administrator must perform configuration steps on the third-party phone that is running SIP; see the following examples:

- Ensure that proxy address in the phone is the IP or Fully Qualified Domain Name (FQDN) of Cisco Unified Communications Manager.
- Ensure directory numbers in the phone match the directory numbers that are configured for the device in Cisco Unified CM Administration.
- Ensure digest user ID (sometimes referred to as Authorization ID) in the phone matches the Digest User ID in the Cisco Unified CM Administration.

For more information, refer to the documentation that came with the third-party phone.

AS-SIP Conferencing

MOH is applied to its target (a held party, transferee just before transfer, or conferee just before joining the conference), if the feature invoker (holder, transferor, or conference initiator) supports Cisco-proprietary feature signaling. If the feature invoker does not support Cisco-proprietary feature signaling, then MOH is not applied to its target. Also, if an endpoint explicitly signals that it is a conference mixer, then MOH will not be played to the target. There are two forms of AS-SIP Conferencing:

- Local mixing
- Conference Factory

Local mixing

To the Unified CM, the conference initiator simply appears to have established simultaneously active calls, one to each of the other conference attendees. The initiator host the conference locally and the voices are mixed there. The calls from the conference initiator have special signaling that prevent it from being connected to an MOH source.

Conference Factory

The conference initiator calls a Conference Factory Server located off a SIP trunk. Through IVR signaling, the conference initiator instructs the Conference Factory to reserve a conference bridge. The Conference Factory gives the numeric address (a routable DN) to the conference initiator, who then establishes a subscription with the bridge to receive conference list information to track the participants. The Conference Factory sends special signaling that prevent it from being connected to an MOH Source.

AS-SIP Prerequisites

Determine whether sufficient Device License Units are available. For details, see Smart Software Licensing, on page 7

AS-SIP Enpdoint Configuration Task Flow

Complete the following tasks to configure an AS-SIP endpoint.

Procedure

	Command or Action	Purpose
Step 1	Configure a Digest User, on page 660	Configure the end user to use digest authentication for SIP requests.
Step 2	Configure SIP Phone Secure Port, on page 348	Cisco Unified Communications Manager uses this port to listen to SIP phones for SIP line registrations over TLS.
Step 3	Restart Services, on page 348	After configuring the secure port, restart the Cisco CallManager and Cisco CTL Provider services.
Step 4	Configure SIP Profile for AS-SIP, on page 662	Configure a SIP profile with SIP settings for your AS-SIP endpoints and for your SIP trunks. **Note** The phone-specific parameters are not downloaded to a third-party AS-SIP phone. They are used only by Cisco Unified Communications Manager. Third-party phones must locally configure the same settings.
Step 5	Configure Phone Security Profile for AS-SIP, on page 662	You can use the phone security profile to assign security settings such as TLS, SRTP, and digest authentication
Step 6	Configure AS-SIP Endpoint, on page 663	Configure a Cisco IP Phone or a third-party endpoint with AS-SIP support.
Step 7	Associate Device with End User, on page 664	Associate the endpoint with a user.
Step 8	Configure SIP Trunk Security Profile for AS-SIP, on page 664	You can use the sip trunk security profile to assign security features such as TLS or digest authentication to a SIP trunk.
Step 9	Configure SIP Trunk for AS-SIP, on page 665	Configure a SIP trunk with AS-SIP support.
Step 10	Configure AS-SIP Features, on page 666	Configure additional AS-SIP features such as MLPP, TLS, V.150 and IPv6.

Configure a Digest User

Use this procedure to configure an end user as a digest user whom uses digest authentication. Devices that are associated to the user will be authenticated via the user's digest credentials.

Procedure

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

Step 2 Do either of the following:

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

Step 3 Make sure the following mandatory fields are completed:

- User ID
- Last Name

Step 4 In the **Digest Credentials** field, enter a password. End users must authenticate themselves via this password when using the endpoint.

Step 5 Complete any remaining fields. For help with the fields and their settings, see the online help.

Step 6 Click **Save**.

Configure SIP Phone Secure Port

Follow these steps to configure the SIP Phone Secure Port. Cisco Unified Communications Manager uses this port to listen to SIP phones for SIP line registrations over TLS.

Procedure

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

Step 2 In the **Cisco Unified Communications Manager TCP Port Settings for this Server** section, specify a port number in the **SIP Phone Secure Port** field, or leave the field set to default. The default value is 5061.

Step 3 Click **Save**.

Step 4 Click **Apply Config**.

Step 5 Click **Ok**.

Restart Services

Follow these steps to restart Cisco CallManager and Cisco CTL Provider services.

Procedure

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

Step 2 Choose the Cisco Unified Communications Manager server from the **Servers** drop-down list.
In the CM Services area, Cisco CallManager displays in the **Service Name** column.

Step 3 Click the radio button that corresponds to the Cisco CallManager service.

Step 4 Click **Restart**.
The service restarts and displays the message, `Service Successfully Restarted`.

Step 5 Repeat step 3 and step 4 to restart Cisco CTL Provider service.

Configure SIP Profile for AS-SIP

Use this procedure to configure SIP profile with SIP settings for your AS-SIP endpoints and for your SIP trunks.

Procedure

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

Step 2 Do either of the following:

- Click **Add New** to create a new SIP Profile.
- Click **Find** and select an existing SIP Profile.

Step 3 Enter a **Name** and **Description** for the SIP Profile.

Step 4 Check the **Assured Services SIP conformance** check box.

Note This checkbox must be checked for SIP trunks and for third-party AS-SIP phones. It's not mandatory for Cisco IP Phones that support AS-SIP.

Step 5 In the **Parameters used in Phone** section, configure DSCP precedence values for the types of calls that you expect to make.

Note You can also configure DSCP values via clusterwide service parameters. However, the DSCP values within a SIP Profile override the clusterwide settings for all devices that use the SIP Profile.

Step 6 From the **Early Offer support for voice and video calls** drop-down list, select one of the following options to configure Early Offer support for SIP trunks that use this profile:

- Disabled
- Best Effort (no MTP Inserted)
- Mandatory (insert MTP if needed)

Step 7 Complete the remaining fields in the **SIP Profile Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 8 Click **Save**.

Configure Phone Security Profile for AS-SIP

Use this procedure to configure a phone security profile for AS-SIP endpoints. You can use the security profile to assign security settings such as TLS and SRTP.

Procedure

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

Step 2 Perform one of the following steps:

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

Step 3 For new profiles, select an option from the **Phone Security Profile** drop-down, choose the phon emodel**Third-party AS-SIP Endpoint** and click **Next**.

- For Cisco IP phones, select the phone model and click **Next**.
- For third-party AS-SIP endpoints, select **Third-party AS-SIP Endpoint** and click **Next**.

Step 4 For the protocol, select **SIP** and click **Next**.

Step 5 Enter a **Name** and **Description** for the protocol.

Step 6 Assign the **Device Security Mode**, to one of the following settings:

- **Authenticated**—Cisco Unified Communications Manager uses TLS signaling, providing integrity and authentication for the phone.
- **Encrypted**—Cisco Unified Communications Manager uses TLS signaling, providing integrity and authentication for the phone. In addition, SRTP encrypts the media streams.

Step 7 Check the **Enable Digest Authentication** check box.

Step 8 Configure the remaining fields in the **Phone Security Profile Configuration** window. For help with the fields and their settings, see the online help.

Step 9 Click **Save**.

Configure AS-SIP Endpoint

Use this procedure to configure an AS-SIP endpoint. Many Cisco IP Phones support AS-SIP. In addition, you can configure AS-SIP for third-party endpoints.

Procedure

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

Step 2 Click **Add New**.

Step 3 From the Phone Type drop-down list, select a Cisco IP Phone that supports AS-SIP. Otherwise, select **Third-Party AS-SIP Endpoint**.

Step 4 Click **Next**.

Step 5 Configure the following mandatory fields.For more information on the fields and their configuration options, see Online Help.

- Device Trust Mode—For third-party AS-SIP endpoints only. Select **Trusted** or **Not Trusted**.
- MAC Address
- Device Pool

- Phone Button Template
- Owner User ID
- Device Security Profile—Select the phone security profile that you set up for AS-SIP.
- SIP Profile—Select the AS-SIP-enabled SIP Profile that you configured.
- Digest User—Select the user ID that you configure as a digest user. The user must be enabled for digest authentication
- Require DTMF Reception—Check this check box to allow the endpoint to accept DTMF digits.
- Early Offer support for voice and video calls—Check this check box to enable early offer support. This field appears for third-party phones only.

Step 6 Configure the fields in the **MLPP and Confidential Access Level Information** section.

Step 7 Click **Save**.

Step 8 Add a Directory Number:

a) In the left navigation bar, click **Add a new DN**. The **Directory Number Configuration** window opens.
b) Add a **Directory Number**.
c) Complete any remaining fields in the **Directory Number Configuration** window
d) Click **Save**.

Step 9 From **Related Links**, select **Configure Device** and click **Go**.

Step 10 Click **Apply Config**.

Associate Device with End User

Use this procedure to associate an end user to the AS-SIP endpoint.

Procedure

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

Step 2 Click **Find** and select the user whom you want to associate to the device.

Step 3 In the **Device Information** section, click **Device Association**.
The User Device Association window appears.

Step 4 Click **Find** to view a list of available devices.

Step 5 Select the device that you want to associate, and click **Save Selected/Changes**.

Step 6 From **Related Links**, choose **Back to User**, and click **Go**.
The **End User Configuration** window appears, and the associated device that you chose appears in the **Controlled Devices** pane.

Configure SIP Trunk Security Profile for AS-SIP

Use this procedure to configure a security profile for a SIP trunk that supports AS-SIP

Procedure

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

Step 2 Click **Add New**.

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

Step 4 From the **Device Security Mode** drop-down list, choose **Authenticated** or **Encrypted**.

Step 5 The **Incoming Transport Type** and **Outgoing Transport Type** fields change to **TLS** automatically.

Step 6 Check the **Enable Digest Authentication** check box.

Step 7 If you are deploying V.150, configure a value for the **SIP V.150 Outbound SDP Offer Filtering** drop-down list.

Step 8 Complete the remaining fields in the **SIP Trunk Security Profile Configuration** window.For more information on the fields and their configuration options, see Online Help.

Step 9 Click **Save**.

Configure SIP Trunk for AS-SIP

Use this procedure to set up a SIP trunk that supports AS-SIP.

Procedure

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

Step 2 Do either of the following:

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

Step 3 For new trunks, from the **Trunk Type** drop-down list, select **SIP Trunk**.

Step 4 From the **Trunk Service Type** drop-down list, select **None (Default)** and click **Next**.

Step 5 Enter a **Device Name** for the trunk.

Step 6 From the **Device Pool** drop-down list, select a device pool.

Step 7 In the **Destination Address** field, enter the address of the server to which you are connecting the trunk.

Step 8 From the **SIP Trunk Security Profile** drop-down list, select the profile that you created for AS-SIP.

Step 9 From the **SIP Profile** drop-down list, select the SIP Profile that you set up for AS-SIP.

Step 10 Complete any remaining fields in the **Trunk Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 11 Click **Save**.

Configure AS-SIP Features

The procedures in the preceding task flow describe how to configure AS-SIP support on endpoints and trunk. The following table outlines the AS-SIP features that you can deploy and provides configuration reference for each.

