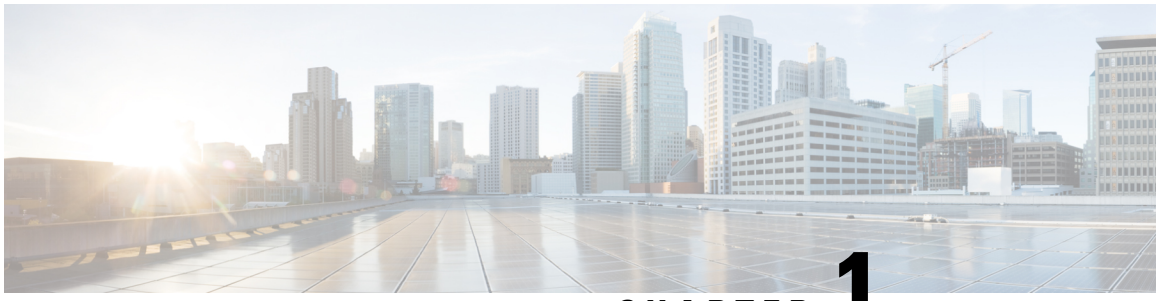
System Configuration Guide for Cisco Unified Communications Manager, Release 12.5(1)SU4 to 12.5(1)SU7

First Published: 2021-02-23

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

CONTENTS



CHAPTER 1

Introduction

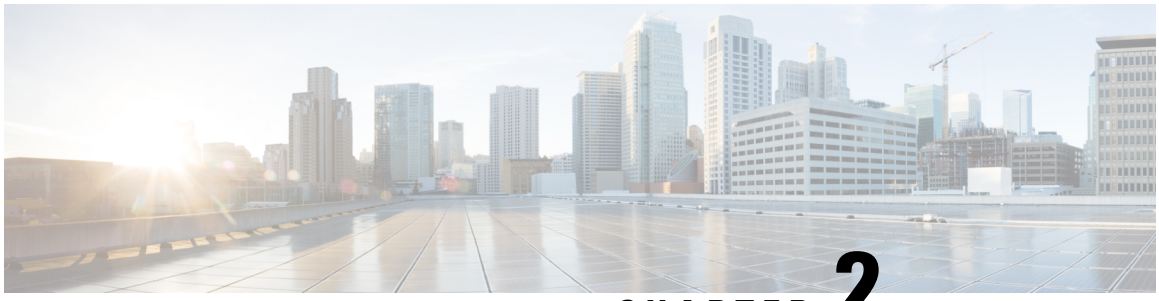
System Configuration Overview

This document contains basic configuration tasks for a post-install setup of the call control system. This document lets you configure system parameters, the dial plan and call routing, media resources, integrate applications and provisioning end users and endpoints. When you complete this document, you should have a basic condiguration that includes a configured dial plan, call routing, media resources, bandwidth management resources and basic security. In addition, users and endpoints are provisioned.

This document contains the following sections:

- System Components—Configure items such as system licensing, basic security, SSO, device pools, trunks, gateways, media resources and call admission control.
- Dial Plan—Configure dial plan and call routing elements.
- Integrate Applications—Integrate applications such as Cisco Emergency Responder, Cisco Unity Connection, and Cisco Expressway.
- Provisioning Users—Add users to your system.
- Provisioning Devices—Register devices for your users.

After completing the tasks in this guide, your system will be setup with users, devices, basic security and SSO. You can then proceed to configure Cisco solutions.



CHAPTER 2

New and Changed Information

New and Changed Information

The following table provides an overview of the significant changes to the features in this guide up to this current release. The table does not provide an exhaustive list of all changes made to the guide or of the new features up to this release.

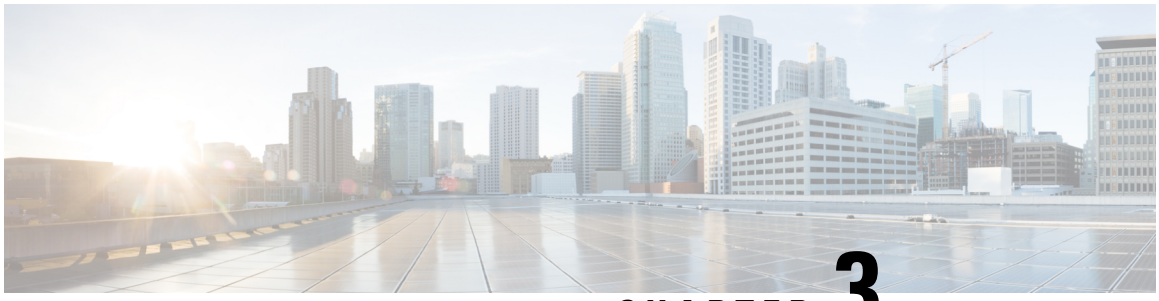
Table 1: New Features and Changed Behavior in Unified Communications Manager and IM and Presence Service

Feature or Change	Description	See	Date
Initial Release of Document for Release 12.5(1)SU4	—	—	February 22, 2021
Initial Release of Document for Release 12.5(1)SU7	—	—	December 8, 2022
Oauth enhancement - Eliminate refresh token dependency on CUCM publisher	The Unified CM supports updation of refresh token by subscriber node.	—	December 8, 2022

New and Changed Information

PART I

System Components



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.

Note The Unified CM running in Dual Stack mode supports satellite configured with IPv4 and IPv6 address.

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.

Note You cannot deploy a secure SIP trunk while running with a 90-day evaluation period. To deploy a secure SIP trunk, your system must have registered to a Smart Software Manager account with the **Allow export-controlled functionality** product registration token selected.

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.

	Command or Action	Purpose
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:
  - Authentication needed on HTTP or HTTPS proxy—Enable the checkbox if want to register to Cisco Smart Software Manager using authentication based proxy server.
  - IP Address/Host Name
  - Port—For HTTPS, use port 443.
  - User Name
  - Password

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.

	Command or Action	Purpose
		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 16	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 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.

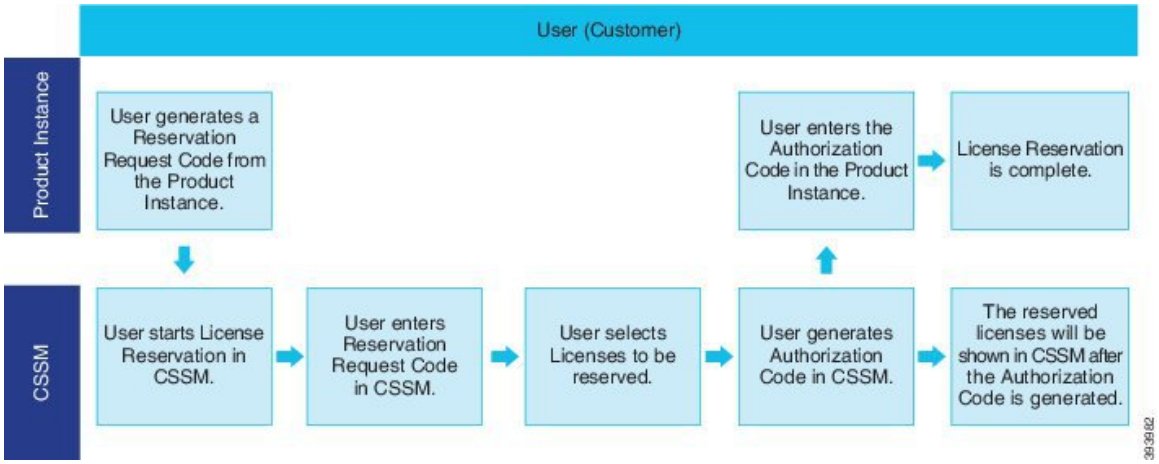
Note Usage information is updated once every 24 hours automatically. For more information on the fields and their configuration options, see the system Online Help.

Specific License Reservation

Specific License Reservation is a feature that is used in highly secure networks. It provides a method for customers to deploy a software license on a device (Product Instance - Unified Communications Manager) without communicating usage information.

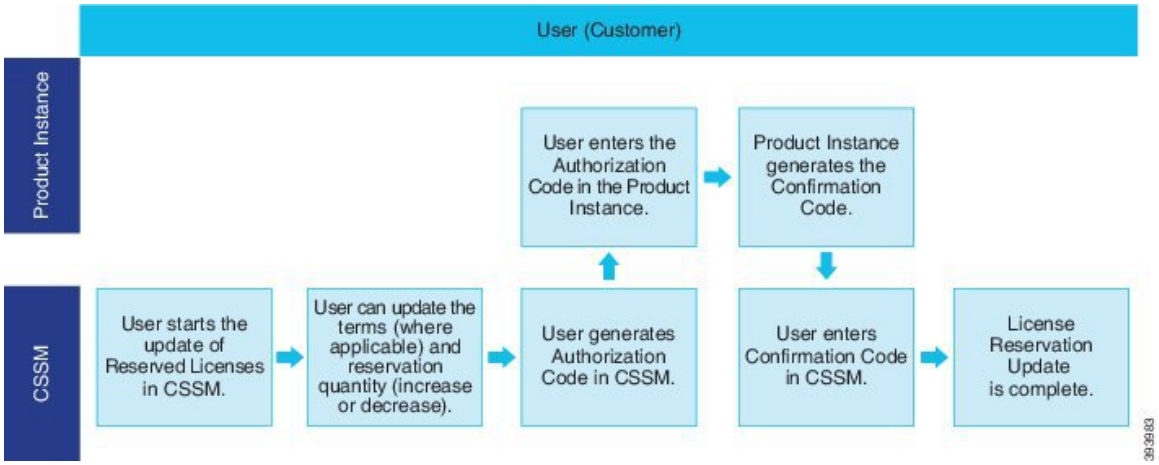
The user can specify and reserve perpetual or term-based licenses against the Unified Communications Manager product. After authorization code is exchanged, regular product synchronization is not required until there are changes in the reservation. Reserved licenses remain blocked in Cisco Smart Software Manager unless released from the product with a return code.

Figure 1: Reserve Licenses



An update or change in reserved licenses (increase or decrease) can be done on previously reserved licenses in Cisco Smart Software Manager. The new authorization code can be installed on the Product and a confirmation code can be obtained. The new changes remain in transit status unless confirmation code from the product is installed on the Cisco Smart Software Manager.

Figure 2: Update Reserve Licenses

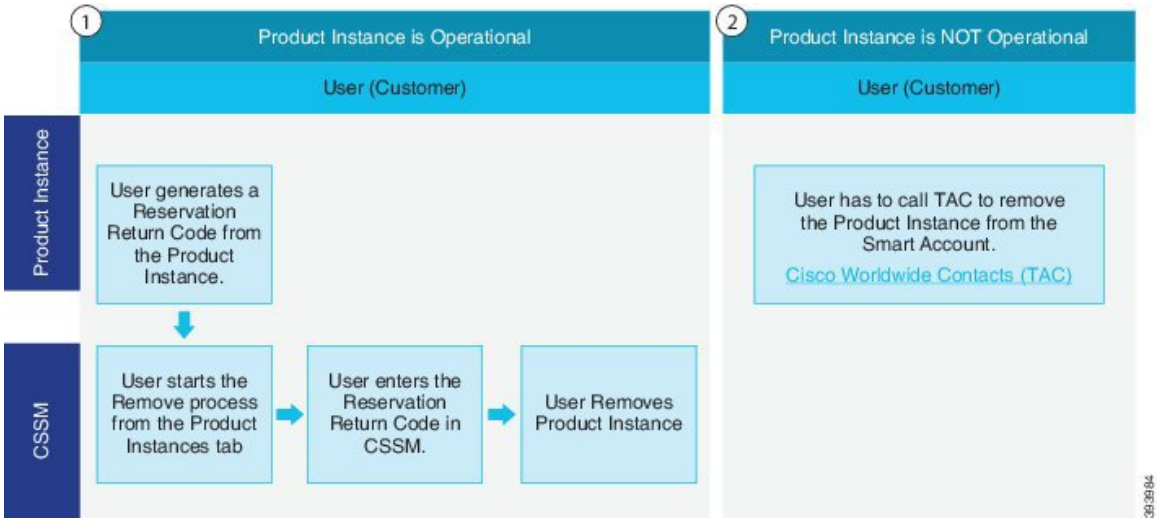


When licenses are reserved on a Product Instance (Unified Communications Manager), there are two ways to remove the product from the smart account and release all the licenses that are reserved for that Product Instance (Unified Communications Manager):

Product Instance is operational (graceful removal): User can return the Specific License Reservation authorization by creating a Reservation Return code on the Product Instance (which removes the Authorization Code) and then enter the Reservation Return code into Cisco Smart Software Manager.

Product Instance is not operational (failure/RMA or due to destroying the VM/container): User must contact TAC, who can remove the Product Instance from thier smart account.

Figure 3: Remove a Product Instance - Unified Communications Manager



Note User can use only the CLI configuration to enable Specific License Reservation.

Note When Specific License Reservation is enabled on Unified Communications Manager, voucher generation for cloud on-boarding will is not supported.

Customer who is entitled to License reservation feature on their Smart Account can reserve licenses from their virtual account, tie them to a devices UDI and use their device with these reserved licenses in a disconnected mode. The customer reserves specific licenses and counts for a UDI from their virtual account. The following options describe the new functionality and design elements for Specific License Reservation:

- license smart reservation enable
- license smart reservation disable
- license smart reservation request
- license smart reservation cancel
- update license reservation
- license smart reservation install "<authorization-code>"
- license smart reservation install-file <url>
- license smart reservation return
- license smart reservation return-authorization "<authorization-code>"

Specific License Reservation Task Flow

Complete these tasks to reserve specific licenses for Unified Communications Manager.

license smart reservation enable

Use this procedure to enable Specific License Reservation.

Before you begin

Unified Communications Manager is unregistered with Cisco Smart Software Manager or satellite.

Procedure

From Cisco Unified CM Admin Console execute the below CLI command.

- license smart reservation enable

license smart reservation request

Use this procedure to generate reservation request code generate request code from Unified Communications Manager product.

Before you begin

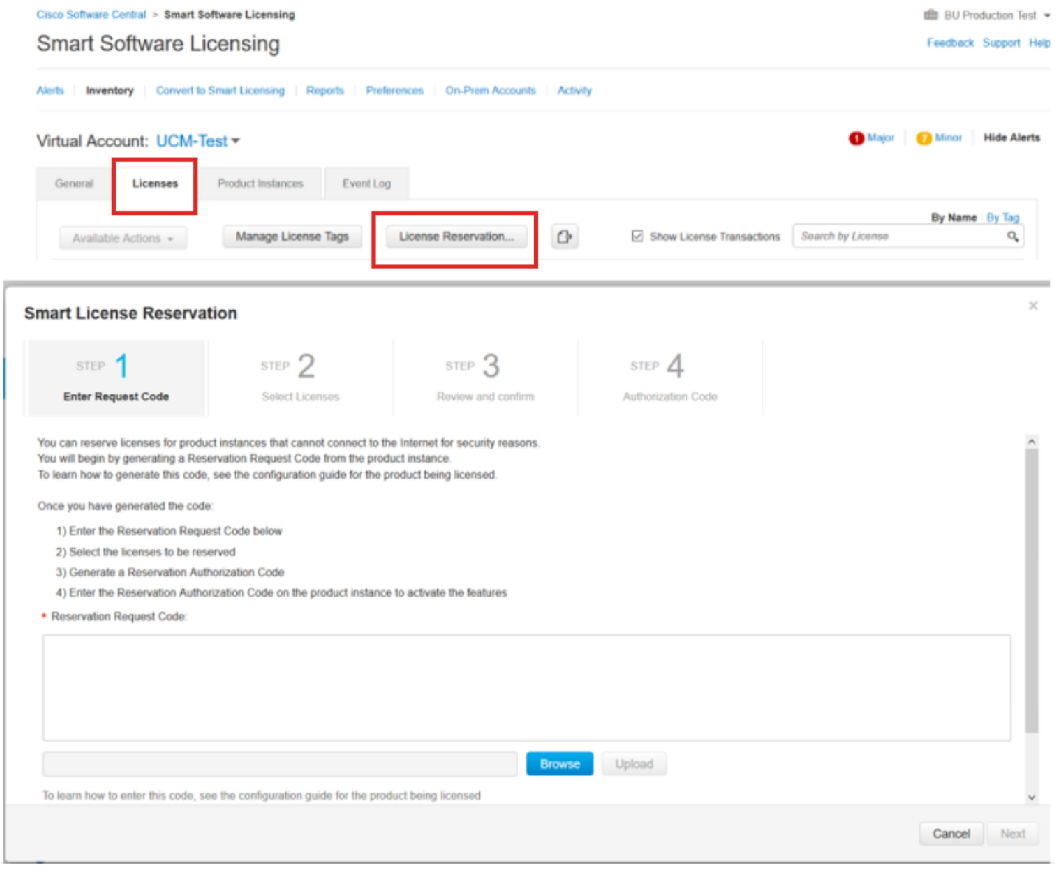
Make sure Unified Communications Manager Registration Status is Reservation in progress, by executing **license smart reservation enable**.

command

Procedure

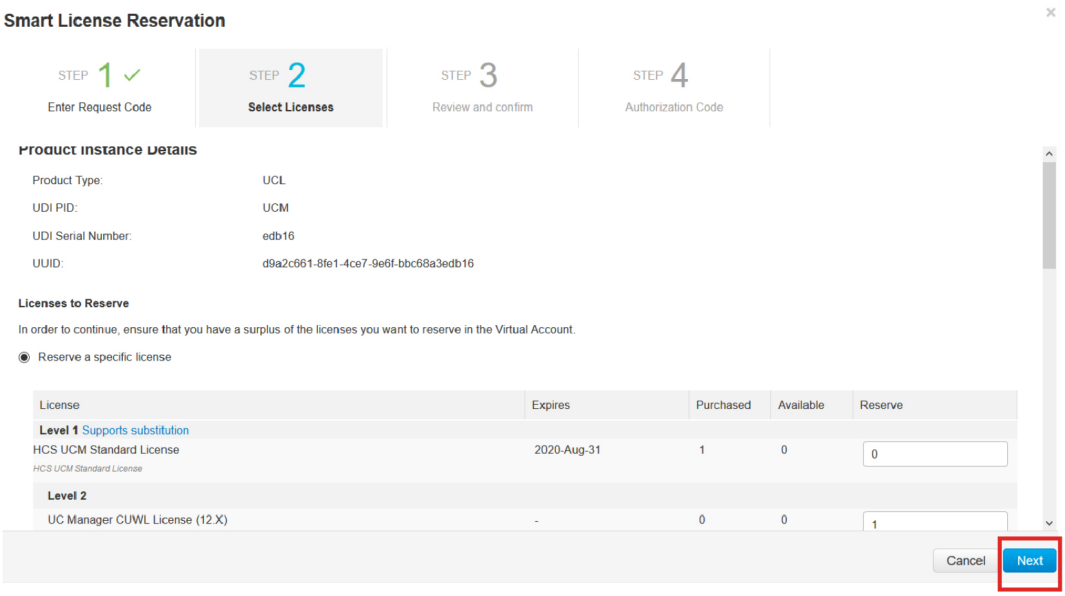
Step 1 From Cisco Unified CM Admin Console execute*license smart reservation request* command.

Step 2 Log into CSSM [Cisco Smart Software manager] and enter the reservation request code.



450364

Step 3 Select the licenses that have to be reserved for this device and generate Authorization code.



450365

Step 4 Copy the authorization code to the product instance and execute the **license smart reservation install "<authorization-code>** "command to install.

450366

license smart reservation install "<authorization-code>"

Use this procedure to install license reservation authorization-code generated from Cisco Smart Software Manager.

Before you begin

Make Unified Communications Manager Registration Status is Reservation In Progress, by executing commands in below sequence:

- **license smart reservation enable**
- **license smart reservation request**

Procedure

From Cisco Unified CM Admin Console execute the below CLI command.

- license smart reservation install "<authorization-code>"

license smart reservation install-file <url>

Use this procedure to install the license reservation authorization-code file generated on the Cisco Smart Software Manager.

Before you begin

Make sure Unified Communications Manager registration status is Reservation In Progress, by executing commands in below sequence.:

- **license smart reservation enable**
- **license smart reservation request**

Note url is mandatory Path to the authorization-code file on SFTP server in below format:

sftp://<HostName/IP>:<port>/<Path to Authorization-Code file>

Procedure

From Cisco Unified CM Admin Console execute the below CLI command.

- license smart reservation install-file <url>

Additional Tasks with Specific License Reservation

The following additional tasks are available on Unified Communications Manager for Specific License Reservation:

license smart reservation disable

Use this procedure to disable specific license reservation.

Before you begin

Specific License Reservation is enabled on Unified Communications Manager

Procedure

From Cisco Unified CM Admin Console execute the below CLI command.

- license smart reservation disable

update license reservation

Use this procedure to update the license reservation for your product instance and get a new authorization code.

Before you begin

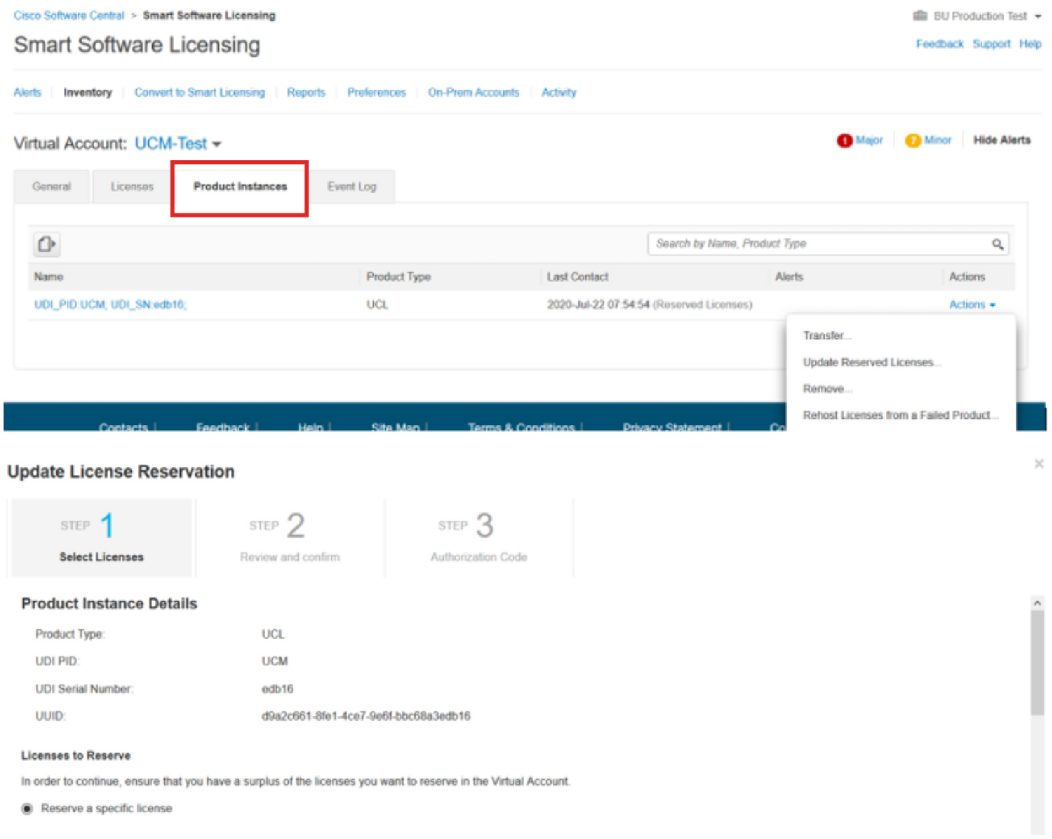
Make sure Unified Communications Manager Registration Status is Registered- Specific License Reservation by executing commands in below sequence:

- license smart reservation enable
- license smart reservation request
- license smart reservation install "<authorization-code>"

Note License borrowing from a higher tier does not happen automatically when a Specific License Reservation is enabled on Unified Communications Manager. License Reservation has to be updated manually to the Unified Communications Manager license consumption/usage.

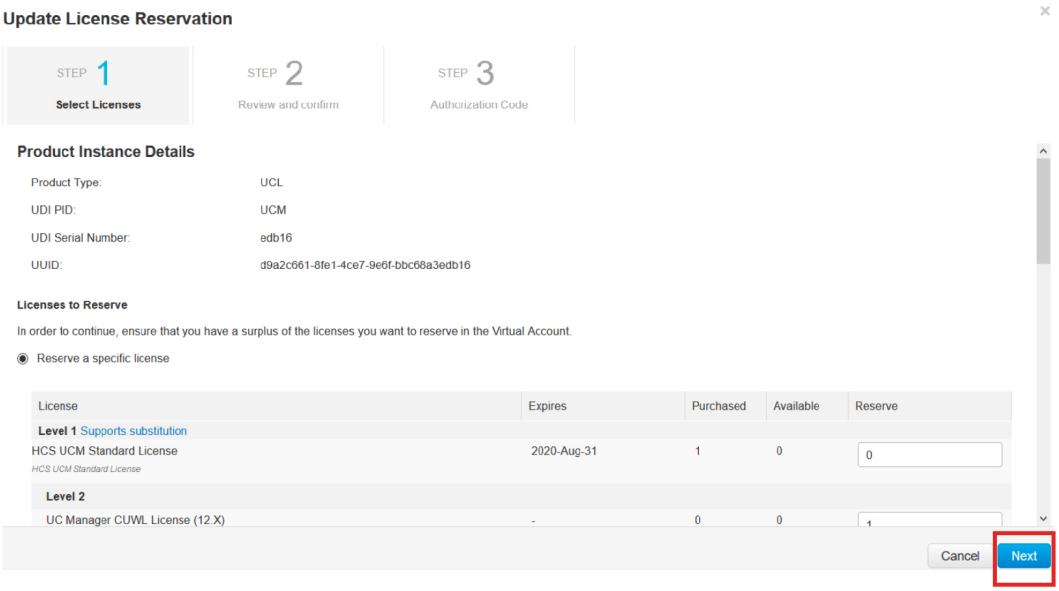
Procedure

Step 1 Select Update Reserved Licenses from Actions drop-down list next to the Product Instance that you wish to update reservation on CSSM.



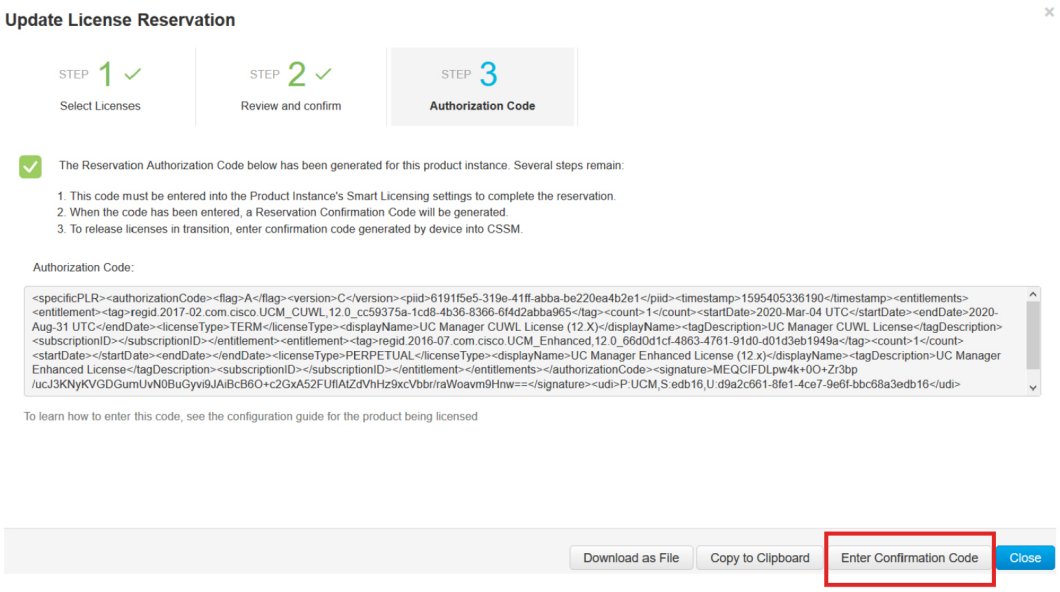
450363

Step 2 Update the reservation (Add/Remove/Update licenses for this product instance) and generate authorization code.



450367

Step 3 Copy the authorization code to the product instance and execute the **license smart reservation install "<authorization-code>"** command to install.