AS-SIP Feature	Configuration Description
Early Offer	SIP Early Offer allows your endpoints to negotiate media during the INVITE request and the 200OK response. There are two modes for Early Offer: • Best Effort Early Offer (no MTP Inserted) • Mandatory Early Offer (insert MTP if needed) Configure Early Offer support via the fields in the following configuration windows. Refer to the online help for detailed field descriptions: **SIP Profile Configuration** window • Early Offer support for voice and video calls—Configure this field to enable Early Offer support on a SIP trunk • SDP Session-level Bandwidth Modifier for Early Offer and Re-invite • Send send-receive SDP in mid-call INVITE **Phone Configuration** window (only if the Third Pary AS-SIP Endpoint device type is used) • Early Offer support for voice and video calls - check this check box to enable early offer support
Conference Factory	Specify the URI that an IMS client uses to set up a conference: **1.** From Cisco Unified CM Administration, choose **System** > **Service Parameters**. **2.** From the **Server** drop-down select your Cisco Unified Communications Manager server. **3.** From the **Service**, select **Cisco CallManager**. **4.** Under **Clusterwide Paramters (Feature - Conference)** assign an **IMS Conference Factory URI**. **5.** Click **Save**.

AS-SIP Feature	Configuration Description
DSCP Markings	DSCP settings allow you to manage QoS and bandwidth within your network. DSCP settings are used to assign a prioritized Traffic Class Label to calls on a per-call basis. You can configure clusterwide DSCP settings via service parameters and you can use the SIP Profile to assign a customized QoS policy for users whom use that profile. For example, you could assign higher priority for the calls of an executive (for example, a CEO) or a sales team to ensure that their calls are not dropped if network bandwidth issues arise. To configure DSCP, see DSCP Settings Configuration Task Flow, on page 515.
IPv6	By default, Cisco Unified Communications Manager is configured to use IPv4 addressing. However, you can configure the system to support the IPv6 stack thereby allowing you to deploy a SIP network with IPv6-only endpoints. To configure IPv6, see IPv6 Configuration Task Flow, on page 92
Multilevel Precedence and Preemption (MLPP)	The Multilevel Precedence and Preemption (MLPP) service allows placement of priority calls. This capability assures high-ranking personnel of communication to critical organizations and personnel during network stress situations, such as a national emergency or degraded network situations. To configure MLPP, see Multilevel Precendence and Preemption Task Flow, on page 669.
Secure Real-Time Transport Protocol (SRTP)	The Secure Real-time Transport Protocol (SRTP) can be used to provide encryption and authentication to media streams in your calls. SRTP can be configured for phones within the **Phone Security Profile Configuration** that the phone uses. You must set the **Device Security Mode** field to **Encrypted**.
Transport Layer Signalling (TLS)	Transport Layer Security (TLS) provides secure and reliable signaling and data transfer between two systems or devices, by using secure ports and certificate exchange. To configure TLS, see the "TLS Setup" chapter in the *Security Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

AS-SIP Feature	Configuration Description
V.150	The V.150 Minimum Essential Requirements feature allows you to make secure calls in a modem over IP network. The feature uses a dialup modem for large installed bases of modems and telephony devices operating on a traditional public switched telephone network (PSTN). To configure V.150, see the "Cisco V.150 Minimum Essential Requirements (MER)" chapter in the *Security Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

CHAPTER 87

Configure Multilevel Precedence and Preemption

Multilevel Precedence and Preemption Overview

The Multilevel Precedence and Preemption (MLPP) service allows placement of priority calls. Properly validated users can preempt lower priority phone calls with higher priority calls. An authenticated user can preempt calls either to targeted stations or through fully subscribed TDM trunks. This capability assures high-ranking personnel of communication to critical organizations and personnel during network stress situations, such as a national emergency or degraded network situations.

Multilevel Precedence and Preemption Prerequisites

Supported SCCP or SIP phones. See the *Cisco IP Phone Administration Guide* and *Cisco IP Phone User Guide* for your phones for feature support and more information.

Multilevel Precendence and Preemption Task Flow

Before you begin

Procedure

	Command or Action	Purpose
Step 1	To Configure Domains and Domain Lists, on page 671, perform the following subtasks: • Configure a Multilevel Precedence and Preemption Domain, on page 672 • Configure a Resource Priority Namespace Network Domain, on page 672	Configure an MLPP domain to specify the devices and resources that are associated with an MLPP subscriber.

	Command or Action	Purpose
	• Configure a Resource Priority Namespace Network Domain List, on page 673	
Step 2	Configure a Common Device Configuration for Multilevel Precedence and Preemption, on page 673	A common device configuration includes MLPP-related information that can be applied to multiple users and their devices. Ensure that each device is associated with a common device configuration. These settings override the enterprise parameter settings.
Step 3	Configure the Enterprise Parameters for Multilevel Precedence and Preemption, on page 674	Set enterprise parameters to enable MLPP indication and preemption. If individual devices and devices in common device configurations have MLPP settings of Default, the MLLP-related enterprise parameters apply to these devices and common device configurations.
Step 4	Configure a Partition for Multilevel Precedence and Preemption, on page 675	Configure a partition to create a logical grouping of directory numbers (DNs) and route patterns with similar reachability characteristics. Devices that are typically placed in partitions include DNs and route patterns. These entities associate with DNs that users dial. For simplicity, partition names usually reflect their characteristics.
Step 5	Configure a Calling Search Space for Multilevel Precedence and Preemption, on page 676	A calling search space is an ordered list of partitions. Calling search spaces determine the partitions that calling devices, including IP phones, softphones, and gateways, can search when attempting to complete a call.
Step 6	Configure a Route Pattern for Multilevel Precedence and Preemption, on page 677	Configure route patterns to route or block both internal and external calls.
Step 7	Configure a Translation Pattern for Multilevel Precedence and Preemption, on page 678	Configure translation patterns to specify how to route a call after it is placed. Configuring translation patterns allows your system to manipulate calling and called digits as needed. When the system identifies that a pattern match occurred, your system uses the calling search space that is configured for the translation pattern to perform the subsequent match.
Step 8	Configure Multilevel Precedence and Preemption for Gateways, on page 679	Configure Cisco Unified Communications Manager to communicate with non-IP telecommunications devices.
Step 9	Configure Multilevel Precedence and Preemption for Phones, on page 680	

	Command or Action	Purpose
Step 10	Configure a Directory Number to Place Multilevel Precedence and Preemption Calls, on page 682	After you configure a device, you can add a line (directory number) from the updated **Device Configuration** window.
Step 11	Configure a User Device Profile for Multilevel Precedence and Preemption, on page 682	When a user profile is assigned to a phone, the phone inherits the configuration of the assigned user, including any CSS that is associated with the user. The phone CSS can, however, override the user profile. Cisco Unified Communications Manager assigns the precedence level that is associated with the dialed pattern to the call when a pattern match occurs. The system sets the call request as a precedence call with the assigned precedence level.
Step 12	Configure the Default Device Profile for Multilevel Precedence and Preemption, on page 683	Use the default device profile for whenever a user logs on to a phone model for which no user device profile exists. A default device profile comprises the set of services and features that are associated with a particular device.

Configure Domains and Domain Lists

Configure an MLPP domain to specify the devices and resources that are associated with an MLPP subscriber.

Procedure

	Command or Action	Purpose
Step 1	Configure a Multilevel Precedence and Preemption Domain, on page 672	Associate devices and resources 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, the MLPP service can preempt the existing call that the called MLPP subscriber is on for a higher precedence call. MLPP service availability does not span across different domains. The MLPP domain subscription of the originating user determines the domain of the call and its connections. Only higher precedence calls in one domain can preempt connections that calls in the same domain are using.
Step 2	Configure a Resource Priority Namespace Network Domain, on page 672	Configure namespace domains for a Voice over Secured IP (VoSIP) network that uses SIP trunks. Your system prioritizes the SIP-signaled

	Command or Action	Purpose
		resources so that those resources can be used most effectively during emergencies and congestion of telephone circuits, IP bandwidth, and gateways. Endpoints receive the precedence and preemption information.
Step 3	Configure a Resource Priority Namespace Network Domain List, on page 673	Configure a list of acceptable network domains. Incoming calls are compared to the list and processed, if an acceptable network domain is in the list.

Configure a Multilevel Precedence and Preemption Domain

Associate devices and resources 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, the MLPP service can preempt the existing call that the called MLPP subscriber is on for a higher precedence call. MLPP service availability does not span across different domains.

The MLPP domain subscription of the originating user determines the domain of the call and its connections. Only higher precedence calls in one domain can preempt connections that calls in the same domain are using.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **MLPP** > **Domain** > **MLPP Domain**.

Step 2 Click **Add New**.

Step 3 In the **Domain Name** field, enter the name that you want to assign to the new MLPP domain.

You can enter up to 50 alphanumeric characters, and any combination of spaces, periods (.), hyphens (-), and underscore characters (_).

Step 4 In the **Domain ID** field, enter a unique six-character hexadecimal MLPP domain ID.

Domain IDs must fall in the range between 000001 and FFFFFF. (000000 is reserved for the default MLPP domain ID.)

Step 5 Click **Save**.

Configure a Resource Priority Namespace Network Domain

Configure namespace domains for a Voice over Secured IP (VoSIP) network that uses SIP trunks. Your system prioritizes the SIP-signaled resources so that those resources can be used most effectively during emergencies and congestion of telephone circuits, IP bandwidth, and gateways. Endpoints receive the precedence and preemption information.

Procedure

Step 1 From Cisco Unified CM Administration, **System** > **MLPP** > **Namespace** > **Resource Priority Namespace Network Domain**.

Step 2 Enter the name for the Resource Priority Namespace Network Domain in the information section. The maximum number of domain names is 100.

Step 3 Enter a description for the domain name.

The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), or angle brackets (<>).

Step 4 Check the **Make this the Default Resource Priority Namespace Network Domain** check box if you want the domain name to be the default.

Step 5 Click **Save**.

Configure a Resource Priority Namespace Network Domain List

Configure a list of acceptable network domains. Incoming calls are compared to the list and processed, if an acceptable network domain is in the list.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **MLPP** > **Namespace** > **Resource Priority Namespace List**.

Step 2 Enter the name for the Resource Priority Namespace List. The maximum number of characters is 50.

Step 3 Enter a description for the list. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).

Step 4 Use the Up and Down Arrows to move a Resource Priority Namespace Network Domain to the **Selected Resource Priority Namespaces** field.

Step 5 Click **Save**.

Configure a Common Device Configuration for Multilevel Precedence and Preemption

A common device configuration includes MLPP-related information that can be applied to multiple users and their devices. Ensure that each device is associated with a common device configuration. These settings override the enterprise parameter settings.

Procedure

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

Step 2 Perform one of the following tasks:

- Click **Find** to modify an existing common device configuration and choose a common device configuration from the resulting list.
- Click **Add New** to add a new common device configuration.

Step 3 Configure the fields on the **Common Device Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 4 Click **Save**.

Configure the Enterprise Parameters for Multilevel Precedence and Preemption

Set enterprise parameters to enable MLPP indication and preemption. If individual devices and devices in common device configurations have MLPP settings of Default, the MLLP-related enterprise parameters apply to these devices and common device configurations.

Procedure

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

Step 2 Configure the MLPP enterprise parameters on the **Enterprise Parameters Configuration** window. See the Related Topics section for more information about the parameters and their configuration options.

Step 3 Click **Save**.

Enterprise Parameters for Multilevel Precedence and Preemption

Table 96: Enterprise Parameters for Multilevel Precedence and Preemption

Parameter	Description
MLPP Domain Identifier	Set this parameter to define a domain. Because MLPP service applies to a domain, Cisco Unified Communications Manager marks only connections and resources that belong to calls from MLPP users in a given domain with a precedence level. Cisco Unified Communications Manager can preempt only lower precedence calls from MLPP users in the same domain. The default is **000000**.
MLPP Indication Status	This parameter specifies whether devices use MLPP tones and special displays to indicate MLPP precedence calls. To enable MLPP indication across the enterprise, set this parameter to MLPP Indication turned on. The default is **MLPP Indication turned off**.
MLPP Preemption Setting	This parameter determines whether devices should apply preemption and preemption signaling (such as preemption tones) to accommodate higher precedence calls. To enable MLPP preemption across the enterprise, set this parameter to Forceful Preemption. The default is **No preemption allowed**.