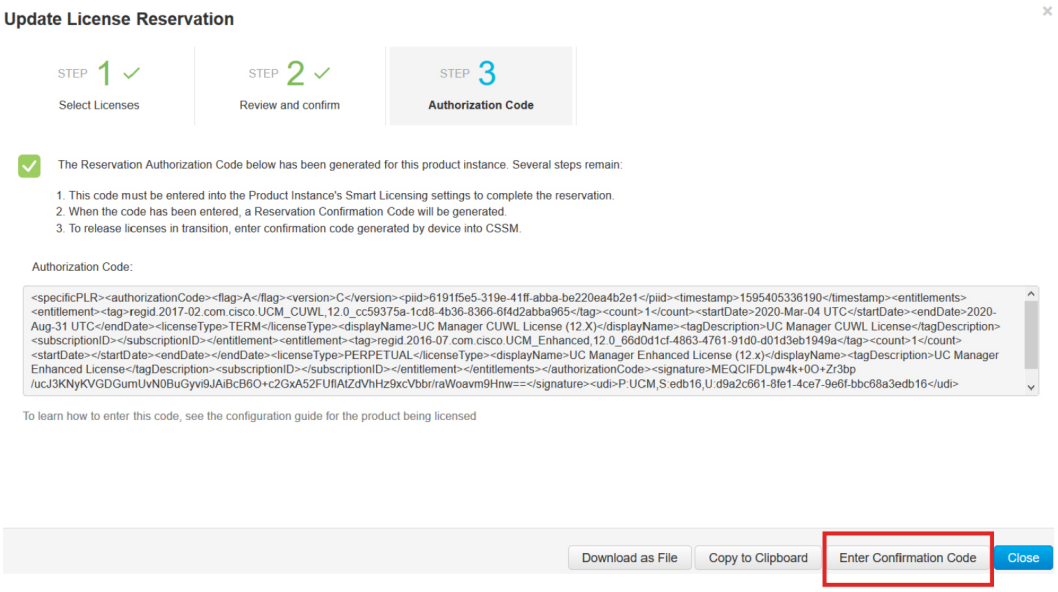


450362

Step 4 Confirmation code is generated on the product after the authorization code is successfully installed.

450368

Step 5 Copy the confirmation code to the CSSM and enter to complete the reservation update.



450362

license smart reservation cancel

Use this procedure to cancel the reservation process before the authorization code from Cisco Smart Software Manager against CUCM request code is installed.

Before you begin

Make sure Unified Communications Manager Registration Status is Reservation In Progress, by executing commands in below sequence:

- **license smart reservation enable**
- **license smart reservation request**

Procedure

From Cisco Unified CM Admin Console execute the below CLI command.

- license smart reservation cancel

license smart reservation return

Use this procedure to generate a return code that must be entered into the Cisco Smart Software Manager to return the licenses to the virtual account pool and remove the product instance from CSSM.

Before you begin

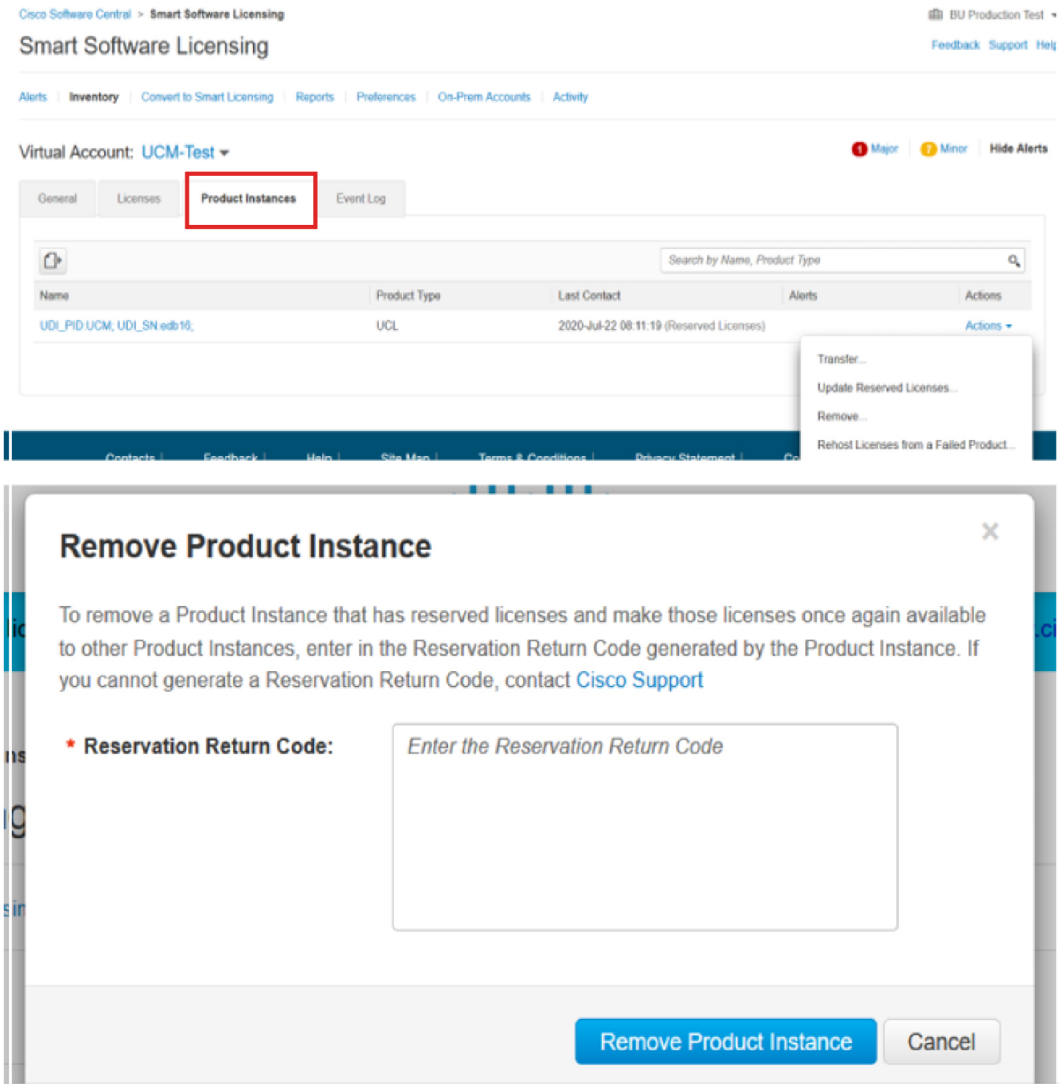
Make sure Unified Communcations Manger Registration Status is Registered- Specific License Reservation by executing commands in below sequence:

- **license smart reservation enable**
- **license smart reservation request**
- **license smart reservation install "<authorization-code>"**

Procedure

Step 1 From Cisco Unified CM Admin Console execute the license smart reservation return command.

Step 2 Copy the reservation return code to CSSM and remove the product instance.



license smart reservation return-authorization "<authorization-code>"

Use this procedure to generate a return code for the authorization code not installed yet. The return code must be entered into the Cisco Smart Software Manager to return the licenses to the virtual account pool and remove the product instance from CSSM.

Before you begin

Make sure Unified Communcations Manager Registration Status is Reservation In Progress, by executing commands in below sequence:

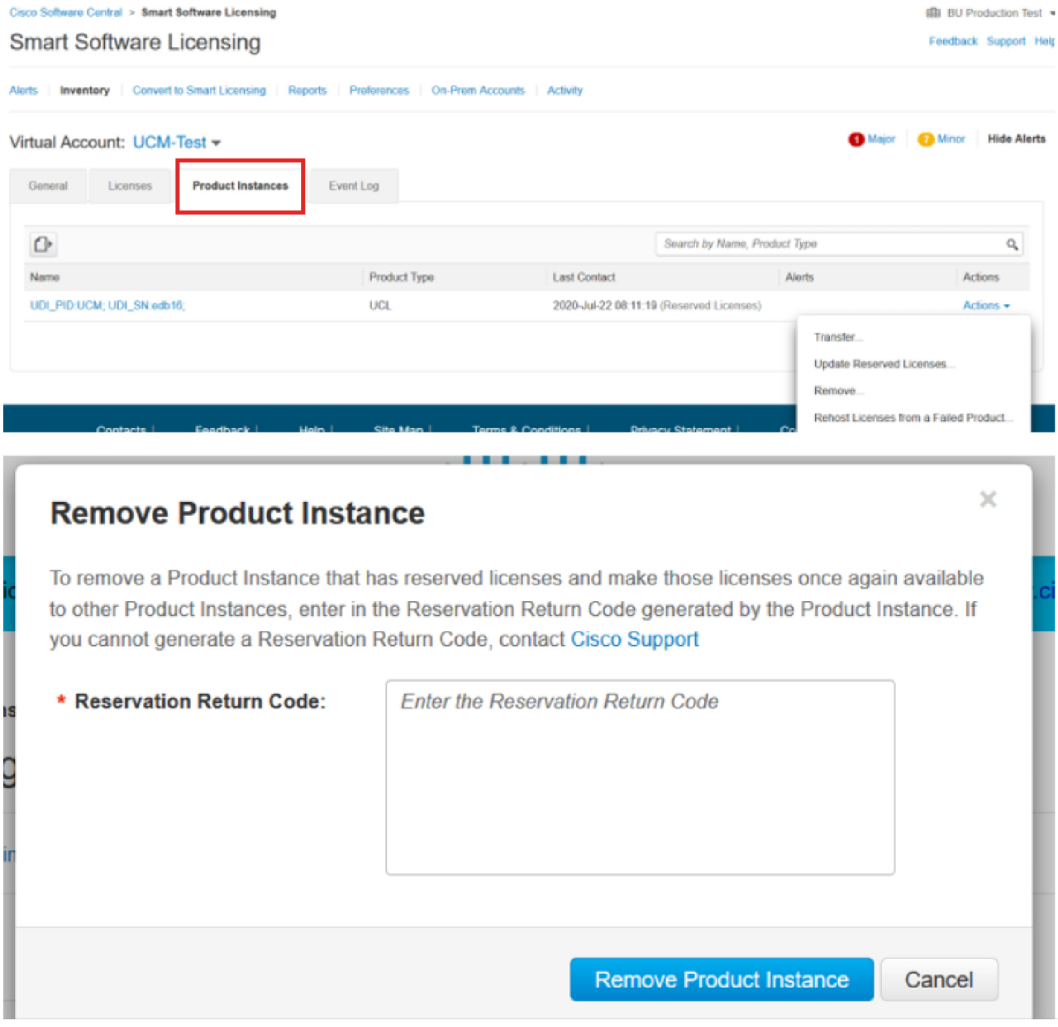
- **license smart reservation enable**

- **license smart reservation request**

Procedure

Step 1 From Cisco Unified CM Admin Console execute the license smart reservation return-authorization "<authorization-code>" command.

Step 2 Copy the reservation return code to CSSM and remove the product instance.



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.

Smart Licensing Export Compliance

Smart Licensing provides a method that allows user to use export control features. In the connected state, use export control feature using the registration process. In the disconnected state, use export control feature using Smart License Reservation.

This export control feature is a solution for customers with a smart account, for whom Export Restrictions apply. This feature allows the user to request a regulatory Export License that is granted in the Cisco Smart Software Manager or the satellite and enable the export restricted feature on Cisco Unified Communications Manager.

The following options describe the new functionality and design elements for the export control feature:

- license smart export request local <exportfeaturename>
- license smart export return local <exportfeaturename>
- license smart export cancel

Export Control Task Flow

Complete the following tasks to export control licenses for Cisco Unified Communications Manager.

license smart export request local <exportfeaturename>

This command allows user with Smart Account for whom Export Restrictions apply, to request a regulatory export license from Cisco Smart Software Manager or satellite.

The command returns an export authorization key if regulatory export license is available on Cisco Smart Software Manager or satellite and enable export restricted feature on the product.

Before you begin

Cisco Unified Communications Manager is registered with Cisco Smart Software Manager or satellite. Make sure <CUCM Export Restricted Authorization Key> license is available on Cisco Smart Software Manager.

Procedure

From Cisco Unified CM Admin Console, execute the following CLI command:

- license smart export request local <exportfeaturename>

license smart export return local <exportfeaturename>

The command allows to return a previously requested export restricted license to Cisco Smart Software Manager or satellite. The export authorization key for the export restricted feature is removed from the system.

Before you begin

Export authorization key is generated for the feature.

Procedure

From Cisco Unified CM Admin Console, execute the following CLI command:

- license smart export return local <exportfeaturename>

license smart export cancel

This command allows user with Smart Account for whom Export Restrictions apply, to cancel the automatic retry of previously failed export request or return from Cisco Smart Software Manager or satellite.

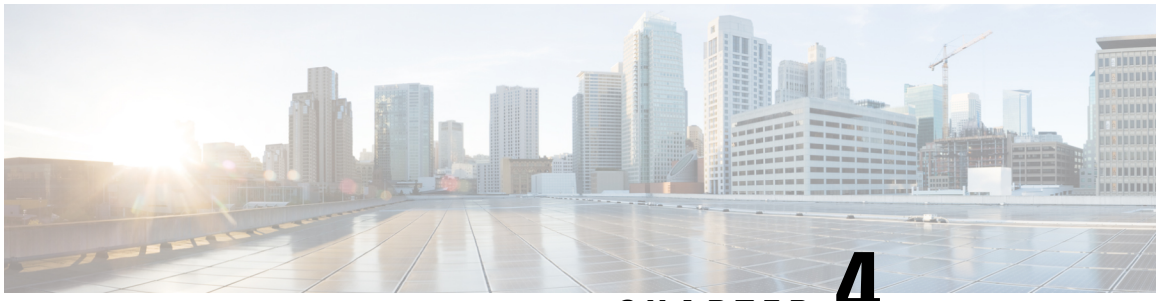
Before you begin

Cisco Unified Communications Manager is registered with Cisco Smart Software Manager or satellite.

Procedure

From Cisco Unified CM Admin Console, execute the following CLI command:

- license smart export cancel



CHAPTER 4

Configure Enterprise Parameters and Services

Enterprise Parameters Overview

Enterprise parameters provide default settings that apply to all devices and services in the same cluster. A cluster comprises a set of Cisco Unified Communications Managers that share the same database. When you install a new Cisco Unified Communications Manager, it uses the enterprise parameters to set the initial values of its device defaults.

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

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 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.

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.

System Parameters Task Flow

Before you begin

Set up your Unified Communications Manager node and port settings.

Procedure

	Command or Action	Purpose
Step 1	Configure Enterprise Parameters, on page 35.	Configure the system-wide parameters that are required for an initial setup of your Unified Communications Manager node.
Step 2	Activate Essential Services, on page 40.	You can activate services on the node using Cisco Unified Serviceability.
Step 3	Configure Service Parameters, on page 42.	Configure service parameters for the publisher and subscriber nodes in the cluster.

Configure Enterprise Parameters

Use this procedure to edit enterprise-level parameters for your deployment. You can use this to set enterprise-level settings, such as your Organization Top-Level Domain or Cluster Fully Qualified Domain Name.

Note If you edit a parameter in Cisco Unified CM Administration, the new setting also reflects in Cisco Unified CM, IM and Presence Administration.

Procedure

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

The **Enterprise Parameters** window displays the list of enterprise parameters.

Step 2 Edit any of the parameter settings.

For parameter descriptions, click the parameter name in the GUI. For more information on a list of common enterprise parameters, see Common Enterprise Parameters, on page 35.

Step 3 Click **Save**.

Step 4 Click **Reset**, and then click **OK** to reset all devices.

Note Most parameters require that you reset devices after saving the setting. If you have registered devices, we recommend completing all your configuration changes before resetting devices.

You can reset every device pool in the system to reset all the devices.

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	

Parameter Name	Description
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	
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.

Parameter Name	Description
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	
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	

Parameter Name	Description
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	
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).

Parameter Name	Description
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. **Important** This feature is applicable for Release 12.5(1)SU7 and 14SU3 onwards. Along with the publisher, the subscriber node also has the access to update the refresh token on the requester node database and the same will be replicated across the cluster. This is a required field. Default: Disabled.
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.

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 40
- Recommended Services for Subscriber Nodes, on page 41

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

Type	Service Name
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 40.

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.

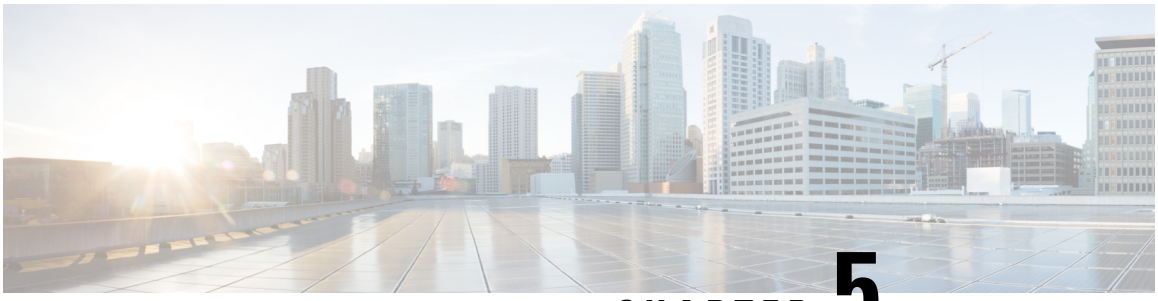
d) Click the (**?**) icon in the **Service Parameter Configuration** window to view a list of service parameters along with their descriptions.

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 5

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 51.

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 47	Configure the operating system with support for IPv6 addresses.
Step 2	Configure Server for IPv6, on page 47	Configure the servers in your cluster with IPv6 addresses.
Step 3	Enable IPv6, on page 48	Configure enterprise parameters that enable the system for IPv6.
Step 4	Perform any of the following: • Configure IP Addressing Preference for Cluster, on page 48 • Configure IP Addressing Preferences for Devices, on page 49	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 50	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 48
- Configure IP Addressing Preferences for Devices, on page 49

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 50.

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 51.

Restart Services

After configuring your system for IPv6, restart essential services.

Procedure

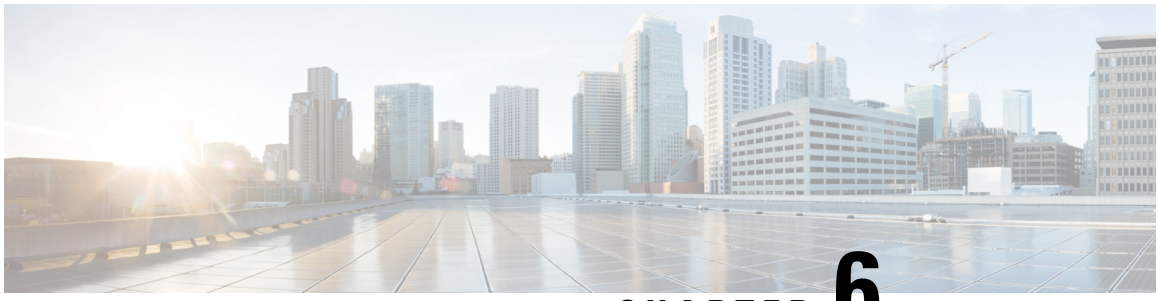
Step 1 Log into Cisco Unified Serviceability and choose **Tools** > **Control Center - Feature Services**.

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 6

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 46.

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 52	Configure a SIP Profile that supports both IPv4 and IPv6 stacks simultaneously.
Step 2	Apply ANAT to SIP Phone, on page 53	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 53	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 53	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 89.

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

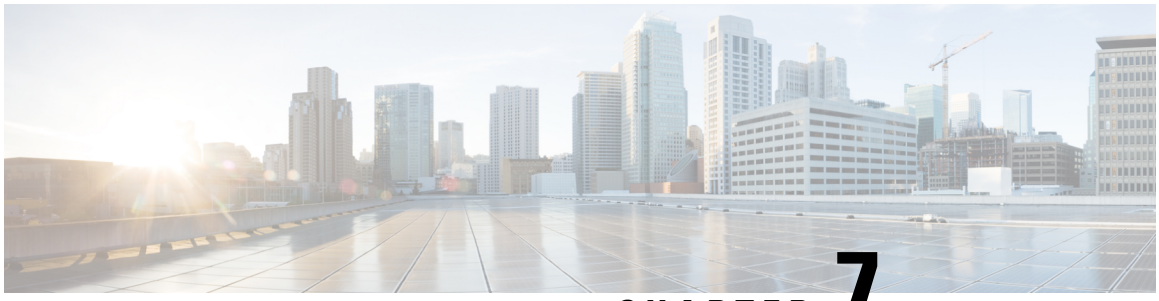
Step 1 Log into Cisco Unified Serviceability and choose **Tools** > **Control Center - Feature Services**.

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**.



CHAPTER 7

Configure Basic Security

About Security Configuration

This section provides information about the basic security configuration tasks that you have to perform to set up Cisco Unified Communications Manager.

Security Configuration Tasks

Perform the following tasks to set up the basic security configurations:

Enable Mixed Mode for Cluster

Use this procedure to enable mixed mode in the cluster.

Procedure

Step 1 Log in to the Command Line Interface on the publisher node.

Step 2 Run the **utils ctl set-cluster mixed-mode** CLI command.

Note Make sure that Communications Manager is registered with the Cisco Smart Software Manager or Cisco Smart Software Manager satellite and the Registration Token received from the Smart account or Virtual account has Allow export-controlled functionality enabled while registering with this cluster.

Download Certificates

Use the download certificates task to have a copy of your certificate or upload the certificate when you submit a CSR request.

Procedure

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

Step 2 Specify search criteria and then click **Find**.

Step 3 Choose the required file name and Click **Download**.

Generate a Certificate Signing Request

Generate a Certificate Signing Request (CSR) which is a block of encrypted text that contains certificate application information, public key, organization name, common name, locality, and country. A certificate authority uses this CSR to generate a trusted certificate for your system.

Note If you generate a new CSR, you overwrite any existing CSRs.

Procedure

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

Step 2 Click **Generate CSR**.

Step 3 Configure fields on the **Generate Certificate Signing Request** window. See the online help for more information about the fields and their configuration options.

Step 4 Click **Generate**.

Download a Certificate Signing Request

Download the CSR after you generate it and have it ready to submit to your certificate authority.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.
Step 2 Click **Download CSR**.
Step 3 Choose the certificate name from the **Certificate Purpose** drop-down list.
Step 4 Click **Download CSR**.
Step 5 (Optional) If prompted, click **Save**.

Upload Root Certificate for Third-Party CAs

Upload the CA root certificate to the CAPF-trust store and the Unified Communications Manager trust store to use an external CA to sign LSC certificates.

Note Skip this task if you don't want to use a third-party CA to sign LSCs.

Procedure

Step 1 From Cisco Unified OS Administration choose **Security** > **Certificate Management**.
Step 2 Click **Upload Certificate/Certificate chain**.
Step 3 From the **Certificate Purpose** drop-down list, choose **CAPF-trust**.
Step 4 Enter a **Description** for the certificate. For example, **Certificate for External LSC-Signing CA**.
Step 5 Click **Browse**, navigate to the file, and then click **Open**.
Step 6 Click **Upload**.
Step 7 Repeat this task, uploading certificates to **callmanager-trust** for the **Certificate Purpose**.

TLS Prerequisites

Before you configure the minimum TLS version, make sure that your network devices and applications both support the TLS version. Also, make sure that they are enabled for TLS that you want to configure with Unified Communications Manager and IM and Presence Services. If you have any of the following products deployed, confirm that they meet the minimum TLS requirement. If they do not meet this requirement, upgrade those products:

- Skinny Client Control Protocol (SCCP) Conference Bridge
- Transcoder
- Hardware Media Termination Point (MTP)
- SIP Gateway
- Cisco Prime Collaboration Assurance

- Cisco Prime Collaboration Provisioning
- Cisco Prime Collaboration Deployment
- Cisco Unified Border Element (CUBE)
- Cisco Expressway
- Cisco TelePresence Conductor

You will not be able to upgrade conference bridges, Media Termination Point (MTP), Xcoder, Prime Collaboration Assurance, and Prime Collaboration Provisioning.

Note If you are upgrading from an earlier release of Unified Communications Manager, make sure that all your devices and applications support the higher version of TLS before you configure it. For example, Unified Communications Manager and IM and Presence Services, Release 9.x supports TLS 1.0 only.

Set Minimum TLS Version

By default, Unified Communications Manager supports a minimum TLS version of 1.0. Use this procedure to reset the minimum supported TLS version for Unified Communications Manager and the IM and Presence Service to a higher version, such as 1.1 or 1.2.

Make sure that the devices and applications in your network support the TLS version that you want to configure. For details, see TLS Prerequisites, on page 57.

Procedure

Step 1 Log in to the **Command Line Interface**.

Step 2 To confirm the existing TLS version, run the **show tls min-version** CLI command.

Step 3 Run the **set tls min-version** <*minimum*> CLI command where <*minimum*> represents the TLS version.

For example, run **set tls min-version 1.2** to set the minimum TLS version to 1.2.

Step 4 Perform Step 3 on all Unified Communications Managerand IM and Presence Service Service cluster nodes.

Set TLS Ciphers

You can disable the weaker cipher, by choosing available strongest ciphers for the SIP interface. Use this procedure to configure the ciphers that Unified Communications Manager supports for establishing TLS connections.

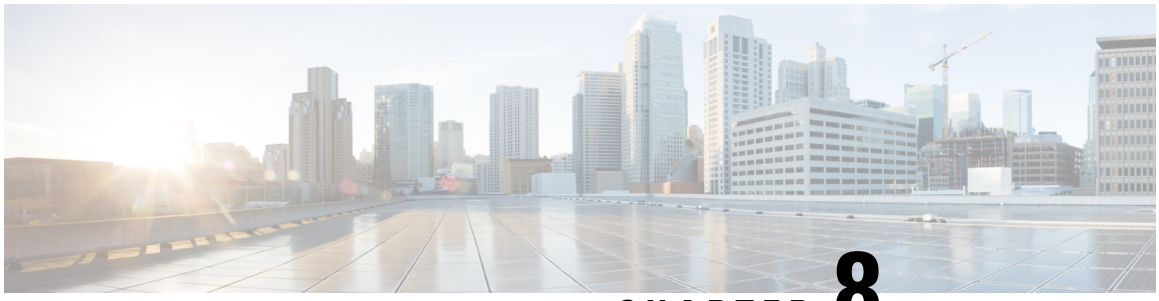
Procedure

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

Step 2 In **Security Parameters**, configure a value for the **TLS Ciphers** enterprise parameter. For help on the available options, refer to the enterprise parameter online help.

Step 3 Click **Save**.

Note All TLS Ciphers will be negotiated based on client cipher preference



CHAPTER 8

Configure Single Sign-On

About SAML SSO Solution

Important When deploying Cisco Jabber with Cisco Webex meeting server, Unified Communications Manager and the Webex meeting server must be in the same domain.

SAML is an XML-based open standard data format that enables administrators to access a defined set of Cisco collaboration applications seamlessly after signing into one of those applications. SAML describes the exchange of security related information between trusted business partners. It is an authentication protocol used by service providers (for example, Unified Communications Manager) to authenticate a user. SAML enables exchange of security authentication information between an Identity Provider (IdP) and a service provider.

SAML SSO uses the SAML 2.0 protocol to offer cross-domain and cross-product single sign-on for Cisco collaboration solutions. SAML 2.0 enables SSO across Cisco applications and enables federation between Cisco applications and an IdP. SAML 2.0 allows Cisco administrative users to access secure web domains to exchange user authentication and authorization data, between an IdP and a Service Provider while maintaining high security levels. The feature provides secure mechanisms to use common credentials and relevant information across various applications.

The authorization for SAML SSO Admin access is based on Role-Based Access Control (RBAC) configured locally on Cisco collaboration applications.

SAML SSO establishes a Circle of Trust (CoT) by exchanging metadata and certificates as part of the provisioning process between the IdP and the Service Provider. The Service Provider trusts the IdP's user information to provide access to the various services or applications.

Important Service providers are no longer involved in authentication. SAML 2.0 delegates authentication away from the service providers and to the IdPs.

The client authenticates against the IdP, and the IdP grants an Assertion to the client. The client presents the Assertion to the Service Provider. Since there is a CoT established, the Service Provider trusts the Assertion and grants access to the client.

SAML SSO Configuration Task Flow

Complete these tasks to configure Unified Communications Manager for SAML SSO.