Parameter	Description
Precedence Alternate Party Timeout	In a precedence call, if the called party subscribes to alternate party diversion, this timer indicates the seconds after which Cisco Unified Communications Manager will divert the call to the alternate party if the called party does not acknowledge preemption or does not answer a precedence call. The default is **30** seconds.
Use Standard VM Handling For Precedence Calls	This parameter determines whether a precedence call will forward to the voice-messaging system. If the parameter is set to False, precedence calls do not forward to the voice-messaging system. If the parameter is set to True, precedence calls forward to the voice-messaging system. For MLPP, the recommended setting for this parameter is False, as users, not the voice-messaging system, should always answer precedence calls. The default is **False**.

Configure a Partition for Multilevel Precedence and Preemption

Configure a partition to create a logical grouping of directory numbers (DNs) and route patterns with similar reachability characteristics. Devices that are typically placed in partitions include DNs and route patterns. These entities associate with DNs that users dial. For simplicity, partition names usually reflect their characteristics.

Procedure

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

Step 2 Click **Add New** to create a new partition.

Step 3 In the **Partition Name, Description** field, enter a name for the partition that is unique to the route plan.

Partition names can contain alphanumeric characters, as well as spaces, hyphens (-), and underscore characters (_). See the online help for guidelines about partition names.

Step 4 Enter a comma (,) after the partition name and enter a description of the partition on the same line.

The description can contain up to 50 characters in any language, but it cannot include double quotes ("), percentage sign (%), ampersand (&), backslash (\), angle brackets (<>), or square brackets ([ ]).

If you do not enter a description, Cisco Unified Communications Manager automatically enters the partition name in this field.

Step 5 To create multiple partitions, use one line for each partition entry.

Step 6 From the **Time Schedule** drop-down list, choose a time schedule to associate with this partition.

The time schedule specifies when the partition is available to receive incoming calls. If you choose **None**, the partition remains active at all times.

Step 7 Select one of the following radio buttons to configure the **Time Zone**:

- **Originating Device**—When you select this radio button, the system compares the time zone of the calling device to the **Time Schedule** to determine whether the partition is available is available to receive an incoming call.
- **Specific Time Zone**—After you select this radio button, choose a time zone from the drop-down list. The system compares the chosen time zone to the **Time Schedule** to determine whether the partition is available is available to receive an incoming call.

Step 8 Click **Save**.

Partition Naming Guidelines

The list of partitions in a calling search space is limited to a maximum of 1024 characters. This means that the maximum number of partitions in a CSS varies depending on the length of the partition names. Use the following table to determine the maximum number of partitions that you can add to a calling search space if partition names are of fixed length.

Table 97: Partition Name Guidelines

Partition Name Length	Maximum Number of Partitions
2 characters	340
3 characters	256
4 characters	204
5 characters	172
...	...
10 characters	92
15 characters	64

Configure a Calling Search Space for Multilevel Precedence and Preemption

A calling search space is an ordered list of partitions. Calling search spaces determine the partitions that calling devices, including IP phones, softphones, and gateways, can search when attempting to complete a call.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **Calling Search Space**.

Step 2 Click **Add New**.

Step 3 In the **Name** field, enter a name.

Ensure that each calling search space name is unique to the system. The name can include up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_).

Step 4 In the **Description** field, enter a description.

The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).

Step 5 From the **Available Partitions** drop-down list, perform one of the following steps:

- For a single partition, select that partition.
- For multiple partitions, hold down the **Control (CTRL)** key, then select the appropriate partitions.

Step 6 Select the down arrow between the boxes to move the partitions to the **Selected Partitions** field.

Step 7 (Optional) Change the priority of selected partitions by using the arrow keys to the right of the **Selected Partitions** box.

Step 8 Click **Save**.

Configure a Route Pattern for Multilevel Precedence and Preemption

Configure route patterns to route or block both internal and external calls.

Procedure

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

Step 2 Perform one of the following tasks:

- To modify the settings for an existing route pattern, enter search criteria, click **Find**, and then choose an existing route pattern from the resulting list.
- To add a new route pattern, click **Add New**.

Step 3 Configure the fields on the **Route Pattern Configuration** window. See the Related Topics section for more information about the fields and their configuration options.

Step 4 Click **Save**.

Route Pattern Configuration Fields for Multilevel Precedence and Preemption

Table 98: Route Pattern Configuration Fields for Multilevel Precedence and Preemption

Field	Description
Route Pattern	Enter the route pattern, including numbers and wildcards, without 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 +.

Field	Description
MLPP Precedence	Choose an MLPP precedence setting for this route pattern from the drop-down list: • Executive Override—Highest precedence setting for MLPP calls. • Flash Override—Second highest precedence setting for MLPP calls. • Flash—Third highest precedence setting for MLPP calls. • Immediate—Fourth highest precedence setting for MLPP calls. • Priority—Fifth highest precedence setting for MLPP calls. • Routine—Lowest precedence setting for MLPP calls. • Default-—Does not override the incoming precedence level but rather lets it pass unchanged.
Apply Call Blocking Percentage	Check this check box to enable the Destination Code Control (DCC) feature. By enabling DCC, all calls other than flash and higher precedence calls made to the destination are filtered and allowed or disallowed based on the Call Blocking Percentage quota set for the destination. Flash and higher precedence calls are allowed at all times. DCC is disabled by default. The Apply Call Blocking Percentage field is enabled only if the MLPP level is immediate, priority, routine or default.
Call Blocking Percentage (%)	Enter the percentage of calls to be blocked for this destination in numerals. This value specifies the percentage of lower precedence calls made to this destination that get blocked by the route pattern. This percentage limits the lower precedence calls only; the flash and higher precedence calls made to this destination are allowed at all times The Call Blocking Percentage (%) field is enabled only if the Apply Call Blocking Percentage check box is checked.
Resource Priority Namespace Network Domain	Choose a Resource Priority Namespace Network Domain from the drop-down list. To configure the Resource Priority Namespace Network Domains, choose System > MLPP > Namespace > Resource Priority Namespace Network Domain.

Configure a Translation Pattern for Multilevel Precedence and Preemption

Configure translation patterns to specify how to route a call after it is placed. Configuring translation patterns allows your system to manipulate calling and called digits as needed. When the system identifies that a pattern match occurred, your system uses the calling search space that is configured for the translation pattern to perform the subsequent match.

Procedure

Step 1 In Cisco Unified CM Administration, choose **Call Routing** > **Translation Pattern**.

Step 2 Perform one of the following tasks:

- To modify the settings for an existing translation pattern, enter search criteria, click **Find**, and choose an existing Translation Pattern from the resulting list.
- To add a new translation pattern, click **Add New**.

Step 3 From the **MLPP Precedence** drop-down list, choose one of the following settings for this translation pattern:

- **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.

Step 4 From the **Resource-Priority Namespace Network Domain** drop-down list, choose a resource priority namespace network domain that you configured.

Step 5 From the **Calling Search Space** drop-down list, choose the calling search space that you configured.

Step 6 Click **Save**.

Configure Multilevel Precedence and Preemption for Gateways

Configure Cisco Unified Communications Manager to communicate with non-IP telecommunications devices.

Before you begin

- Configure one of the following gateways:
  - Cisco Catalyst 6000 24 port FXS Gateway
  - Cisco Catalyst 6000 E1 VoIP Gateway
  - Cisco Catalyst 6000 T1 VoIP Gateway
  - Cisco DE-30+ Gateway
  - Cisco DT-24+ Gateway
  - H.323 Gateway

Procedure

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

Step 2 Perform one of the following tasks:

- To modify the settings for an existing gateway, enter search criteria, click **Find**, and choose a gateway from the resulting list.
- To add a new gateway:

  a. Click **Add New**.

b. From the **Gateway Type** drop-down list, choose one of the supported gateway models.

c. Click **Next**.

Step 3 Configure the MLPP fields on the **Gateway Configuration** window. See the Related Topics section for more information about the fields and their configuration options.

Step 4 Click **Save**.

Configure Multilevel Precedence and Preemption for Phones

Caution 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.

Procedure

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

Step 2 Enter search criteria.

Step 3 Click **Find** and choose a phone from the resulting list.

Step 4 Configure the MLPP fields on the **Phone Configuration** window. See the Related Topics section for more information about the fields and their configuration options.

Multilevel Precedence and Preemption Settings for Phones

Table 99: Multilevel Precedence and Preemption Settings for Phones

MLPP Settings for Phones Field	Description
Common Device Configuration	Choose the common device configuration that you configured. The common device configuration includes the attributes (services or features) that are associated with a particular user.
Calling Search Space	From the drop-down list, choose a calling search space (CSS) that you configured . 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 are used together. The directory number CSS takes precedence over the device CSS.

MLPP Settings for Phones Field	Description
MLPP Domain	Choose an MLPP domain from the drop-down list for the MLPP domain that is associated with this device. If you leave the **None** value, this device inherits its MLPP domain from the value that was set in the common device configuration. If the common device configuration does not have an MLPP domain setting, this device inherits its MLPP domain from the value that was set for the MLPP Domain Identifier enterprise parameter.
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, choose a setting to assign to this device from the following options: • **Default**—This device inherits its MLPP indication setting from the common device configuration. • **Off**—This device does not handle nor process indication of an MLPP precedence call. • **On**—This device handles and processes indication of an MLPP precedence call. **Note** Do not configure a device with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful. Turning on MLPP Indication (at the enterprise parameter or device level) disables normal Ring Setting behavior for the lines on a device, unless MLPP Indication is turned off (overridden) for the device.
MLPP Preemption	Be aware that this setting is not available on all devices. If available, this setting specifies whether a device that can preempt calls in progress will use the capability when it places an MLPP precedence call. From the drop-down list, choose a setting to assign to this device from the following options: • **Default** —This device inherits its MLPP preemption setting from the common device configuration. • **Disabled**—This device does not allow preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. • **Forceful**—This device allows preemption of lower precedence calls to take place when necessary for completion of higher precedence calls.

Configure a Directory Number to Place Multilevel Precedence and Preemption Calls

After you configure a device, you can add a line (directory number) from the updated **Device Configuration** window.

Procedure

Step 1 From Cisco Unified CM Administration in the **Device Configuration** window, click **Add a new DN** for the appropriate line.

Step 2 In the **Target (Destination)** field, 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 (*).

Step 3 From the **MLPP Calling Search Space** drop-down list, choose the calling search space to associate with the MLPP alternate party target (destination) number.

Step 4 In the **MLPP No Answer Ring Duration (seconds)**, enter the number of seconds (between 4 and 60) after which an MLPP precedence call is 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 **Precedence Alternate Party Timeout** enterprise parameter.

Step 5 Click **Save**.

Configure a User Device Profile for Multilevel Precedence and Preemption

When a user profile is assigned to a phone, the phone inherits the configuration of the assigned user, including any CSS that is associated with the user. The phone CSS can, however, override the user profile. Cisco Unified Communications Manager assigns the precedence level that is associated with the dialed pattern to the call when a pattern match occurs. The system sets the call request as a precedence call with the assigned precedence level.

Procedure

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

Step 2 Perform one of the following tasks:

- To modify the settings for an existing device profile, enter search criteria, click **Find**, and then choose an existing device profile from the resulting list.
- To add a new device profile:
    - Click **Add New**.
    - From the **Device Profile Type** drop-down list, choose a profile type.

- Click **Next**.
- From the **Device Protocol** drop-down list, choose either **SIP** or **SCCP**.