Before you begin

SAML SSO configuration requires that you configure the Identity provider (IdP) at the same time that you configure Unified Communications Manager. For IdP-specific configuration examples, see:

- Active Directory Federation Services
- Okta
- Open Access Manager
- PingFederate

Note The above links are examples only. Refer to your IdP documentation for official documentation.

Procedure

	Command or Action	Purpose
Step 1	Export UC Metadata from Cisco Unified Communications Manager, on page 63	To create a trust relationship, you must exchange metadata files between Unified Communications Manager and the IdP.
Step 2	Configure SAML SSO on the Identity Provider (IdP)	Complete the following tasks: • Upload the UC metadata file that was exported from Unified Communications Manager in order to complete the Circle of Trust relationship. • Configure SAML SSO on the IdP • Export an IdP metadata file. This file will be imported into the Unified Communications Manager
Step 3	Enable SAML SSO in Cisco Unified Communications Manager	Import your IdP metadata and enable SAML SSO in Unified Communications Manager.
Step 4	Restart Cisco Tomcat Service, on page 65	Before and After you enable SSO, you must restart the Cisco Tomcat service on all cluster nodes where SSO is enabled.
Step 5	Verify the SAML SSO Configuration, on page 65	Verify that SAML SSO has been configured successfully.

Export UC Metadata from Cisco Unified Communications Manager

Use this procedure to export a UC metadata file from the Service Provider (Unified Communications Manager). The metadata file will be imported into the Identity Provider (IdP) in order to build a Circle of Trust relationship.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **SAML Single Sign-On**

Step 2 From the **SAML Single Sign-On** window, choose one of the options for the **SSO Mode** field:

- **Cluster wide**—A single SAML agreement for the cluster.

  Note If you choose this option, ensure that Tomcat servers for all the nodes in the cluster have the same certificate, which is the multi-server SAN certificate.

- **Per Node**—Each node has a separate SAML agreement.

Step 3 From the **SAML Single Sign-On** window, choose one of the options for the **Certificate** field.

- **Use system generated self-signed certificate**
- **Use Tomcat certificate**

Step 4 Click **Export All Metadata** to export the metadata file.

Note If you choose the **Cluster wide** option in Step 3, a single metadata XML file appears for a cluster for download. However, if you choose the **Per Node** option, one metadata XML file appears for each node of a cluster for download.

What to do next

Complete the following tasks on the IdP:

- Upload the UC metadata file that was exported from Unified Communications Manager
- Configure SAML SSO on the IdP
- Export an IdP metadata file. This file will be imported into the Unified Communications Manager in order to complete the Circle of Trust relationship.

Enable SAML SSO in Cisco Unified Communications Manager

Use this procedure to enable SAML SSO on the Service Provider (Unified Communications Manager). This process includes importing the IdP metadata onto the Unified Communications Manager server.

Important Cisco recommends that you restart Cisco Tomcat service after enabling or disabling SAML SSO.

Note The Cisco CallManager Admin, Unified CM IM and Presence Administration, Cisco CallManager Serviceability, and Unified IM and Presence Serviceability services are restarted after you enable or disable SAML SSO.

Before you begin

Prior to completing this procedure, make sure of the following:

- You require an exported metadata file from your IdP.
- Make sure that the end-user data is synchronized to the Unified Communications Manager database
- Verify that the Unified Communications Manager IM and Presence Cisco Sync Agent service has completed data synchronization successfully. Check the status of this test in **Cisco Unified CM IM and Presence Administration** by choosing **Diagnostics** > **System Troubleshooter** The "Verify Sync Agent has sync'ed over relevant data (e.g. devices, users, licensing information)" test indicates a "Test Passed" outcome if data synchronization has completed successfully
- At least one LDAP synchronized user is added to the Standard CCM Super Users group to enable access to Cisco Unified Administration. For more information about synchronizing end-user data and adding LDAP-synchronized users to a group, see the "System setup" and "End user setup" sections in the Unified Communications Manager Administration Guide

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **SAML Single Sign-On**.

Step 2 Click **Enable SAML SSO** and then click **Continue**.

A warning message notifies you that all server connections will be restarted.

Step 3 If you have configured the **Cluster wide** SSO mode, click the **Test for Multi-server tomcat certificate** button. Otherwise, you can skip this step.

Step 4 Click **Next**.

A dialog box that allows you to import IdP metadata appears. To configure the trust relationship between the IdP and your servers, you must obtain the trust metadata file from your IdP and import it to all your servers.

Step 5 Import the metadata file that you exported from your IdP:

a) **Browse** to locate and select your exported IdP metadata file.
b) Click **Import IdP Metadata**.
c) Click **Next**.
d) At the **Download Server Metadata and Install on IdP** screen, click **Next**.

Note The **Next** button is enabled only if the IdP metadata file is successfully imported on at least one node in the cluster.

Step 6 Test the connection and complete the configuration:

a) In the **End User Configuration** window, choose a user that is LDAP-synchronized and has the permission as "Standard CCM Super User" from the **Permissions Information** list box

b) Click **Run Test**.

The IdP login window appears.

Note You cannot enable SAML SSO until the test succeeds.

c) Enter a valid username and password.

After successful authentication, the following message is displayed:

```
SSO Test Succeeded
```

Close the browser window after you see this message.

If the authentication fails, or takes more than 60 seconds to authenticate, a "Login Failed" message appears on the IdP login window. The following message is displayed on the SAML Single Sign-On window:

```
SSO Metadata Test Timed Out
```

To attempt logging in to the IdP again, select another user and run another test.

d) Click **Finish** to complete the SAML SSO setup.

SAML SSO is enabled and all the web applications participating in SAML SSO are restarted. It may take one to two minutes for the web applications to restart.

Restart Cisco Tomcat Service

Before and after enabling or disabling SAML Single Sign-On, restart the Cisco Tomcat service on all Unified CM and IM and Presence Service cluster nodes where Single Sign-On is running.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Run the `utils service restart Cisco Tomcat` CLI command.

Step 3 Repeat this procedure on all cluster nodes where Single Sign-On is enabled.

Verify the SAML SSO Configuration

After you configure SAML SSO on both the Service Provider (Unified Communications Manager) and on the IdP, use this procedure on Unified Communications Manager to confirm that the configuration works.

Before you begin

Confirm the following:

- The **SAML Single Sign-On Configuration** window in Unified CM Administration shows that you have successfully imported the **IdP Metadata Trust** file.
- The Service Provider metadata files are installed on the IdP.

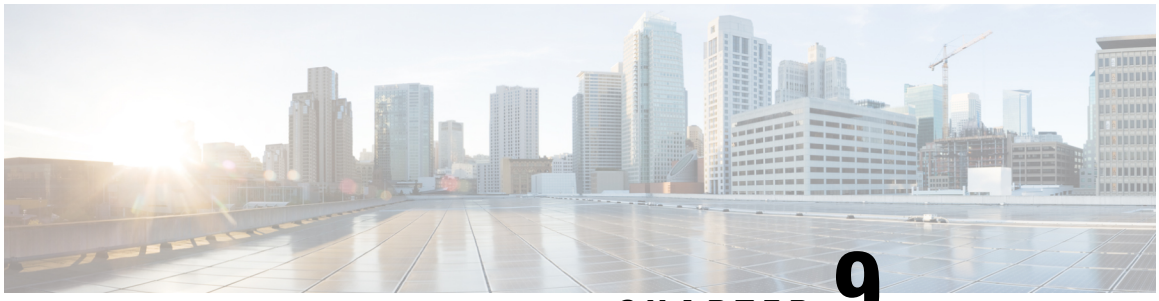
Procedure

Step 1 From the Cisco Unified CM Administration, choose **System** > **SAML Single Sign-On** and the **SAML Single Sign-On Configuration** window opens, click **Next**.

Step 2 Choose an administrative user form the **Valid Administrator Usernames** area and click the **Run SSO Test…** button.

Note The user for the test must have administrator rights and has been added as a user on the IdP server. The Valid Administrator Usernames area displays a list of users, which can be drawn on to run the test.

If the test succeeds, SAML SSO is successfully configured.



CHAPTER 9

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. 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.

You can choose from the following authentication methods:

- **Authentication through Symmetric Key**: If you choose this option, the devices in your network use a symmetric key to encrypt and authenticate NTP messages. This option is recommended by some vendors, such as RedHat.
- **Authentication through Autokey (PKI-based infrastructure)**: If you choose this option, the devices in your network use the autokey protocol to encrypt and authenticate NTP messages. This method is mandatory for Common Criteria compliance.
- **No Authentication**: If you choose not to configure Authentication through Symmetric Key or Authentication through Autokey methods, NTP messages will not be authenticated.

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.
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.

Audio Codec	Description
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.
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.

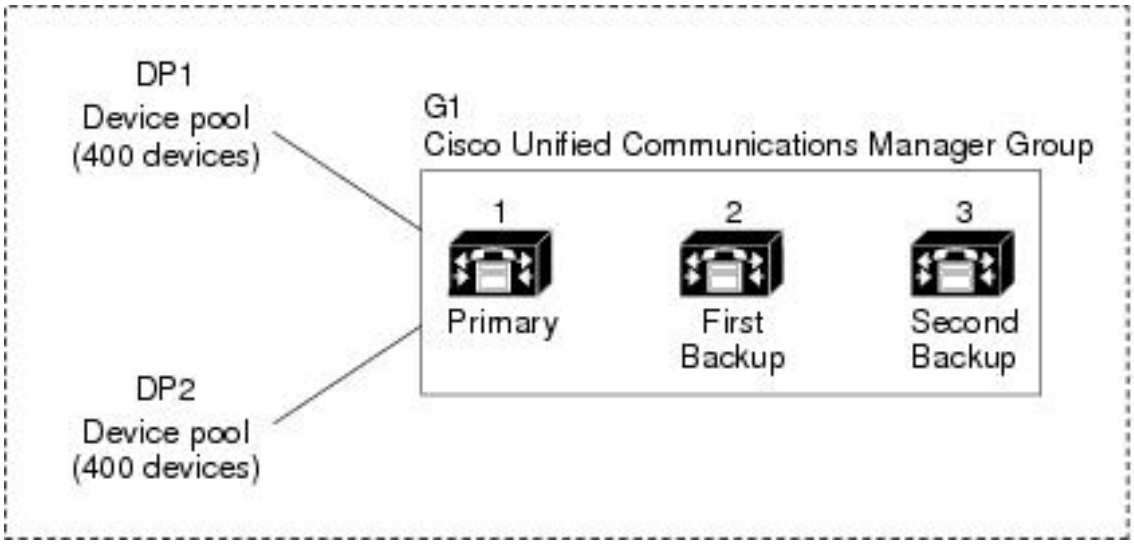
If the primary Unified Communications Manager fails for any reason, the first backup Unified Communications Manager in the group takes control of the devices that were registered with the primary Unified Communications Manager. If you specify a second backup Unified Communications Manager for the group, 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 4: 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.

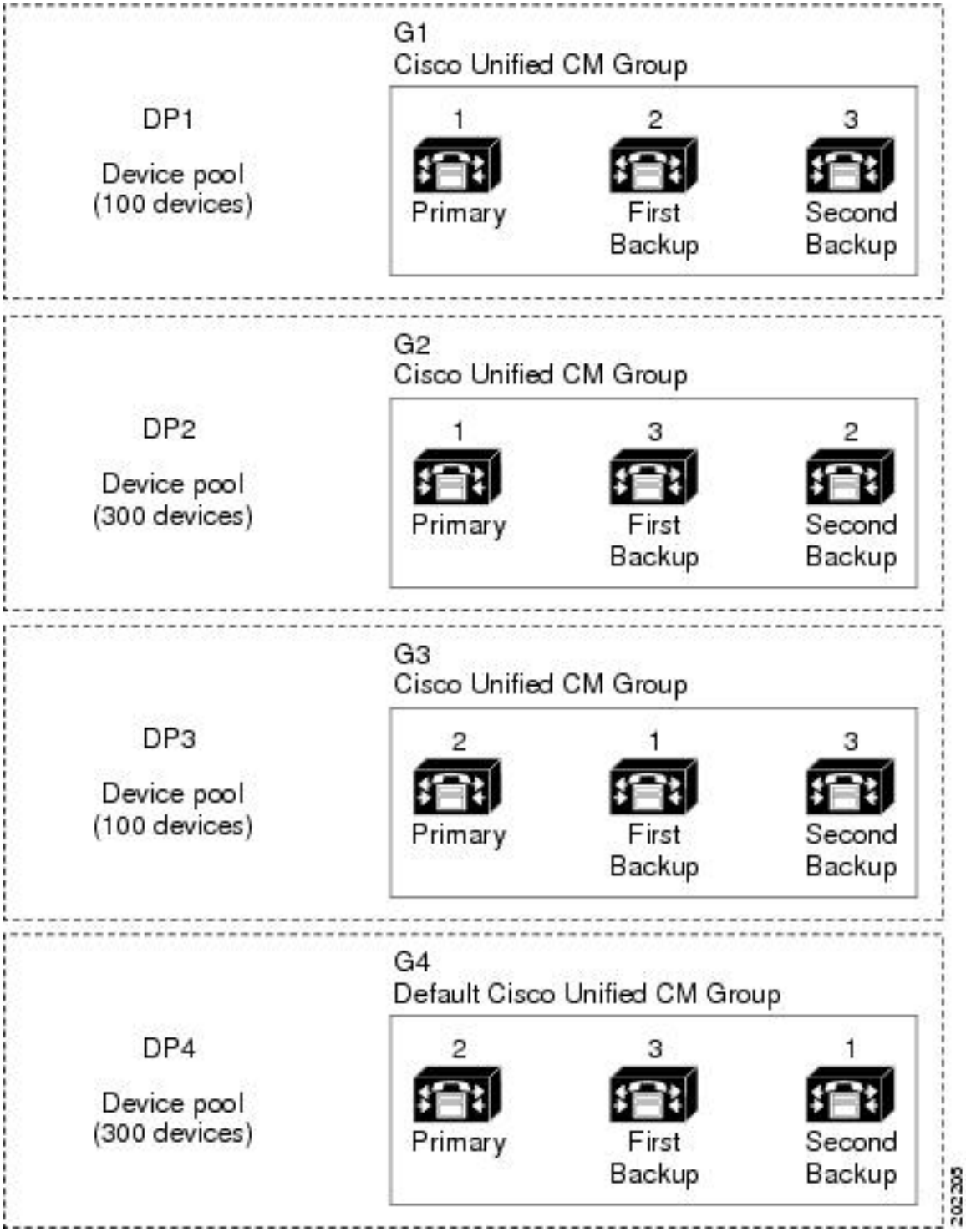
Note Empty Unified Communications Manager groups will not function.