Step 3 Click **Next**.

Step 4 From the **MLPP Domain** drop-down list, choose an MLLP domain that you configured.

Step 5 From the **MLPP Indication** drop-down list, choose one of the following settings to specify whether a device that is capable of playing precedence tones will use the capability when it places an MLPP precedence call:

- • **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.

Step 6 From the **MLPP Preemption** drop-down list, choose one of the following settings to specify whether a device that is capable of preempting calls in progress will use the capability when it places an MLPP precedence call:

- • **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.

Step 7 Click **Save**.

Configure the Default Device Profile for Multilevel Precedence and Preemption

Use the default device profile for whenever a user logs on to a phone model for which no user device profile exists. A default device profile comprises the set of services and features that are associated with a particular device.

Caution 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.

Procedure

Step 1 In Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Default Device Profile**.

Step 2 Perform one of the following tasks:

- To modify the settings for an existing default device profile, choose an existing default device profile from the **Device Profile Defaults** section.

- To add a new default device profile, choose a device profile type from the drop-down list, click **Next**, choose a device protocol, and then click **Next**.

Step 3 From the **MLPP Domain** drop-down list, choose an MLPP domain that you configured to associate to the device.

Step 4 From the **MLPP Indication** drop-down list, choose one of the following settings to specify whether a device that is capable of playing precedence tones will use the capability when it places an MLPP precedence call:

- **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.

Step 5 From the **MLPP Preemption** drop-down list, choose one of the following settings to specify whether a device that is capable of preempting calls in progress will use the capability when it places an MLPP precedence call:

- **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.

Step 6 Click **Save**.

Multilevel Precedence and Preemption Interactions and Restrictions

Multilevel Precedence and Preemption Interactions

Table 100: Multilevel Precedence and Preemption Interactions

Feature	Interaction
729 Annex A	729 Annex A is supported.
Cisco Extension Mobility	The MLPP service domain remains associated with a user device profile when a user logs in to a device by using extension mobility. The MLPP Indication and Preemption settings also propagate with extension mobility. If either the device or the device profile do not support MLPP, these settings do not propagate.

Feature	Interaction
Cisco Unified Communications Manager Assistant	MLPP interacts with Cisco Unified Communications Manager Assistant as follows: • When Cisco Unified Communications Manager Assistant handles an MLPP precedence call, Cisco Unified Communications Manager Assistant preserves call precedence. • Cisco Unified Communications Manager Assistant filters MLPP precedence calls in the same manner as it filters all other calls. The precedence of a call does not affect whether the call is filtered. • Because Cisco Unified Communications Manager Assistant does not register the precedence of a call, it does not provide any additional indication of the precedence of a call on the assistant console.
Immediate Divert	Immediate Divert diverts calls to voice-messaging mail boxes regardless of the type of call (for example, a precedence call). When Alternate Party Diversion (call precedence) is activated, Call Forward No Answer (CFNA) is also deactivated.
Resource Reservation Protocol (RSVP)	RSVP supports MLPP inherently. The Cisco Unified Communications Manager System Guide explains how MLPP functions when RSVP is activated.
Supplementary Services	MLPP interacts with multiple line appearances, call transfer, call forwarding, three-way calling, call pickup, and hunt pilots as documented in the and the subsections that describe the interaction with each service.

Multilevel Precedence and Preemption Restrictions

Table 101: Multilevel Precedence and Preemption Restrictions

Restriction	Description
Bandwidth	Cisco Unified Communications Manager preempts lower precedence calls when adjusting video bandwidth for high priority calls. If the bandwidth is not sufficient to preempt, Cisco Unified Communications Manager instructs endpoints to use previously reserved lower video bandwidth. When Cisco Unified Communications Manager preempts a video call, the preempted party receives a preemption tone and the call gets cleared.
Call Detail Records	For the DRSN, CDRs represent precedence levels with values 0, 1, 2, 3, and 4 where 0 specifies Executive Override and 4 specifies Routine, as used in DSN. CDRs thus do not use the DRSN format.
Common Network Facility Preemption	Common Network Facility Preemption support exists only for T1-CAS and T1-PRI (North American) interfaces on targeted Voice over IP gateways that Cisco Unified Communications Manager controls by using MGCP protocol and that have been configured as MLPP Preemption Enabled.

Restriction	Description
Intercluster trunks	Intercluster trunk MLPP carries precedence information through dialed digits. Domain information does not get preserved and must be configured per trunk for incoming calls.
Line Groups	MLPP-enabled devices are not supported in line groups. We recommend the following guidelines: • MLPP-enabled devices should not be configured in a line group. Route groups, however, are supported. Both trunk selection and hunting methods are supported. • If an MLPP-enabled device is configured in a line group or route group, in the event of preemption, if the route list does not lock onto the device, the preempted call may be rerouted to other devices in the route/hunt list and preemption indication may be returned only after no devices are able to receive the call. • Route lists can be configured to support either of two algorithms of trunk selection and hunting for precedence calls. In method 1, perform a preemptive search directly. In method 2, first perform a friendly search. If this search is not successful, perform a preemptive search. Method 2 requires two iterations through devices in a route list. If route lists are configured for method 2, in certain scenarios involving line groups, route lists may seem to iterate through the devices twice for precedence calls.
Look Ahead For Busy	Cisco Unified Communications Manager does not support the Look Ahead for Busy (LFB) option.
MLPP Notification	Only MLPP Indication Enabled devices generate MLPP-related notifications, such as tones and ringers. If a precedence call terminates at a device that is not MLPP Indication Enabled, no precedence ringer gets applied. If a precedence call originates from a device that is not MLPP Indication Enabled, no precedence ringback tone gets applied. If a device that is not MLPP Indication Enabled is involved in a call that is preempted (that is, the other side of the call initiated preemption), no preemption tone gets applied to the device.
Phones and trunks	For phones, devices that are MLPP indication disabled (that is, MLPP Indication is set to Off) cannot be preempted. For trunks, MLPP indication and preemption function independently.
Ring Setting Behavior	Turning on MLPP Indication (at the enterprise parameter, common device configuration, or device level) disables normal Ring Setting behavior for the lines on a device, unless MLPP Indication is turned off (overridden) for the device.
SCCP	IOS gateways support the SCCP interface to Cisco Unified Communications Manager. They support BRI and analog phones which appear on Cisco Unified Communications Manager as supported phone models. SCCP phones support the MLPP feature, and so do some phones with specific SIP loads. See the relevant phone administration and user guides for Cisco IP phone support information.

Restriction	Description
Supplementary Services	MLPP support for supplementary services specifies the following restrictions: • MLPP addresses only the basic Call Pickup feature and Group Call Pickup feature, not Other Group Pickup. • Call Forward All (CFA) support for inbound MLPP calls always forwards the call to the MLPP Alternate Party (MAP) target of the called party, if the MAP target is configured. In the event of an incorrect configuration (that is, if no MAP target is specified), the call is rejected, and the calling party receives a reorder tone. • Call Forward No Answer (CFNA) support for inbound MLPP calls forwards the call once to a CFNA target. After the first hop, if the call is unanswered, the call is sent to the MAP target of the original called party, if the MAP target has been configured. In the event of an incorrect configuration (that is, if no MAP target is specified), the call gets rejected, and the calling party receives reorder tone. • Call Forward Busy (CFB) support for inbound MLPP calls forwards the call up to the maximum number that has been configured for forwarding hops. If the maximum hop count gets reached, the call gets sent to the MAP target of the original called party, if the MAP target has been configured. In the event of an incorrect configuration (that is, no MAP target is specified), the call gets rejected, and the calling party receives reorder tone. • For hunt pilot support, the hunt group algorithm must specify Longest Idle Time, Top Down, or Circular. Ensure the hunt group options for busy treatment, no answer treatment, and unregistered treatment are set to Try next member, but do not go to next group. Preemption only occurs across a single hunt group.
User Access Channel	User Access Channel support exists only for the following Cisco Unified IP Phone models, which must be configured as MLPP Preemption Enabled: • Cisco Unified IP Phone 7960, 7962, 7965 • Cisco Unified IP Phone 7940, 7942, 7945

CHAPTER 88

Configure Two Stacks (IPv4 and IPv6)

Two Stacks (IPv4 and IPv6) Overview

When your SIP network is configured for both IPv4 and IPv6 stacks, SIP devices can handle calls for each of the following scenarios:

- All devices in the call support IPv4 only
- All devices in the call support IPv6 only
- All devices in the call support both IPv4 and IPv6 stacks. In this scenario, the system determines the IP address type by the configuration for the **IP Addressing Mode Preference for Signaling** setting for signaling events and the **IP Addressing Mode Preference for Media** enterprise parameter for media events.
- One device supports IPv4 only and the other supports IPv6 only. In this scenario, Unified Communications Manager inserts an MTP into the call path to translate the signaling between the two addressing types.

For SIP devices and trunks, you can enable two-stack support by configuring Alternate Network Address Types (ANAT). When ANAT is applied to a SIP device or trunk, the SIP signaling that the device or trunk sends includes both an IPv4 and IPv6 address, if both are available. ANAT allows the endpoint to interoperate seamlessly in both IPv4-only and IPv6-only networks.

Two Stacks (IPv4 and IPv6) Prerequisites

You must first configure Cisco Unified Communications Manager to support the IPv6 stack (IPv4 is enabled by default). This includes setting IP addressing preferences for both media and signaling. For configuration details, see IPv6 Configuration Task Flow, on page 92.

Two Stacks (IPv4 and IPv6) Configuration Task Flow

Complete the following tasks to configure SIP devices and trunks to support both IPv4 and IPv6 addressing simultaneously.

Procedure

	Command or Action	Purpose
Step 1	Configure ANAT for a SIP Profile, on page 690	Configure a SIP Profile that supports both IPv4 and IPv6 stacks simultaneously.
Step 2	Apply ANAT to SIP Phone, on page 691	Apply the ANAT-enabled SIP Profile to a SIP phone. This allows the SIP phone to support both IPv4 and IPv6 stacks simultaneously.
Step 3	Apply ANAT to a SIP Trunk, on page 691	Apply the ANAT-enabled SIP Profile to a SIP trunk. This allows the trunk to support both IPv4 and IPv6 stacks simultaneously.
Step 4	Restart Services, on page 691	After configuring your system to support both IPv4 and IPv6 stacks simultaneously, restart essential services.

Configure ANAT for a SIP Profile

Use this procedure to configure a SIP Profile that supports Alternate Network Address Types (ANAT). SIP devices and trunks that use this profile can interoperate seamlessly between IPv4-only and IPv6-only networks.

Procedure

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

Step 2 Do one of the following:

a) Click **Add New** to create a new SIP Profile.
b) Click **Find** and select an existing SIP Profile.

Step 3 Check the **Enable ANAT** check box.

Step 4 Complete the remaining fields in the **SIP Profile Configuration** window. For more information on the fields and their configuration options, see the system Online Help.

Step 5 Click **Save**.

You must apply the SIP Profile to a SIP phone or SIP trunk to enable those devices to support both IPv4 and IPv6 stacks simultaneously.

Apply ANAT to SIP Phone

Use this procedure to apply the Alternate Network Address Types (ANAT) configuration to a SIP phone. When ANAT is enabled, the phone can communicate with both IPv4-only and IPv6-only networks simultaneously.

Procedure

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

Step 2 Click **Find** and select an existing phone.

Step 3 From the **SIP Profile** drop-down list box, select the SIP Profile on which you enabled ANAT.

Step 4 Complete the remaining fields in the **Phone Configuration** window. For more information on the fields and their configuration options, see the system Online Help.

Step 5 Click **Save**.