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 5: 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. For more information, see *Media Resources Configuration Task Flow* section of this book.
- 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. For more information, see *Survivable Remote Site Telephony Configuration Task Flow* section in this book.
- Call Routing Information—For information on how to route calls between clusters, see *Call RoutingConfiguration Task Flow* section in this book.
- Device Mobility—Configure Device Mobility groups to allow devices to assume the settings based on their physical location. For more information, 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 75	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 81	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 81	Configure Unified Communications Manager groups for call processing redundancy and load balancing.
Step 4	Configure Device Pools, on page 82	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 76	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	Choose one of these methods to authenticate NTP messages: • Configure NTP Authentication via Symmetric Key, on page 76	Optional. For additional security, configure authenticated NTP. You can configure authentication via either a symmetric key or via autokey. The autokey method is required for Common Criteria compliance.

	Command or Action	Purpose
	• Configure NTP Authentication via Autokey, on page 77	
Step 3	Configure Phone NTP References, on page 77	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 78	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 NTP Authentication via Autokey

Use this procedure if you want to configure NTP authentication via the PKI-based autokey.

Note If NTP authentication with a symmetric key is enabled, you must disable it before enabling authentication with autokey. To disable NTP authentication with a symmetric key, see Configure NTP Authentication via Symmetric Key, on page 76.

Before you begin

Common Criteria mode must be enabled for you to enable NTP authentication via autokey. For details on enabling Common Criteria mode, see the "FIPS Setup" chapter of the *Security Guide for Cisco Unified Communications Manager*.

Procedure

Step 1 Log into the Command Line Interface.

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

Step 3 Do one of the following:

- To enable NTP authentication run the **utils ntp auth auto-key enable** CLI command.
- To disable NTP authentication, run the **utils ntp auth auto-key disable** CLI command.

Step 4 Enter the number for the NTP server for which you want to enable or disable NTP authentication.

Step 5 If you are enabling authentication, enter the IFF client key. Paste the client key for 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 78

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 79	Optional. Use this procedure if you want to customize priorities for your audio codecs. You 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 80	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 81	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 114.

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:

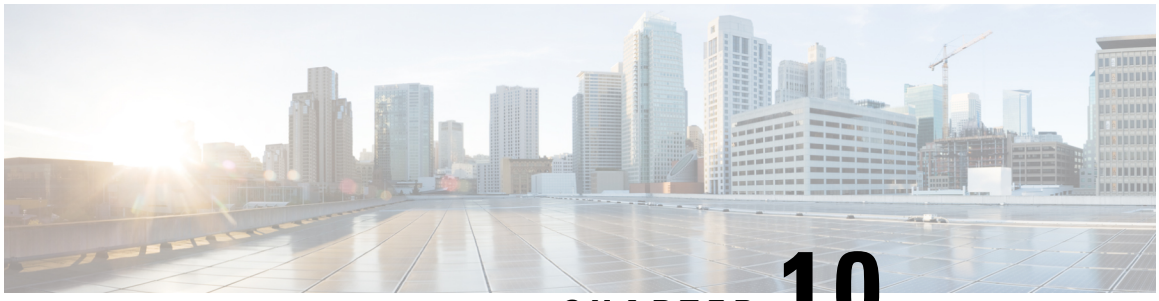
- Annunciator
- H.323 endpoints such as NetMeeting or third-party H.323 endpoints
- CTI applications
- TAPI applications
- JTAPI applications

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.
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.



CHAPTER 10

Configure Trunks

SIP Trunk Overview

If you are deploying SIP for call control signaling, configure SIP trunks to connect Cisco Unified Communications Manager to external devices such as SIP gateways, SIP Proxy Servers, Unified Communications applications, conference bridges, 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 a single DNS SRV record.

SIP Trunk 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.
- Make sure that you have a device pool configured for the trunk.
- If you are deploying IPv6 on the trunk, you must configure the trunk's Addressing Preference via a clusterwide enterprise parameter or via a Common Device Configuration that you can apply to the trunk.
- If there are SIP interoperability issues with the applications that use the trunk, you may need to use one of the default SIP Normalization or Transparency scripts. If none of the default scripts meet your needs,

you can create your own script. For details on creating customized SIP Normalization and Transparency scripts, see the *Feature Configuration Guide for Cisco Unified Communications Manager*.

SIP Trunk Configuration Task Flow

Complete these tasks to set up your SIP trunks.

Procedure

	Command or Action	Purpose
Step 1	Configure SIP Profiles, on page 88	Configure common SIP settings that you will apply to your SIP trunks.
Step 2	Configure SIP Trunk Security Profile, on page 89	Configure a security profile with security settings such as TLS signaling or digest authentication.
Step 3	Configure SIP Trunks, on page 89	Set up a SIP trunk and apply the SIP Profile and security profile to the trunk.

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**.

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 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**.

SIP Trunk Interactions and Restrictions

Feature	Description
Multiple Secure SIP Trunks to Same Destination	As of Release 12.5(1), Cisco Unified Communications Manager supports the configuration of multiple secure SIP trunks to the same Destination IP Address and Destination Port Number. This capability provides the following benefits: • Bandwidth optimization—Provides a route for emergency calls with unrestricted bandwidth • Selective routing based on a particular region or calling search space configuration

Feature	Description
Multiple Non-secure SIP Trunks to Same Destination	When multiple non-secure SIP trunks with different listening ports point to the same destination or port, they may incorrectly use the port in the mid call INVITE. Hence, the call drops.
Unified Communications Manager sends SIP-UPDATE message when it receives SIP 180 Ringing	The sip trunk sends an "UPDATE" SIP message when it receives "180 Ringing" after "183 Session Progress", provided the "UPDATE" value is supported in the call flow.
Presentation Sharing using BFCP	If you are deploying Presentation Sharing for Cisco endpoints, make sure that the **Allow Presentation Sharing with BFCP** check box is checked in the SIP Profile of all intermediate SIP trunks. **Note** For third-party SIP endpoints, you must also make sure that the same check box is checked within the **Phone Configuration** window.
iX Channel	If you are deploying iX Media Channel, make sure that the **Allow iX Application Media** check box is checked in the SIP Profiles that are used by all intermediate SIP trunks. **Note** For information on encrypted iX Channel, see the *Security Guide for Cisco Unified Communications Manager*.
90-day Evaluation License	You cannot deploy a secure SIP trunk while running with a 90-day evaluation period. To deploy a secure SIP trunk, your system must have registered to a Smart Software Manager account with the **Allow export-controlled functionality** product registration token selected.

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 intracluster communications, except for 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 intercluster 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 that is 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 that 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, see *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 configurations in Core Settings for Device Pools Configuration Task Flow, on page 74 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.

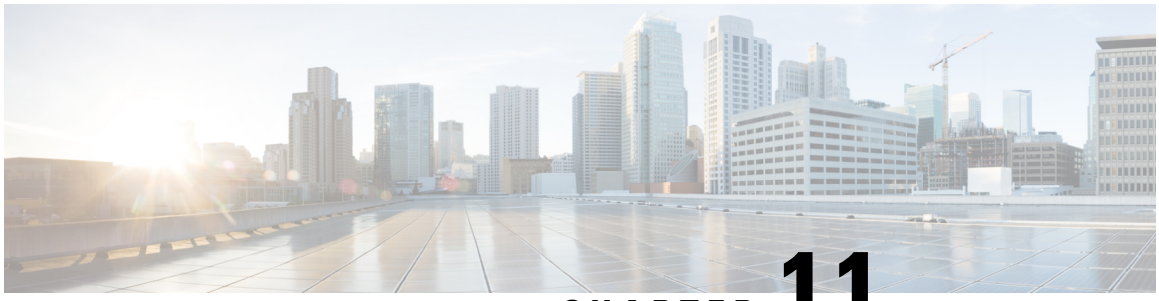
Step 6 From the **Device Pool** drop-down list box, select the device pool that you configured for this trunk.

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 11

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.

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.

Procedure

	Command or Action	Purpose
Step 1	Perform any of the following procedures depending on the protocol that you want to deploy: • Configure MGCP Gateway, on page 97 • Configure SCCP Gateway, on page 104 • Configure SIP Gateway, on page 107 • Configure H.323 Gateway, on page 109	Configure your gateways in the Unified Communications Manager. 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.
Step 2	Configure Clusterwide Call Classification for Gateway, on page 110	**Optional**. Configure a clusterwide service parameter to classify all calls coming from the gateway ports in your network to be internal (OnNet) or external (OffNet).
Step 3	Block OffNet Gateway Transfers, on page 110	**Optional**. 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.

Configure MGCP Gateway

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

Before you begin

Confirm Unified CM port connections for MGCP gateways. From Cisco Unified CM Administration, go to **System** > **Cisco Unified CM**, select the server and confirm the configured MGCP Listen port and MGP Keep-alive ports. In most cases, there is no need to change the default port settings.

Procedure

	Command or Action	Purpose
Step 1	Configure MGCP (IOS) Gateway, on page 98	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 Gateway Port Interface, on page 99	Configure the gateway port interface 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
		Tip After you configure a port interface, from the **Related Links** drop-down list, 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 102	**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 103	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 Gateway Port Interface

You can 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.

Select any of the following tasks, depending on the type of interface that you want to configure:

- Configure Digital Access PRI Ports, on page 99
- Configure Digital Access T1 Ports for MGCP Gateway, on page 99
- Configure FXS Ports, on page 100
- Configure FXO Ports, on page 101
- Configure BRI Ports, on page 102

Configure Digital Access PRI Ports

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

Before you begin

Configure MGCP (IOS) Gateway, on page 98

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 103.

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 98

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 102.

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 103.

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 98

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 103.

Configure BRI Ports

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

Before you begin

Configure MGCP (IOS) Gateway, on page 98

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 103.

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 99

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 103.

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

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

Procedure

	Command or Action	Purpose
Step 1	Configure SCCP as Gateway Protocol, on page 104	Configures a gateway to use SCCP as the gateway protocol.
Step 2	Enable Autoregistration of Nonconfigured Analog FXS Ports	Enables auto registration of nonconfigured analog FXS ports.
Step 3	Enable Auto Registration for Analog Phones, on page 105	Enables auto registration for the specified ports to fetch the DN from the pool of auto-registration DNs.

Configure SCCP as Gateway Protocol

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**.

Enable Auto Registration for Analog Phones

Enable auto registration for specified ports to fetch the directory numbers from the pool of auto-registration DNs. By default, Unified Communications Manager does not allow auto registration for analog phones. The administrator must configure the gateway module to support analog phones to auto-register with Unified CM through their corresponding gateways using the SCCP protocol.

Note Supported gateway types are VG310, VG350, VG400, VG450, and ISR4K series.

Before you begin

- Enable autoregistration and specify the range of DNs that get assigned to the new endpoints while they connect to the network. For more information, see Enable Autoregistration, on page 375 section.
- Enable auto-config with SCCP protocol in the gateway. For more information, see CUCM Auto Configuration for SCCP Gateways guide.

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 **Gateway Details** section, perform the following steps:

a) Enter the last 10 digits of the **MAC Address** in the text box. The **Description** field value is auto-populated when you enter the MAC Address.

Note The MAC address of the gateway can either be the Ethernet MAC address or the Virtual MAC address assigned in the SCCP gateway's interface, communicating to the Unified Communications Manager.

When you provide the MAC address, each FXS port obtains the port name from the configured MAC address and its port number. The corresponding analog phones automatically register with this gateway.

For example, if NM-4VWIC-MBRD is selected in Module in Slot 0 drop-down list and VIC3-4FXS/DID-SCCP is selected in the **Subunit 0** drop-down list, 4 FXS port values are displayed namely **0/0/0, 0/0/1, 0/0/2, 0/0/3**. Click each port to view the corresponding port name in the **Description** field of **Phone Configuration** window. The displayed port name is the combination of MAC address and the port value.

The gateway uses the Virtual MAC address or Ethernet MAC address to communicate with the Unified Communications Manager based on the configuration. The Virtual MAC address can be used even when you replace the damaged gateway so that you do not need to perform any configuration changes in the Unified Communications Manager application.

b) Select the required **Cisco Unified Communications Manager Group** from the drop-down list to enable autoregistration.

Step 6 In the **Configured Slots, VICs and Endpoints** section, perform the following steps:

a) Select a slot corresponding to the Network Interface Module hardware that is installed on the gateway for each **Module** drop-down list and click **Save** to enable respective **Subunits**.

b) Select corresponding VICs installed on the gateway for one or more Subunits and click **Save**.

Note Slot and module indicate which slot and module have FXS ports. It also indicates a number of FXS ports.

Configure gateways only up to a Subunit level and not up to the port level as it auto-registers and obtain an auto DNs. For example, when the Subunit is selected to FXS, the corresponding FXS port selects one of the DN available in the auto-register DN pool and assigns the DN to the selected ports.

Step 7 Click **Apply Config**.

The gateway sends register request for all FXS configured ports regardless of whether that port is connected to a phone or not.

Enable Autoregistration of Nonconfigured Analog FXS Ports

Use this procedure to enable the autoregistration of nonconfigured Analog FXS Ports.

Procedure

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

Step 2 From the **Server** drop-down list, choose the required server that is running.

Step 3 From the **Service** drop-down list, choose **Cisco Call Manager(Active)**.

Step 4 In the **Clusterwide Parameters (Device-PRI and MGCP Gateway)** section, ensure that the value of **Enable Auto Registration for FXS Ports** drop-down list is set to **True**.

Note Set the value of **Enable Auto Registration for FXS Ports** to **False** to disable the auto registration of nonconfigured Analog FXS ports.

Step 5 Click **Save**.

Troubleshooting Tips

Perform the following in Unified Communications Manager to ensure the ports are registered and obtain an auto DNs.

1. Configure SCCP as Gateway Type.
2. Enable Auto-registration
3. Select an Analog Phone as the Device Type
4. Ensure sufficient DNs are available in the pool to accommodate the number of voice ports.

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 108	Configure SIP settings and apply to a SIP profile. Trunk uses this settings to connect to the SIP gateway.
Step 2	Configure SIP Trunk Security Profile., on page 108	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 108	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.

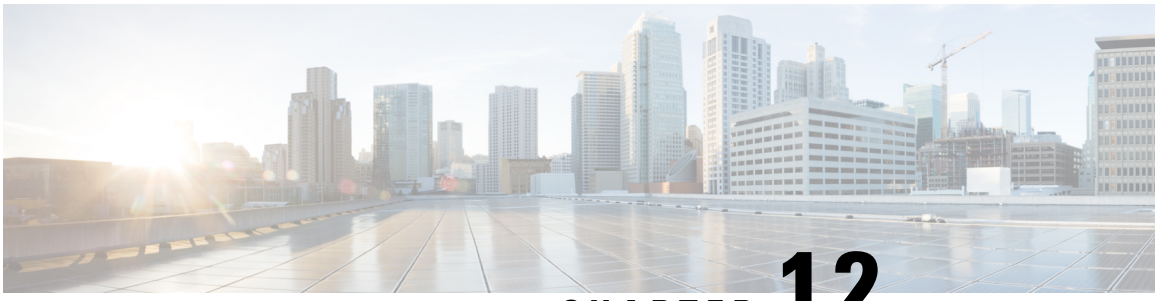
Step 3 From the **Service** drop-down list, choose **Cisco CallManager**.

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 12

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 186.

Procedure

	Command or Action	Purpose
Step 1	Configure an SRST Reference, on page 114	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 115	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 115 • Configure Connection Monitor Duration for a Device Pool, on page 116	**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 116	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 115
- (Optional) Perform one of the following tasks:
  - Configure Connection Monitor Duration for the Cluster, on page 115
  - Configure Connection Monitor Duration for a Device Pool, on page 116

Procedure

Step 1 Log into the SRST gateway (router).

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

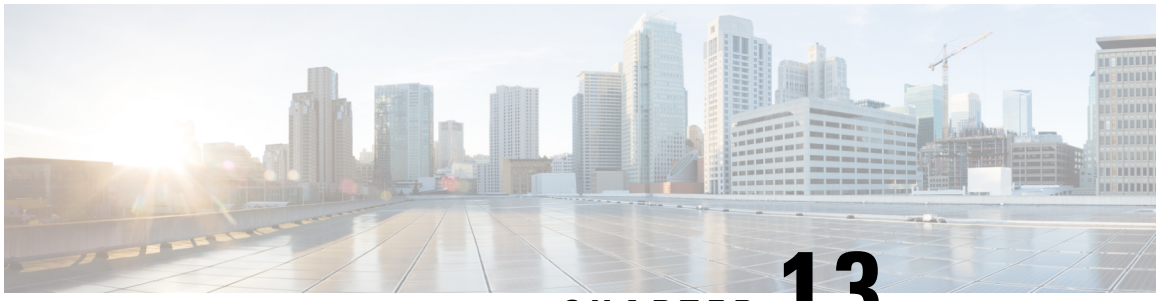
Step 3 Enter the command **max-ephones** max-phones, where max-phones is the maximum number of supported Cisco IP phones.

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.



CHAPTER 13

Configure Media Resources

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 Termination Points

A media termination point (MTP) is an entity that accepts two full-duplex media streams, bridging the streams together and allowing them to be set up and torn down independently. Cisco Unified Communications Manager can insert an MTP in the media path to resolve many situations:

- To act as a Trusted Relay Point (TRP)

- To provide conversion between IPv4 and IPv6 for RTP streams
- To deliver SIP Early Offer over SIP trunks
- To address DTMF transport mismatches
- To act as an RSVP agent

MTP for H.323 Calls

Media Termination Points can be inserted in the media path for H.323 calls in order to 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.

MTP Types

Cisco Unified Communications Manager supports the following MTP types:

- Software MTPs in IOS gateways
- Hardware MTPs in IOS gateways
- Software MTP provided by the Cisco IP Voice Media Streaming service

The Cisco Media Termination Point Software MTP type 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.

MTP Registration

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 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.

Media Termination Points Interactions and Restrictions

Table 7: 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.

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 with MTP Functionality

In addition to codec conversion, a transcoder can provide the same functionality as a media termination point (MTP). In cases where both transcoder functionality and MTP functionality are needed, the system allocates a transcoder due to the fact that transcoders can provide both sets of functionality simultaneously. If only MTP functionality is required, the system allocates either a transcoder or an MTP from the resource pool. The choice of resource will be determined by the media resource groups.

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 the **Fail Call If Trusted Relay Point Allocation Fails** and **Fail Call If MTP Allocation Fails** fields are set to 'False' in the **Cisco Unified CM Administration** > **System** > **Service Parameters** > **Service Parameter Configuration** window. If hardware transcoder functionality is required (to convert one codec to another) and a transcoder is not available, the call will fail.

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 8: 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 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.

Interactions or Restriction	Description
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.

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 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.
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.

Call Behavior with Insufficent TRP Resources

The following sections provide examples of how Cisco Unified Communications Manager handles calls when insufficient MTP resources are allocated. The ulimate call behavior depends on whether MTPs and TRPs are required for those endpoints, and whether the system is configured to fail calls automatically when MTP or TRP allocation fails.

MTP and TRP are Both Required

The following table shows whether a call fails when both the **Media Termination Point Required** and **Use Trusted Relay Point** options are selected for an endpoint, and insufficient MTP and TRP resources exist.

The final call status depends on whether the **Fail Call If Trusted Relay Point Allocation Fails** and the **Fail Call if MTP Allocation Fails** service parameters are set to fail calls automatically.

Fail Call If TRP Allocation Fails Service Parameter	Fail Call If MTP Allocation Fails Service Parameter	Unified CM Fails
True	True	Yes
True	False	Yes
False	True	Yes, if MTP is rec MTP is required f
False	False	No

Automatic Call Failure for Insufficient MTP/TRP Resources Not Enabled

The following table shows the call behavior when insufficient MTP/TRP resources exists and both the **Fail Call If Trusted Relay Point Allocation Fails** and **Fail Call If MTP Allocation Fails** service parameters are set to **`False`**.

MTP Required = Yes	Use TRP = Yes	Resource Allocation Status	Call Behavior
Y	Y	TRP allocated	Audio call only because no pass-through support exists.
Y	Y or N	MTP only	Audio call only. No TRP support.
Y	Y or N	None allocated	If MTP required is checked for H.323 endpoint, supplementary services will be disabled.
N	Y	TRP allocated	Audio or video call depends on endpoint capabilities, and call admission control (CAC). Supplementary services still work.
N	Y	None allocated	Audio or video call. Supplementary services still work, but no TRP support exists.

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 9: 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.
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 10: 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.

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 11: 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.
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.

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 12: 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

Media Resources Configuration Task Flow

Complete these tasks to configure media resources for your system.

Procedure

	Command or Action	Purpose
Step 1	Activate Software Media Resources, on page 133	Turning on the IPVMS service activates software media resources on the server.
Step 2	Configure Media Termination Points, on page 134	Configure Media Termination Points (MTPs) for your system.
Step 3	Configure Transcoders, on page 134	Add Transcoder resources to the system.

	Command or Action	Purpose
Step 4	Configure the Interactive Voice Response (IVR), on page 135	Configure default settings for the system IVR.
Step 5	Configure the Annunicator, on page 135	Configure system settings for the Annunciator.
Step 6	Configure Media Resource Groups, on page 136	Add your media resources into a Media Resource Group. Set up multiple groups with different combinations of resources.
Step 7	Configure Media Resource Group Lists, on page 136	Create a list of Media Resource Groups that you can assign to an endpoint, or class of endpoints.
Step 8	Assign Media Resources to Device or Device Pool, on page 137	Make media resources available to endpoints by assigning them to a device or device pool.
Step 9	Configure Announcement, on page 137	**Optional**. Configure settings for specific announcements. Announcements are used in normal processing, or for features like Music On Hold or IVR.
Step 10	Upload a Customized Announcement, on page 137	**Optional**. Upload a prerecorded announcement. Assign the file to a new or existing announcement.

Activate Software Media Resources

Activate the **Cisco IP Voice Media Streaming** service to turn on the following software media resources:

- Annunciator
- Interactive Voice Response (IVR)
- Media Termination Point (MTP)
- Software Conference Bridges
- Music On Hold

Procedure

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

Step 2 From the **Server**, select a Unified Communications Manager node.

Step 3 Check the **Cisco IP Voice Media Streaming Service** and click **Save**.

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**.

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**.

Configure the Interactive Voice Response (IVR)

Use this procedure to configure settings for the IVR.

Before you begin

The Cisco IP Voice Media Streaming service must be running for the Interactive Voice Response (IVR) to be active.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Media Resources** > **Interactive Voice Response**.

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

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

Step 4 If you want IVR calls to use a trusted relay point, set the **Use Trusted Relay Point** drop-down to **On**.

Step 5 Complete the remaining fields in the **Interactive Voice Response Configuration** window. For help with the fields and their settings, see the online help.

Step 6 Click **Save**.

Configure the Annunicator

Configure system settings for the Annunciator.

Before you begin

The Cisco IP Voice Media Streaming service must be running for the Annunciator to be active.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Media Resources** > **Annunciator**.

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

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

Step 4 Select a **Device Pool**.

Step 5 If you want the annunciator to use a trusted relay point, set the **Use Trusted Relay Point** drop-down to **On**.

Step 6 Click **Save**.

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**.

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 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 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.

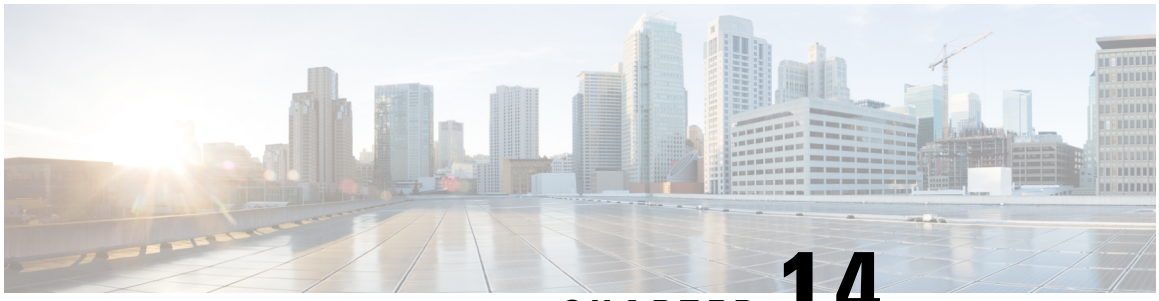
Step 5 (Optional) If you want Unified Communications Manager to play the customized announcement instead of playing the Cisco-provided announcement, check the **Enable** check box appears in the **Announcement by Locale** pane in the **Announcements Configuration** window.

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 14

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 13: 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 IOS Heterogeneous Video Conference Bridge	Cisco Integrated Services Routers Generation 2 (ISR G2) can act as IOS-based conference bridges that support ad hoc and meet-me video conferencing. DSP modules must be installed on the router to enable the router as a conference bridge. In a heterogeneous video conference, all the conference participants connect to the conference bridge with phones that use different video format attributes. In heterogeneous conferences, transcoding and transsizing features are required from the DSP to convert the signal between the various formats. For heterogeneous video conferences, callers connect to the conference as audio participants under either of the following conditions: • Insufficient DSP resources. • The conference bridge is not configured to support the video capabilities of the phone. For more detailed information about video conferencing with ISR G2 routers, refer to the document *Configuring Video Conferences and Video Transcoding*.
Cisco Guaranteed Audio Video Conference Bridge	Cisco Integrated Services Routers Generation 2 (ISR G2) can act as IOS-based conference bridges that support ad hoc and meet-me voice and video conferencing. DSP modules must be installed on the router to enable the router as a conference bridge. DSP resources are reserved for the audio portion of the conference, and video service is not guaranteed. Callers on video phones may have video service if DSP resources are available at the start of the conference. Otherwise, the callers connect to the conference as audio participants. For more detailed information about video conferencing with ISR G2 routers, refer to the document *Configuring Video Conferences and Video Transcoding*.
Cisco IOS Homogeneous Video Conference Bridge	Cisco Integrated Services Routers Generation 2 (ISR G2) can act as IOS-based conference bridges that support ad hoc and meet-me video conferencing. DSP modules must be installed on the router to enable the router as a conference bridge. Cisco IOS Homogeneous Video Conference Bridge specifies the IOS-based conference bridge type that supports homogeneous video conferencing. A homogeneous video conference is a video conference in which all participants connect using the same video format attributes. All the video phones support the same video format and the conference bridge sends the same data stream format to all the video participants. If the conference bridge is not configured to support the video format of a phone, the caller on that phone connects to the conference as an audio only participant. For more detailed information about video conferencing with ISR G2 routers, refer to the document *Configuring Video Conferences and Video Transcoding*.

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 144	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 145	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 145	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 145.

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**.

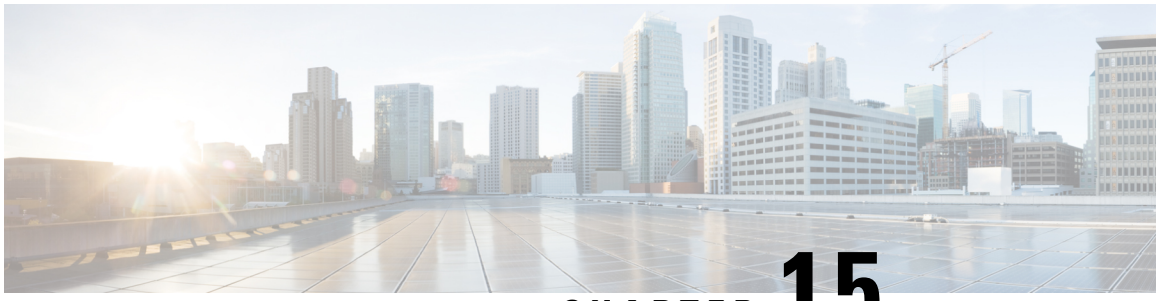
Step 5 Create an entry for the conference bridge in the **Destination** area by adding the IP address or hostname for the conference bridge. If you need a new line, you can click **(+)** to add it.

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 15

Configure Enhanced Locations Call Admission Control

Enhanced Locations Call Admission Control Overview

Enhanced Locations Call Admission Control (CAC) lets you regulate audio quality and video availability over complex WAN topologies and intercluster networks. This includes multi-tier and multi-hop networks.