Apply ANAT to a SIP Trunk

Use this procedure to apply the Alternate Network Address Types configuration to an existing SIP trunk. This allows the SIP trunk to support both IPv4 and IPv6 stacks simultaneously.

Note For more information on SIP trunk configuration options, see Configure SIP Trunks, on page 101.

Procedure

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

Step 2 Click **Find** and select an existing SIP trunk.

Step 3 From the **SIP Profile** drop-down list box, select the SIP Profile on which you enabled ANAT.

Step 4 Complete the remaining fields in the **Trunk Configuration** window. For more information on the fields and their configuration options, see the system Online Help.

Step 5 Click **Save**

Restart Services

After configuring your system to support both IPv4 and IPv6 stacks simultaneously, restart essential services.

Procedure

Step 1 Log into Cisco Unified Serviceability and choose **Tools** > **Control Center - Feature Services**.

Step 2 Check the check box corresponding to each of the following services:

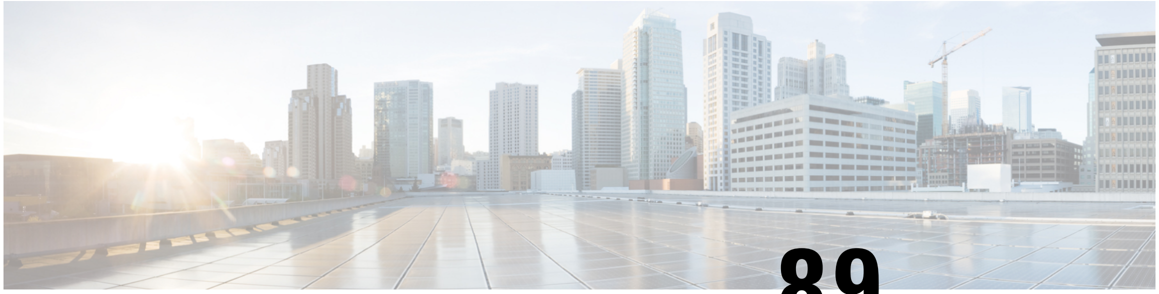
- Cisco CallManager
- Cisco CTIManager
- Cisco Certificate Authority Proxy Function
- Cisco IP Voice Media Streaming App

Step 3 Click **Restart**.

Step 4 Click **OK**.

PART XI

Reference Information



CHAPTER 89

Cisco Unified Communications Manager TCP and UDP Port Usage

Cisco Unified Communications Manager TCP and UDP Port Usage Overview

Cisco Unified Communications Manager TCP and UDP ports are organized into the following categories:

- Intracluster Ports Between Cisco Unified Communications Manager Servers
- Common Service Ports
- Ports Between Cisco Unified Communications Manager and LDAP Directory
- Web Requests From CCMAdmin or CCMUser to Cisco Unified Communications Manager
- Web Requests From Cisco Unified Communications Manager to Phone
- Signaling, Media, and Other Communication Between Phones and Cisco Unified Communications Manager
- Signaling, Media, and Other Communication Between Gateways and Cisco Unified Communications Manager
- Communication Between Applications and Cisco Unified Communications Manager
- Communication Between CTL Client and Firewalls
- Special Ports on HP Servers

See “Port Descriptions” for port details in each of the above categories.

Note Cisco has not verified all possible configuration scenarios for these ports. If you are having configuration problems using this list, contact Cisco technical support for assistance.

Port references apply specifically to Cisco Unified Communications Manager. Some ports change from one release to another, and future releases may introduce new ports. Therefore, make sure that you are using the correct version of this document for the version of Cisco Unified Communications Manager that is installed.

While virtually all protocols are bidirectional, directionality from the session originator perspective is presumed. In some cases, the administrator can manually change the default port numbers, though Cisco does not recommend this as a best practice. Be aware that Cisco Unified Communications Manager opens several ports strictly for internal use.

Installing Cisco Unified Communications Manager software automatically installs the following network services for serviceability and activates them by default. Refer to “Intracluster Ports Between Cisco Unified Communications Manager Servers” for details:

- Cisco Log Partition Monitoring (To monitor and purge the common partition. This uses no custom common port.)
- Cisco Trace Collection Service (TCTS port usage)
- Cisco RIS Data Collector (RIS server port usage)
- Cisco AMC Service (AMC port usage)

Configuration of firewalls, ACLs, or QoS will vary depending on topology, placement of telephony devices and services relative to the placement of network security devices, and which applications and telephony extensions are in use. Also, bear in mind that ACLs vary in format with different devices and versions.

Note You can also configure Multicast Music on Hold (MOH) ports in Cisco Unified Communications Manager. Port values for multicast MOH are not provided because the administrator specifies the actual port values.

Note The ephemeral port range for the system is 32768 to 61000, and the ports needs to be open to keep the phones registered. For more information, see http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-series-home.html.

Note Make sure that you configure your firewall so that connections to port 22 are open, and are not throttled. During the installation of IM and Presence subscriber nodes, multiple connections to the Cisco Unified Communications Manager publisher node are opened in quick succession. Throttling these connections could lead to a failed installation.

Port Descriptions

Intracluster Ports Between Cisco Unified Communications Manager Servers

Table 102: Intracluster Ports Between Cisco Unified Communications Manager Servers

From (Sender)	To (Listener)	Destination Port	Purpose
Endpoint	Unified Communications Manager	514 / UDP	System logging se
Unified Communications Manager	Unified Communications Manager	443 / TCP	This port is used f communication be subscriber and pul COP file installati subscriber node.
Unified Communications Manager	RTMT	1090, 1099 / TCP	Cisco AMC Servi performance mon collection, logging
Unified Communications Manager (DB)	Unified Communications Manager (DB)	1500, 1501 / TCP	Database connect TCP is the second connection)
Unified Communications Manager (DB)	Unified Communications Manager (DB)	1510 / TCP	CAR IDS DB. CA listens on waiting f requests from the
Unified Communications Manager (DB)	Unified Communications Manager (DB)	1511 / TCP	CAR IDS DB. An used to bring up a instance of CAR I upgrade.
Unified Communications Manager (DB)	Unified Communications Manager (DB)	1515 / TCP	Database replicati nodes during insta
Cisco Extended Functions (QRT)	Unified Communications Manager (DB)	2552 / TCP	Allows subscriber Cisco Unified Cor Manager database notification
Unified Communications Manager	Unified Communications Manager	2551 / TCP	Intracluster comm between Cisco Ex Services for Activ determination
Unified Communications Manager (RIS)	Unified Communications Manager (RIS)	2555 / TCP	Real-time Informa (RIS) database se

From (Sender)	To (Listener)	Destination Port	Purpose
Unified Communications Manager (RTMT/AMC/SOAP)	Unified Communications Manager (RIS)	2556 / TCP	Real-time Informatio (RIS) database client RIS
Unified Communications Manager (DRS)	Unified Communications Manager (DRS)	4040 / TCP	DRS Primary Agent
Unified Communications Manager (Tomcat)	Unified Communications Manager (SOAP)	5001/TCP	This port is used by S monitor for Real Tim Monitoring Service.
Unified Communications Manager (Tomcat)	Unified Communications Manager (SOAP)	5002/TCP	This port is used by S monitor for Performa Monitor Service.
Unified Communications Manager (Tomcat)	Unified Communications Manager (SOAP)	5003/TCP	This port is used by S monitor for Control C Service.
Unified Communications Manager (Tomcat)	Unified Communications Manager (SOAP)	5004/TCP	This port is used by S monitor for Log Coll Service.
Standard CCM Admin Users / Admin	Unified Communications Manager	5005 / TCP	This port is used by S CDROnDemand2 ser
Unified Communications Manager (Tomcat)	Unified Communications Manager (SOAP)	5007 / TCP	SOAP monitor
Unified Communications Manager (RTMT)	Unified Communications Manager (TCTS)	Ephemeral / TCP	Cisco Trace Collectio Service (TCTS) -- the service for RTMT Tr Log Central (TLC)
Unified Communications Manager (Tomcat)	Unified Communications Manager (TCTS)	7000, 7001, 7002 / TCP	This port is used for communication betw Trace Collection Too and Cisco Trace Coll servlet.
Unified Communications Manager (DB)	Unified Communications Manager (CDLM)	8001 / TCP	Client database chang notification
Unified Communications Manager (SDL)	Unified Communications Manager (SDL)	8002 / TCP	Intracluster communi service
Unified Communications Manager (SDL)	Unified Communications Manager (SDL)	8003 / TCP	Intracluster communi service (to CTI)

From (Sender)	To (Listener)	Destination Port	Purpose
Unified Communications Manager	CMI Manager	8004 / TCP	Intracluster comm between Cisco Ur Communications CMI Manager
Unified Communications Manager (Tomcat)	Unified Communications Manager (Tomcat)	8005 / TCP	Internal listening Tomcat shutdown
Unified Communications Manager (Tomcat)	Unified Communications Manager (Tomcat)	8080 / TCP	Communication be used for diagnosti
Gateway	Unified Communications Manager	8090	HTTP Port for co between CuCM a (Cayuga interfae) Recording feature
Unified Communications Manager	Gateway		
Unified Communications Manager (IPSec)	Unified Communications Manager (IPSec)	8500 / TCP and UDP	Intracluster replic system data by IP Manager
Unified Communications Manager (RIS)	Unified Communications Manager (RIS)	8888 - 8889 / TCP	RIS Service Mana request and reply
Location Bandwidth Manager (LBM)	Location Bandwidth Manager (LBM)	9004 / TCP	Intracluster comm between LBMs
Unified Communications Manager Publisher	Unified Communications Manager Subscriber	22 / TCP	Cisco SFTP servi open this port wh new subscriber.
Unified Communications Manager	Unified Communications Manager	8443 / TCP	Allows access to C - Feature and Net between nodes.

Common Service Ports

Table 103: Common Service Ports

From (Sender)	To (Listener)	Destination Port	Purpose
Endpoint	Unified Communications Manager	7	Internet Control Message Protocol (ICMP) This protocol number carries echo-related traffic. It does not constitute a port as indicated in the column heading.
Unified Communications Manager	Endpoint		

From (Sender)	To (Listener)	Destination Port	Purpose
Unified Communications Manager (DRS, Call Detail Record)	SFTP server	22 / TCP	Send the backup data to SFTP server. (DRS Local Agent) Send the Call Detail Record data to SFTP server.
Endpoint	Unified Communications Manager (DHCP Server)	67 / UDP	Cisco Unified Communications Manager acting as a DHCP server **Note** Cisco does not recommend running DHCP server on Cisco Unified Communications Manager.
Unified Communications Manager	DHCP Server	68 / UDP	Cisco Unified Communications Manager acting as a DHCP client **Note** Cisco does not recommend running DHCP client on Cisco Unified Communications Manager. Configure Cisco Unified Communications Manager with static IP addresses instead.)
Endpoint or Gateway	Unified Communications Manager	69, 6969, then Ephemeral / UDP	TFTP service to phones and gateways
Endpoint or Gateway	Unified Communications Manager	6970 / TCP	TFTP between primary and proxy servers. HTTP service from the TFTP server to phones and gateways.
Unified Communications Manager	NTP Server	123 / UDP	Network Time Protocol (NTP)
SNMP Server	Unified Communications Manager	161 / UDP	SNMP service response (requests from management applications)

From (Sender)	To (Listener)	Destination Port	Purpose
CUCM Server SNMP Primary Agent application	SNMP trap destination	162 / UDP	SNMP traps
SNMP Server	Unified Communications Manager	199 / TCP	built-in SNMP agent listening port for SMUX support
Unified Communications Manager	DHCP Server	546 / UDP	DHCPv6. DHCP port for IPv6.
Unified Communications Manager Serviceability	Location Bandwidth Manager (LBM)	5546 / TCP	Enhanced Location CAC Serviceability
Unified Communications Manager	Location Bandwidth Manager (LBM)	5547 / TCP	Call Admission requests and bandwidth deductions
Unified Communications Manager	Unified Communications Manager	6161 / UDP	Used for communication between Primary Agent and Native Agent to process Native agent MIB requests
Unified Communications Manager	Unified Communications Manager	6162 / UDP	Used for communication between Primary Agent and Native Agent to forward notifications generated from Native Agent
Centralized TFTP	Alternate TFTP	6970 / TCP	Centralized TFTP File Locator Service
Unified Communications Manager	Unified Communications Manager	7161 / TCP	Used for communication between SNMP Primary Agent and subagents
SNMP Server	Unified Communications Manager	7999 / TCP	Cisco Discovery Protocol (CDP) agent communicates with CDP executable
Endpoint	Unified Communications Manager	443, 8443 / TCP	Used for Cisco User Data Services (UDS) requests
Unified Communications Manager	Unified Communications Manager	9050 / TCP	Service CRS requests through the TAPS residing on Cisco Unified Communications Manager

From (Sender)	To (Listener)	Destination Port	Purpose
Unified Communications Manager	Unified Communications Manager	61441 / UDP	Cisco Unified Communications Manager applications send out alarms to this port through UDP. Cisco Unified Communications Manager MIB agent listens on this port and generates SNMP traps per Cisco Unified Communications Manager MIB definition.
Unified Communications Manager	Unified Communications Manager	5060, 5061 / TCP	Provide trunk-based SIP services
Unified Communications Manager	Unified Communications Manager	7501	Used by Intercluster Lookup Service (ILS) for certificate based authentication.
Unified Communications Manager	Unified Communications Manager	7502	Used by ILS for password-based authentication.
Unified Communications Manager	Unified Communications Manager	9966	Used by Cisco push notification service to communicate between the nodes in the cluster when firewall is enabled.
--	--	8000-48200	ASR and ISR G3 platforms default port range.
		16384-32766	ISR G2 platform default port range.

Ports Between Cisco Unified Communications Manager and LDAP Directory

Table 104: Ports Between Cisco Unified Communications Manager and LDAP Directory

From (Sender)	To (Listener)	Destination Port	Purpose
Unified Communications Manager	External Directory	389, 636, 3268, 3269 / TCP	Lightweight Directory Access Protocol (LDAP) query to external directory (Active Directory, Netscape Directory)
External Directory	Unified Communications Manager	Ephemeral	

Web Requests From CCMAdmin or CCMUser to Cisco Unified Communications Manager

Table 105: Web Requests From CCMAdmin or CCMUser to Cisco Unified Communications Manager

From (Sender)	To (Listener)	Destination Port	Purpose
Browser	Unified Communications Manager	80, 8080 / TCP	Hypertext Transpo (HTTP)
Browser	Unified Communications Manager	443, 8443 / TCP	Hypertext Transpo over SSL (HTTPS

Web Requests From Cisco Unified Communications Manager to Phone

Table 106: Web Requests From Cisco Unified Communications Manager to Phone

From (Sender)	To (Listener)	Destination Port	Purpose
Unified Communications Manager • QRT • RTMT • Find and List Phones page • Phone Configuration page	Phone	80 / TCP	Hypertext Transpo (HTTP)

Signaling, Media, and Other Communication Between Phones and Cisco Unified Communications Manager

Table 107: Signaling, Media, and Other Communication Between Phones and Cisco Unified Communications Manager

From (Sender)	To (Listener)	Destination Port	Purpose
Phone	DNS server	53/ TCP	Session Initiation Protocol (SIP) phones resolve the Fully Qualified Domain Name (FQDN) using a Domain Name System (DNS) **Note** By default, some wireless access points block TCP 53 port, which prevents wireless SIP phones from registering when CUCM is configured using FQDN.
Phone	Unified Communications Manager (TFTP)	69, then Ephemeral / UDP	Trivial File Transfer Protocol (TFTP) used to download firmware and configuration files
Phone	Unified Communications Manager	2000 / TCP	Skinny Client Control Protocol (SCCP)
Phone	Unified Communications Manager	2443 / TCP	Secure Skinny Client Control Protocol (SCCPS)
Phone	Unified Communications Manager	2445 / TCP	Provide trust verification service to endpoints.
Phone	Unified Communications Manager (CAPF)	3804 / TCP	Certificate Authority Proxy Function (CAPF) listening port for issuing Locally Significant Certificates (LSCs) to IP phones
Phone	Unified Communications Manager	5060 / TCP and UDP	Session Initiation Protocol (SIP) phone
Unified Communications Manager	Phone		

From (Sender)	To (Listener)	Destination Port	Purpose
Phone	Unified Communications Manager	5061 TCP	Secure Session Initiation Protocol (SIPS) phone
Unified Communications Manager	Phone		
Phone	Unified Communications Manager (TFTP)	6970 TCP	HTTP-based download of firmware and configuration files
Phone	Unified Communications Manager (TFTP)	6971, 6972 / TCP	HTTPS interface to TFTP. Phones use this port to download a secure configuration file from TFTP.
Phone	Unified Communications Manager	8080 / TCP	Phone URLs for XML applications, authentication, directories, services, and so on. You can configure these ports on a per-service basis.
Phone	Unified Communications Manager	9443 / TCP	Phone use this port for authenticated contact search.
Phone	Unified Communications Manager	9444	
iPhone/iPad (Webex App)	Unified Communications Manager	9560/Secure WebSocket	Webex App uses this port number for the LPNS feature.
IP VMS	Phone	16384 - 32767 / UDP	Real-Time Protocol (RTP), Secure Real-Time Protocol (SRTP) **Note** Cisco Unified Communications Manager only uses 24576-32767 although other devices use the full range.
Phone	IP VMS		

Signaling, Media, and Other Communication Between Gateways and Cisco Unified Communications Manager

Table 108: Signaling, Media, and Other Communication Between Gateways and Cisco Unified Communications Manager

From (Sender)	To (Listener)	Destination Port	Purpose
Gateway	Unified Communications Manager	47, 50, 51	Generic Routing Enca (GRE), Encapsulating Payload (ESP), Authe Header (AH). These p numbers carry encryp traffic. They do not co port as indicated in th heading.
Unified Communications Manager	Gateway		
Gateway	Unified Communications Manager	500 / UDP	Internet Key Exchang for IP Security protoc establishment
Unified Communications Manager	Gateway		
Gateway	Unified Communications Manager (TFTP)	69, then Ephemeral / UDP	Trivial File Transfer (TFTP)
Unified Communications Manager with Cisco Intercompany Media Engine (CIME) trunk	CIME ASA	1024-65535 / TCP	Port mapping service. in the CIME off-path deployment model.
Gatekeeper	Unified Communications Manager	1719 / UDP	Gatekeeper (H.225)
Gateway	Unified Communications Manager	1720 / TCP	H.225 signaling servi H.323 gateways and I Trunk (ICT)
Unified Communications Manager	Gateway		
Gateway	Unified Communications Manager	Ephemeral / TCP	H.225 signaling servi gatekeeper-controlled
Unified Communications Manager	Gateway		

From (Sender)	To (Listener)	Destination Port	Purpose
Gateway	Unified Communications Manager	Ephemeral / TCP	H.245 signaling s establishing voice data **Note** The H used l systen the ty gatew For IC the H range 1100
Unified Communications Manager	Gateway		
Gateway	Unified Communications Manager	2000 / TCP	Skinny Client Con (SCCP)
Gateway	Unified Communications Manager	2001 / TCP	Upgrade port for 6 with Cisco Unifie Communications deployments
Gateway	Unified Communications Manager	2002 / TCP	Upgrade port for 6 with Cisco Unifie Communications deployments
Gateway	Unified Communications Manager	2427 / UDP	Media Gateway C Protocol (MGCP) control
Gateway	Unified Communications Manager	2428 / TCP	Media Gateway C Protocol (MGCP)
--	--	4000 - 4005 / TCP	These ports are use Real-Time Transp (RTP) and Real-Ti Control Protocol (for audio, video a channel when Cis Communications l not have ports for
Gateway	Unified Communications Manager	5060 / TCP and UDP	Session Initiation l gateway and Inter (ICT)
Unified Communications Manager	Gateway		

From (Sender)	To (Listener)	Destination Port	Purpose
Gateway	Unified Communications Manager	5061 / TCP	Secure Session Initiat Protocol (SIPS) gatev Intercluster Trunk (IC
Unified Communications Manager	Gateway		
Gateway	Unified Communications Manager	16384 - 32767 / UDP	Real-Time Protocol (Secure Real-Time Pro (SRTP) **Note** Cisco Ur Commur Manager 24576-32 although devices u full rang
Unified Communications Manager	Gateway		

Communication Between Applications and Cisco Unified Communications Manager

Table 109: Communication Between Applications and Cisco Unified Communications Manager

From (Sender)	To (Listener)	Destination Port	Purpose
CTL Client	Unified Communications Manager CTL Provider	2444 / TCP	Certificate Trust List provider listening ser Cisco Unified Commu Manager
Cisco Unified Communications App	Unified Communications Manager	2748 / TCP	CTI application serve
Cisco Unified Communications App	Unified Communications Manager	2749 / TCP	TLS connection betw applications (JTAPI/T CTIManager
Cisco Unified Communications App	Unified Communications Manager	2789 / TCP	JTAPI application ser
Unified Communications Manager Assistant Console	Unified Communications Manager	2912 / TCP	Cisco Unified Commu Manager Assistant se (formerly IPMA)
Unified Communications Manager Attendant Console	Unified Communications Manager	1103 -1129 / TCP	Cisco Unified Commu Manager Attendant C (AC) JAVA RMI Reg server

From (Sender)	To (Listener)	Destination Port	Purpose
Unified Communications Manager Attendant Console	Unified Communications Manager	1101 / TCP	RMI server sends messages to client ports.
Unified Communications Manager Attendant Console	Unified Communications Manager	1102 / TCP	Attendant Consol server bind port -- sends RMI messa ports.
Unified Communications Manager Attendant Console	Unified Communications Manager	3223 / UDP	Cisco Unified Co Manager Attenda (AC) server line s receives ping and message from, an states to, the atten server.
Unified Communications Manager Attendant Console	Unified Communications Manager	3224 / UDP	Cisco Unified Co Manager Attenda (AC) clients regis AC server for line state information.
Unified Communications ManagerAttendant Console	Unified Communications Manager	4321 / UDP	Cisco Unified Co Manager Attenda (AC) clients regis server for call co
Unified Communications Manager with SAF/CCD	IOS Router running SAF image	5050 / TCP	Multi-Service IO running EIGRP/S
Unified Communications Manager	Cisco Intercompany Media Engine (IME) Server	5620 / TCP Cisco recommends a value of 5620 for this port, but you can change the value by executing the add ime vapserver or set ime vapserver port CLI command on the Cisco IME server.	VAP protocol use communicate to t Intercompany Me server.
Cisco Unified Communications App	Unified Communications Manager	8443 / TCP	AXL / SOAP AP programmatic rea writes to the Cisc Communications database that thir as billing or telep management app

Communication Between CTL Client and Firewalls

Table 110: Communication Between CTL Client and Firewalls

From (Sender)	To (Listener)	Destination Port	Purpose
CTL Client	TLS Proxy Server	2444 / TCP	Certificate Trust List provider listening ser ASA firewall

Communication Between Cisco Smart Licensing Service and Cisco Smart Software Manager

Cisco Smart Licensing Service in Unified Communications Manager sets up direct communication with Cisco Smart Software Manager through Call Home.

Table 111: Communication Between Cisco Smart Licensing Service and Cisco Smart Software Manager

From (Sender)	To (Listener)	Destination Port	Purpose
Unified Communications Manager (Cisco Smart Licensing Service)	Cisco Smart Software Manager (CSSM)	443 / HTTPS	Smart Licensing Service sends the license usage to CSSM to check whether Unified CM is a complaint or not.

Special Ports on HP Servers

Table 112: Special Ports on HP Servers

From (Sender)	To (Listener)	Destination Port	Purpose
Endpoint	HP SIM	2301 / TCP	HTTP port to HP age
Endpoint	HP SIM	2381 / TCP	HTTPS port to HP ag
Endpoint	Compaq Management Agent	25375, 25376, 25393 / UDP	COMPAQ Managem extension (cmaX)
Endpoint	HP SIM	50000 - 50004 / TCP	HTTPS port to HP SI

Port References

Firewall Application Inspection Guides

ASA Series reference information

http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-series-home.html

PIX Application Inspection Configuration Guides

http://www.cisco.com/c/en/us/support/security/pix-firewall-software/products-installation-and-configuration-guides-list.html

FWSM 3.1 Application Inspection Configuration Guide

http://www-author.cisco.com/c/en/us/td/docs/security/fwsm/fwsm31/configuration/guide/fwsm_cfg/inspct_f.html

IETF TCP/UDP Port Assignment List

Internet Assigned Numbers Authority (IANA) IETF assigned Port List

http://www.iana.org/assignments/port-numbers

IP Telephony Configuration and Port Utilization Guides

Cisco CRS 4.0 (IP IVR and IPCC Express) Port Utilization Guide

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

Port Utilization Guide for Cisco ICM/IPCC Enterprise and Hosted Editions

http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_installation_and_configuration_guides_list.html

Cisco Unified Communications Manager Express Security Guide to Best Practices

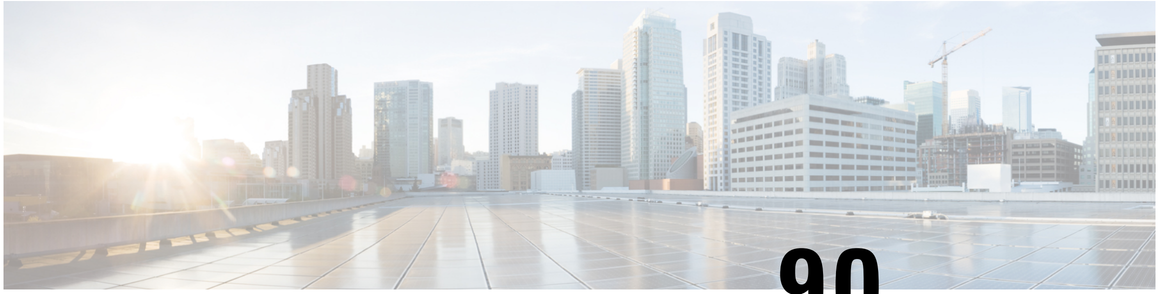
http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_design_guidance09186a00801f8e30.html

Cisco Unity Express Security Guide to Best Practices

http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_design_guidance09186a00801f8e31.html#wp41149

VMware Port Assignment List

TCP and UDP Ports for vCenter Server, ESX hosts, and Other Network Components Management Access



CHAPTER 90

Port Usage Information for the IM and Presence Service

IM and Presence Service Port Usage Overview

This document provides a list of the TCP and UDP ports that the IM and Presence Service uses for intracluster connections and for communications with external applications or devices. It provides important information for the configuration of firewalls, Access Control Lists (ACLs), and quality of service (QoS) on a network when an IP Communications solution is implemented.

Note Cisco has not verified all possible configuration scenarios for these ports. If you are having configuration problems using this list, contact Cisco technical support for assistance.

While virtually all protocols are bidirectional, this document gives directionality from the session originator perspective. In some cases, the administrator can manually change the default port numbers, though Cisco does not recommend this as a best practice. Be aware that the IM and Presence Service opens several ports strictly for internal use.

Ports in this document apply specifically to the IM and Presence Service. Some ports change from one release to another, and future releases may introduce new ports. Therefore, make sure that you are using the correct version of this document for the version of IM and Presence Service that is installed.

Configuration of firewalls, ACLs, or QoS will vary depending on topology, placement of devices and services relative to the placement of network security devices, and which applications and telephony extensions are in use. Also, bear in mind that ACLs vary in format with different devices and versions.

Information Collated in Table

This table defines the information collated in each of the tables in this document.

Table 113: Definition of Table Information

Table Heading	Description
From	The client sending requests to this port
To	The client receiving requests on this port
Role	A client or server application or process
Protocol	Either a Session-layer protocol used for establishing and ending communications, or an Application-layer protocol used for request and response transactions
Transport Protocol	A Transport-layer protocol that is connection-oriented (TCP) or connectionless (UDP)
Destination / Listener	The port used for receiving requests
Source / Sender	The port used for sending requests

IM and Presence Service Port List

The following tables show the ports that the IM and Presence Service uses for intracluster and intercluster traffic.

Table 114: IM and Presence Service Ports - SIP Proxy Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
SIP Gateway -------------- IM and Presence	IM and Presence -------------- SIP Gateway	SIP	TCP/UDP	5060	Ephemeral	Default SIP Proxy UDP and TCP Listener
SIP Gateway	IM and Presence	SIP	TLS	5061	Ephemeral	TLS Server Authentication listener port
IM and Presence	IM and Presence	SIP	TLS	5062	Ephemeral	TLS Mutual Authentication listener port
IM and Presence	IM and Presence	SIP	UDP / TCP	5049	Ephemeral	Internal port. Localhost traffic only.
IM and Presence	IM and Presence	HTTP	TCP	8081	Ephemeral	Used for HTTP requests from the Config Agent to indicate a change in configuration.

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
Third-party Client	IM and Presence	HTTP	TCP	8082	Ephemeral	Default IM and Presence HTTP Listener. Used for Third-Party Clients to connect
Third-party Client	IM and Presence	HTTPS	TLS / TCP	8083	Ephemeral	Default IM and Presence HTTPS Listener. Used for Third-Party Clients to connect

Table 115: IM and Presence Service Ports - Presence Engine Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence	IM and Presence (Presence Engine)	SIP	UDP / TCP	5080	Ephemeral	Default SIP UDP/TCP Listener port
IM and Presence (Presence Engine)	IM and Presence (Presence Engine)	Livebus	UDP	50000	Ephemeral	Internal port. Localhost traffic only. LiveBus messaging port. The IM and Presence Service uses this port for cluster communication.

Table 116: IM and Presence Service Ports - Cisco Tomcat WebRequests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
Browser	IM and Presence	HTTPS	TCP	8080	Ephemeral	Used for web access
Browser	IM and Presence	AXL / HTTPS	TLS / TCP	8443	Ephemeral	Provides database and serviceability access via SOAP
Browser	IM and Presence	HTTPS	TLS / TCP	8443	Ephemeral	Provides access to Web administration
Browser	IM and Presence	HTTPS	TLS / TCP	8443	Ephemeral	Provides access to User option pages

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
Browser	IM and Presence	SOAP	TLS / TCP	8443	Ephemeral	Provides access to Cisco Unified Personal Communicator, Cisco Unified Mobility Advantage, and third-party API clients via SOAP

Table 117: IM and Presence Service Ports - External Corporate Directory Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence -------------- External Corporate Directory	External Corporate Directory -------------- IM and Presence	LDAP	TCP	389 / 3268	Ephemeral	Allows the Directory protocol to integrate with the external Corporate Directory. The LDAP port depends on the Corporate Directory (389 is the default). In case of Netscape Directory, customer can configure different port to accept LDAP traffic. Allows LDAP to communicate between IM&P and the LDAP server for authentication.
IM and Presence	External Corporate Directory	LDAPS	TCP	636	Ephemeral	Allows the Directory protocol to integrate with the external Corporate Directory. LDAP port depends on the Corporate Directory (636 is the default).

Table 118: IM and Presence Service Ports - Configuration Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence (Config Agent)	IM and Presence (Config Agent)	TCP	TCP	8600	Ephemeral	Config Agent heartbeat port

Table 119: IM and Presence Service Ports - Certificate Manager Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence	Certificate Manager	TCP	TCP	7070	Ephemeral	Internal port - Localhost traffic only

Table 120: IM and Presence Service Ports - IDS Database Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence (Database)	IM and Presence (Database)	TCP	TCP	1500	Ephemeral	Internal IDS port for Database clients. Localhost traffic only.
IM and Presence (Database)	IM and Presence (Database)	TCP	TCP	1501	Ephemeral	Internal port - this is an alternate port to bring up a second instance of IDS during upgrade. Localhost traffic only.
IM and Presence (Database)	IM and Presence (Database)	XML	TCP	1515	Ephemeral	Internal port. Localhost traffic only. DB replication port

Table 121: IM and Presence Service Ports - IPSec Manager Request

From Sender	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence (IPSec)	IM and Presence (IPSec)	Proprietary	UDP/TCP	8500	8500	Internal port - cluster manager port used by the ipsec_mgr daemon for cluster replication of platform data (hosts) certs

Table 122: IM and Presence Service Ports - DRF Master Agent Server Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence (DRF)	IM and Presence (DRF)	TCP	TCP	4040	Ephemeral	DRF Master Agent server port, which accepts connections from Local Agent, GUI, and CLI

Table 123: IM and Presence Service Ports - RISDC Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence (RIS)	IM and Presence (RIS)	TCP	TCP	2555	Ephemeral	Real-time Information Services (RIS) database server. Connects to other RISDC services in the cluster to provide clusterwide real-time information
IM and Presence (RTMT/AMC/ SOAP)	IM and Presence (RIS)	TCP	TCP	2556	Ephemeral	Real-time Information Services (RIS) database client for Cisco RIS. Allows RIS client connection to retrieve real-time information
IM and Presence (RIS)	IM and Presence (RIS)	TCP	TCP	8889	8888	Internal port. Localhost traffic only. Used by RISDC (System Access) to link to servM via TCP for service status request and reply

Table 124: IM and Presence Service Ports - SNMP Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
SNMP Server	IM and Presence	SNMP	UDP	161, 8161	Ephemeral	Provides services for SNMP-based management applications
IM and Presence	IM and Presence	SNMP	UDP	6162	Ephemeral	Native SNMP agent that listens for requests forwarded by SNMP master agents
IM and Presence	IM and Presence	SNMP	UDP	6161	Ephemeral	SNMP Master agent that listens for traps from the native SNMP agent, and forwards to management applications
SNMP Server	IM and Presence	TCP	TCP	7999	Ephemeral	Used as a socket for the cdp agent to communicate with the cdp binary

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence	IM and Presence	TCP	TCP	7161	Ephemeral	Used for communication between the SNMP Master agent and subagents
IM and Presence	SNMP Trap Monitor	SNMP	UDP	162	Ephemeral	Sends SNMP traps to management applications
IM and Presence	IM and Presence	SNMP	UDP	Configurable	61441	Internal SNMP trap receiver

Table 125: IM and Presence Service Ports - Racoon Server Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
Gateway -------------- IM and Presence	IM and Presence -------------- Gateway	Ipsec	UDP	500	Ephemeral	Enables Internet Security Association and the KeyManagement Protocol

Table 126: IM and Presence Service Ports - System Service Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence (RIS)	IM and Presence (RIS)	XML	TCP	8888 and 8889	Ephemeral	Internal port. Localhost traffic only. Used to listen to clients communicating with the RIS Service Manager (servM).

Table 127: IM and Presence Service Ports - DNS Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence	DNS Server	DNS	UDP	53	Ephemeral	The port that DNS server listen on for IM and Presence DNS queries. To: DNS Server | From: IM and Presence

Table 128: IM and Presence Service Ports - SSH/SFTP Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence	Endpoint	SSH / SFTP	TCP	22	Ephemeral	Used by many applications to get command line access to the server. Also used between nodes for certificate and other file exchanges (sftp)

Table 129: IM and Presence Service Ports - ICMP Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence -------------- Cisco Unified Communications Manager	Cisco Unified Communications Manager -------------- IM and Presence	ICMP	IP	Not Applicable	Ephemeral	Internet Control Message Protocol (ICMP). Used to communicate with the Cisco Unified Communications Manager server

Table 130: IM and Presence Service Ports - NTP Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence	NTP Server	NTP	UDP	123	Ephemeral	Cisco Unified Communications Manager is the acting NTP server. Used by subscriber nodes to synchronize time with the publisher node.

Table 131: IM and Presence Service Ports - Microsoft Exchange Notify Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
Microsoft Exchange	IM and Presence	HTTP (HTTPu)	) WebDAV - HTTP /UDP/IP notifications 2) EWS - HTTP/TCP /IP SOAP notifications	IM and Presence server port (default 50020)	Ephemeral	Microsoft Exchange uses this port to send notifications (using NOTIFY message) to indicate a change to a particular subscription identifier for calendar events. Used to integrate with any Exchange server in the network configuration. Both ports are created. The kind of messages that are sent depend on the type of Calendar Presence Backend gateway(s) that are configured.

Table 132: IM and Presence Service Ports - SOAP Services Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence (Tomcat)	IM and Presence (SOAP)	TCP	TCP	5007	Ephemeral	SOAP monitor port

Table 133: IM and Presence Service Ports - AMC RMI Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence	RTMT	TCP	TCP	1090	Ephemeral	AMC RMI Object port. Cisco AMC Service for RTMT performance monitors, data collection, logging, and alerting.
IM and Presence	RTMT	TCP	TCP	1099	Ephemeral	AMC RMI Registry port. Cisco AMC Service for RTMT performance monitors, data collection, logging, and alerting.

Table 134: IM and Presence Service Ports - XCP Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
XMPP Client	IM and Presence	TCP	TCP	5222	Ephemeral	Client access port
IM and Presence	IM and Presence	TCP	TCP	5269	Ephemeral	Server to Server connection (S2S) port
Third-party BOSH client	IM and Presence	TCP	TCP	7335	Ephemeral	HTTP listening port used by the XCP Web Connection Manager for BOSH third-party API connections
IM and Presence (XCP Services)	IM and Presence (XCP Router	TCP	TCP	7400	Ephemeral	XCP Router Master Accept Port. XCP services that connect to the router from an Open Port Configuration (for example XCP Authentication Component Service) typically connect on this port.
IM and Presence (XCP Router	IM and Presence (XCP Router	UDP	UDP	5353	Ephemeral	MDNS port. XCP routers in a cluster use this port to discover each other.
IM and Presence (XCP Router	IM and Presence (XCP Router	TCP	TCP	7336	HTTPS	MFT File transfer (On-Premises only).

Table 135: IM and Presence Service Ports - External Database Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence	PostgreSQL database	TCP	TCP	5432[2]	Ephemeral	PostgreSQL database listening port
IM and Presence	Oracle database	TCP	TCP	1521	Ephemeral	Oracle database listening port
IM and Presenc	MSSQL database	TCP	TCP	1433	Ephemeral	MSSQL database listening port

[2] This is the default port, however you can configure the PostgreSQL database to listen on any port.

Table 136: IM and Presence Service Ports - High Availability Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence (Server Recovery Manager)	IM and Presence (Server Recovery Manager)	TCP	TCP	20075	Ephemeral	The port that Cisco Server Recovery Manager uses to provide admin rpc requests.
IM and Presence (Server Recovery Manager)	IM and Presence (Server Recovery Manager)	UDP	UDP	21999	Ephemeral	The port that Cisco Server Recovery Manager uses to communicate with its peer.

Table 137: IM and Presence Service Ports - In Memory Database Replication Messages

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence	IM and Presence	Proprietary	TCP	6603*	Ephemeral	Cisco Presence Datastore
IM and Presence	IM and Presence	Proprietary	TCP	6604*	Ephemeral	Cisco Login Datastore
IM and Presence	IM and Presence	Proprietary	TCP	6605*	Ephemeral	Cisco SIP Registration Datastore
IM and Presence	IM and Presence	Proprietary	TCP	9003	Ephemeral	Cisco Presence Datastore dual node presence redundancy group replication.
IM and Presence	IM and Presence	Proprietary	TCP	9004	Ephemeral	Cisco Login Datastore dual node presence redundancy group replication.
IM and Presence	IM and Presence	Proprietary	TCP	9005	Ephemeral	Cisco SIP Registration Datastore dual node presence redundancy group replication.

* If you want to run the Administration CLI Diagnostic Utility, using the `utils imdb_replication status` command, these ports must be open on all firewalls that are configured between IM and Presence Service nodes in the cluster. This setup is not required for normal operation.

Table 138: IM and Presence Service Ports - In Memory Database SQL Messages

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence	IM and Presence	Proprietary	TCP	6603	Ephemeral	Cisco Presence Datastore SQL Queries.
IM and Presence	IM and Presence	Proprietary	TCP	6604	Ephemeral	Cisco Login Datastore SQL Queries.
IM and Presence	IM and Presence	Proprietary	TCP	6605	Ephemeral	Cisco SIP Registration Datastore SQL Queries.
IM and Presence	IM and Presence	Proprietary	TCP	6606	Ephemeral	Cisco Route Datastore SQL Queries.

Table 139: IM and Presence Service Ports - In Memory Database Notification Messages

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence	IM and Presence	Proprietary	TCP	6607	Ephemeral	Cisco Presence Datastore XML-based change notification.
IM and Presence	IM and Presence	Proprietary	TCP	6608	Ephemeral	Cisco Login Datastore XML-based change notification.
IM and Presence	IM and Presence	Proprietary	TCP	6609	Ephemeral	Cisco SIP Registration Datastore XML-based change notification.
IM and Presence	IM and Presence	Proprietary	TCP	6610	Ephemeral	Cisco Route Datastore XML-based change notification.

Table 140: IM and Presence Service Ports - Force Manual Sync/X.509 Certificate Update Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence (Intercluster Sync Agent)	IM and Presence (Intercluster Sync Agent)	TCP	TCP	37239	Ephemeral	Cisco Intercluster Sync Agent service uses this port to establish a socket connection for handling commands.

Table 141: IM and Presence Service Ports - ICMP Requests

From (Sender)	To (Listener)	Destination Port	Purpose
Endpoint/IM and Presence	IM and Presence	7	Internet Control M Protocol (ICMP) T number carries ec traffic. It does not port as indicated i heading.
IM and Presence	Endpoint/IM and Presence		

Table 142: Ports used for IM and Presence - Cisco Unified CM communication and IM and Presence Publisher - Subscriber communication

From (Sender)	To (Listener)	Transport Protocol	Destination / Listener	Source / Sender	Remarks
Cisco Unified Communications Manager	IM and Presence Publisher	TCP	1500	Bi-directional	Internal ID port for Database clients. Localhost traffic only.
Cisco Unified Communications Manager	IM and Presence Publisher	TCP	8443	Bi-directional	Provides access to Web administration.
Cisco Unified Communications Manager	IM and Presence Publisher	TCP	1090	Bi-directional	AMC RMI Object port. Cisco AMC Service for RTMT performance monitors, data collection, logging, and alerting.
Cisco Unified Communications Manager	IM and Presence Publisher	TCP	2555	Bi-directional	Bi-directional Real-time Information Services (RIS) database server. Connects to other RISDC services in the cluster to provide clusterwide real-time information.
Cisco Unified Communications Manager	IM and Presence Publisher	TCP	8500	Bi-directional	Internal port - cluster manager port used by the ipsec_mgr daemon for cluster replication of platform data (hosts) certificates.
Cisco Unified Communications Manager	IM and Presence Publisher	TCP	8600	Bi-directional	Config Agent heartbeat port
Cisco Unified Communications Manager	IM and Presence Publisher	UDP	123	Bi-directional	Network Time Protocol(NTP) used for time synchronization.

From (Sender)	To (Listener)	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence Publisher	IM and Presence Subscriber	UDP	50000	Bi-directional	Internal port. Localhost traffic only. LiveBus messaging port. TheIM and PresenceService uses this port for cluster communication.
IM and Presence Publisher	IM and Presence Subscriber	UDP	21999	Bi-directional	The port that Cisco Server Recovery Manager uses to communicate with its peer.
IM and Presence Publisher	Cisco Unified Communications Manager	TCP	4040	Bi-directional	DRF Master Agent server port that accepts connections from Local Agent, GUI, and CLI.
IM and Presence Publisher	Cisco Unified Communications Manager	TCP	8001	Bi-directional	Used while configuring persistent chat.
IM and Presence Publisher	Cisco Unified Communications Manager	TCP	6379	Bi-directional	Used while configuring managed file transfer (MFT).
IM and Presence Publisher	IM and Presence Subscriber	TCP	7	Bi-directional	Used while configuring external database (MSSQL).
IM and Presence Publisher	IM and Presence Subscriber	TCP	20075	Bi-directional	The port that Cisco Server Recovery Manager uses to provide admin RPC requests.
IM and Presence Publisher	IM and Presence Subscriber	TCP	8600	Bi-directional	Config Agent heartbeat port
IM and Presence Subscriber	IM and Presence Publisher	TCP	9005	Bi-directional	Cisco SIP Registration Datastore dual node presence redundancy group replication.
IM and Presence Subscriber	IM and Presence Publisher	TCP	9003	Bi-directional	Cisco Presence Datastore dual node presence redundancy group replication.
IM and Presence Subscriber	IM and Presence Publisher	TCP	20075	Bi-directional	The port that Cisco Server Recovery Manager uses to provide admin RPC requests.

From (Sender)	To (Listener)	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence Subscriber	IM and Presence Publisher	TCP	9004	Bi-directional	Cisco Login Datastore dual node presence redundancy group replication.
Cisco Unified Communications Manager	IM and Presence Publisher	TCP	5070	Bi-directional	Used on a call configuration
IM and Presence Publisher	IM and Presence Subscriber	TCP	44000	Bi-directional	Used on a call configuration

Table 143: On-a-call_Presence

From (Sender)	To (Listener)	Source Port	Destination Port	Protocol	Remarks
Cisco Unified Communications Manager	IM and Presence Publisher	[37240 – 61000]	5070	TCP	
IM and Presence Publisher	XMPP client (Jabber)	5222	64846	TCP	Client Access Port
IM and Presence Publisher	XMPP client (Jabber)	5222	56361	TCP	Client Access Port

Table 144: MS-SQL DB Configuration

From (Sender)	To (Listener)	Source Port	Destination Port	Protocol
IM and Presence Publisher	Database	[37240 – 61000]	7	TCP

Table 145: MS-SQL Persistent Chat Configuration

From (Sender)	To (Listener)	Source Port	Destination Port	Protocol
IM and Presence Publisher	Database	37240 – 61000	1433	TCP

Table 146: Managed File Transfer (MFT) Configuration

From (Sender)	To (Listener)	Source Port	Destination Port	Protocol
IM and Presence Publisher	External File Server	37240 – 61000	7	TCP

From (Sender)	To (Listener)	Source Port	Destination Port	Protocol
IM and Presence Publisher	External File Server	37240 – 61000	22	TCP
IM and Presence Publisher	External File Server	37240 – 61000	5432	TCP
IM and Presence Publisher	Database	54288 - 54292	5432	TCP

See the *Cisco Unified Serviceability Administration Guide* for information about SNMP.