You can create a model of the complete network topology, indicating the different Locations (LANs) and WAN links that connect those locations. For each location and WAN link, assign bandwidth limits that represent the total bandwidth that is available for all calls over that link at one time. If bandwidth is not available for a particular call, the call is rejected with a busy signal. This prevents audio and video quality from degrading as a result of a WAN link becoming oversubscribed.

The intercluster replication functionality of the Location Bandwidth Manger (LBM) Replication Group lets you replicate your location configuration across an intercluster network, thereby making it easier to manage in large intercluster networks.

Enhanced Locations CAC Components

This feature uses the following components:

- Locations—A Location represents a LAN. It could contain endpoints or simply serve as a transit location between links for WAN network modeling. Cisco Unified Communications Manager supports up to 2000 locations.
- Links—The connection between two locations. When configuring this feature, you assign bandwidth allocations and weights for each link.
- Weight—The relative priority of the link in forming the effective path between any pairs of locations. Weights are used only when multiple paths exist between two locations. Weights are used to calculate the effective path (the path with the least cumulative weight).

- Bandwidth Allocations—The total bandwidth allocated for a particular type of traffic (audio, desktop video, immersive video) over a specific link. Bandwidth can also be allocated for intralocation calls (the default setting is Unlimited).
- Location Bandwidth Manager (LBM)—A feature service that must be activated in Cisco Unified Serviceability for Enhanced Locations CAC to work. This service assembles the network model and computes the effective path between locations by adding the weight of all links and locations between the source and destination, and choosing the path with the least cumulative weight.

Locations Relationship to Regions

The Locations configuration of Enhanced Locations Call Admission Control works with Regions to manage bandwidth for calls:

- The bandwidth allocations within the Region Configuration assigns the total amount of bandwidth that the endpoints in a call between two regions can use.
- The bandwidth allocations within Locations Configuration assigns the total amount of bandwidth that all calls between those locations can use. For an individual call, the bandwidth within the Regions Configuration is deducted from the amount of bandwidth that the location configuration makes available. For example, if the Locations configuration specifies that 160 kb/s of bandwidth is available over a particular link, that link can support two G.711 calls at 80 kb/s each simultaneously.

Note Do not change the Location Bandwidth Manager bandwidth or link configurations during production hours as that could unecessarily spike CPU utilization on the server.

Cisco Unified Communications Manger supports up to 2,000 locations and 2,000 regions per cluster.

Intercluster LBM Replication

The Intercluster Replication capability of the Location Bandwidth Manager Hub Group lets you replicate your locations and link assignments across the larger intercluster network. You can assign LBMs to the LBM Hub role, which lets them actively replicate locations and link information across a meshed intercluter network. LBM hubs discover each other through their common connections and form a fully-meshed replication network. LBMs that are assigned a spoke role participate indirectly in intercluster replication through the LBM hubs in their cluster.

Intercluster Topology Management

There are multiple ways to configure and manage your intercluster network. The following table summarizes two approaches for configuring and managing the intercluster topology:

Design Approach	Description
Location and Link Management	Use a single cluster to configure and manage bandwidth allocations for all links across the intercluster network. This approach simplifies the configuration overhead, particularly in deployments with many common locations. The intercluster configuration approach is as follows: In the management cluster, configure all locations and links (including bandwidth allocations and weights) for the entire topology. This information will be replicated to the intercluster network. For the other clusters in the topology: • Configure locations for the local cluster only. This is solely to associate devices to a location. • Do not configure link information. • Leave all bandwidth allocations in the local cluster as **Unlimited**. If the management cluster replicates bandwidth allocations that are less than the local cluster, the more restrictive configuration will be applied.
Intercluster Enhanced Locations CAC	With this approach: • Within each cluster, configure the local locations and link information to the neighboring cluster only. • Assign link information, including weighth and bandwidth allocation, to neighboring clusters only. The rest of the topology gets replicated by the • The Hub_None location must be renamed in each cluster or it will be a common location across clusters. • Each cluster requires a unique Cluster ID. **Note** It;s critical for replication to name clusters consistenly across all clusters.

Enhanced Locations CAC Prerequisites

Make sure that you understand your LAN and WAN network topology before you attempt to configure this feature. This is required in order to allocate bandwidth for locations and links.

Enhanced Locations CAC Task Flow

Complete these tasks to configure Enhanced Locations Call Admission Control on your system.

Procedure

	Command or Action	Purpose
Step 1	Activate Location Bandwidth Manager, on page 150	The Cisco Location Bandwidth Manager feature service must be running on at least one cluster node.
Step 2	Configure LBM Group, on page 151	By default, the Cisco CallManager service communicates with the local LBM service. However, LBM groups can be used to manage this communication, providing an active and standby LBM for redundancy.
Step 3	Configure Locations and Links, on page 151	Create the locations (LANs) for your network and assign bandwidth allocations for the WAN links that connect those locations.
Step 4	Configure LBM Intercluster Replication Group, on page 152	Create an intercluster replication group that replicates configured CAC information to other clusters.
Step 5	Configure SIP Intercluster Trunks, on page 152	Assign the **Shadow** location to the SIP intercluster trunks in your network.
Step 6	Configure Call Admission Control Service Parameters, on page 153	Optional. Configure service parameter settings for Call Admission Control. The default settings may be sufficient for many deployments.

Activate Location Bandwidth Manager

For Enhanced Locations Call Admission Control, you must activate the Cisco Location Bandwidth Manager feature service on at least one node in the cluster. This service is off by default.

Procedure

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

Step 2 From the **Server** drop-down, select the cluster node on which you want the service to run and click Go.

Step 3 Under **CM Services**, check the **Cisco Location Bandwidth Manager** service

Step 4 Click **Save**.

Step 5 Repeat this task if you want to start the service on addiitonal nodes.

Note Cisco recommends running the Cisco Location Bandwidth Manager service on each subscriber node in the cluster that is also running the Cisco CallManager service.

Configure LBM Group

Use this procedure to configure an LBM Group. By default the Cisco CallManager service communicates with the local LBM service. However, LBM groups can be used to manage this communication, providing an active and standby LBM for redundancy.

Note The order in which the Cisco CallManager service uses the LBM is as follows:

- LBM Group designation
- Local LBM (co-resident)

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Locations** > **Location Bandwidth Manager Group**.

Step 2 Click **Add New**.

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

Step 4 From the **Active Member** drop-down, select the active member of this group.

Step 5 From the **Standby Member** drop-down, select a desired standby to be used when the active member is unavailable.

Step 6 Click **Save**.

Configure Locations and Links

Use this procedure to create the locations (LANs) in your network. Assign total bandwidth and weights for the calls that use the WAN links between those locations. Refer to the online help for help with the fields and their settings.

Procedure

Step 1 From Cisco Unfiied CM Administration, choose **System** > **Location Info** > **Location**.

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

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

Step 4 In the **Links - Bandwidth Between This Location and Adjacent Locations** area, configure settings for WAN links to a another location:

a) Select a second location from the **Location** list box.
b) Configure the **Weight** that reflects the relative priority of this link in forming the effective path.
c) Configure total bandwidth for audio, video, and immersive video (TelePresence) calls.
d) Repeat these substeps to configure links to any additional locations.

Step 5 Optional. Expand the **Intra-location - Bandwidth for Devices Within This Location** area and configure total bandwidth allocations for intralocation calls for the newly created location. The default setting for all media types for these calls is **Unlimited**.

Step 6 In the **Modify Settings to Other Locations** area, configure RSVP settings to other locations:

a) In the **Location** column select the other location.
b) Select the **RSVP Setting** for calls between these locations.
c) Repeat these substeps to add RSVP settings for calls with additional locations.

Step 7 Click **Save**.

Step 8 Repeat this procedure to create additional locations and to configure links to and from those new locations.

Configure LBM Intercluster Replication Group

Use this procedure to configure an LBM Intercluster Replication Group. This is required to replicate Enhanced Locations Call Admissions Control bandwidth information across the intercluster network.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Location Info** > **Location Bandwidth Manager (LBM) Intercluster Replication Group**.

Step 2 Click **Add New**.

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

Step 4 In the **Bootstrap Servers** area, assign one or more LBM servers to be responsible for replicating connectivity information to other hubs.

Step 5 In the **Role Assignments** area, use the up and down arrows to select the local LBM servers that will act as hubs, and the LBM servers that will remain as spokes.

Step 6 Click **Save**.

Configure SIP Intercluster Trunks

With Enhanced Locations Call Admission Control, you must assign the Shadow location to the SIP intercluster trunks in your intercluster network.

Procedure

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

Step 2 Click **Find** and select the appropriate intercluster trunk.

Step 3 From the **Location** drop-down, select **Shadow**.

Step 4 Complete any other fields that you want in the **Trunk Confiiguration** window. For help with the fields and their settings, see the online help.

Step 5 Click **Save**.

Step 6 Repeat this task for any other intercluster trunks that will replicate information for Enhanced Locations Call Admission Control.

Configure Call Admission Control Service Parameters

Use this procedure to configure optional Service Parameters for Enhanced Locations Call Admission Control.

Procedure

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

Step 2 From the **Server** drop-down, select a cluster node.

Step 3 Configure service parameters for the **Cisco CallManager** service:

a) From the **Service** drop-down, select **Cisco CallManager**.
b) In the **Clusterwide Parameters (Call Admission Control)** area, configure any service parameters. For parameter help descriptions, click the name of the parameter in the GUI.
c) Click **Save**.

Step 4 Configure settings for the **Cisco Location Bandwidth Manager** service:

a) From the **Service** drop-down, select **Cisco Location Bandwidth Manager**.
b) Configure any service parameters that you want. For parameter help descriptions, click the name of the parameter in the GUI.
c) Click **Save**.

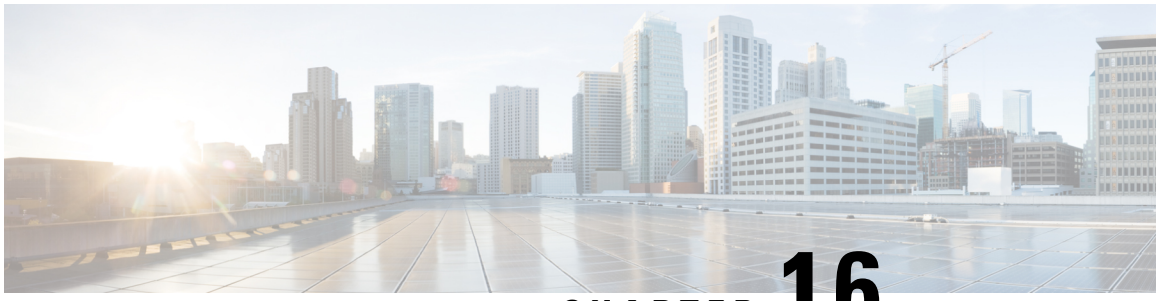
Enhanced Locations CAC Interactions Restrictions

The following table displays feature interactions and restrictions for Enhanced Locations Call Admission Control.

Feature	Interactions and Restrictions
LBM Security Mode	By default, the LBM Security Mode is Insecure. You can reconfigure this setting with the **LBM Security Mode** enterprise parameter. This parameter can be set to **Secure**, **Insecure** or **Mixed**. The **Mixed** setting can be used temporarily to maintain communication while you are securing all of your clusters, following which you can change the setting to **Secure**. After changing this parameter, you must reset all Cisco LBM Service Hubs in the cluster for this to take effect.

Feature	Interactions and Restrictions
Audio Bandwidth Deduction in Video Calls	By default, bandwidth for the audio portion of a video call is deducted from the video pool. You can reconfigure the system so that the audio portion of a video call is deducted from the audio pool by setting the **Deduct Audio Portion from Audio Pool for Video Calls** service parameter to **True** (the default setting is **False**).
Video Call Classification	Cisco TelePresence endpoints have a nonconfigurable video call classification of **Immersive**. Other endpoints have a nonconfigurable video call classification of **Desktop**. For SIP trunks, you can set the video classification (Desktop, Immersive or Mixed) by configuring the **Video Call Traffic Class** within the associated SIP Profile.
Media Resources	Bandwidth for media resources is not allocated via Call Admissions Control.
Locations Serviceability	The Cisco Unified Serviceability interface contains additional tools for managing and monitoring the Locations topology. For details, see the "Locations" topics in the *Cisco Unified Serviceability Administration Guide*.
Session Bandwidth Modifiers	You can assign which Session Bandwidth Modifiers are used by SIP endpoints within the SIP Profile Configuration window.
Bandwidth Allocation Conflicts	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.
Network Failures	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.
Synchronization Issues	The model created by the system is not perfectly synchronized at all times. Use conservative bandwidth allocations to accommodate this restriction.
Clustering over the WAN	For deployments with clustering over the WAN and local failover, intracluster LBM traffic is already calculated into the WAN bandwidth calculations.

Feature	Interactions and Restrictions
Flexible DSCP Marking	For additional QoS, you can use DSCP marking to assign markings that prioritize certain types of call flows over others. For example, you can prioritize audio over video so that even if the network is congested, blocking video media, basic communication can continue via audio. You can configure DSCP marking in two ways: • Service Parameters—Configure clusterwide DSCP defaults within the **Service Parameter Configuration** window's **Clusterwide Parameters (System - QoS)** section. • SIP Profile—Configure customized DSCP settings in a SIP Profile and apply them to certain groups of SIP devices. This setting overrides the clusterwide default.
APIC-EM Controller	You can use an APIC_EM Controller to manage SIP media flows for external QoS management. For details, refer to the *Feature Configuration Guide for Cisco Unified Communications Manager*.



CHAPTER 16

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 158	Configure the RSVP policy for all nodes in the cluster.
Step 2	Configure Location-pair RSVP Policy, on page 159	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 160	Configure the frequency and number of RSVP retries.
Step 4	Configure Midcall RSVP Error Handling, on page 160	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 161	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 162	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 162	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 159.
- If you are using the same RSVP policy for all nodes in the cluster, Configure RSVP Retry, on page 160.

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 160

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 158
- Optional. Configure Location-pair RSVP Policy, on page 159

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 160

Configure Midcall RSVP Error Handling

Use this procedure to configure midcall RSVP error handling.

Before you begin

Configure RSVP Retry, on page 160

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 161 if you are using multilevel precedence and preemption in your network.
- Configure the Application ID, on page 162

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 162.

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 162

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 162

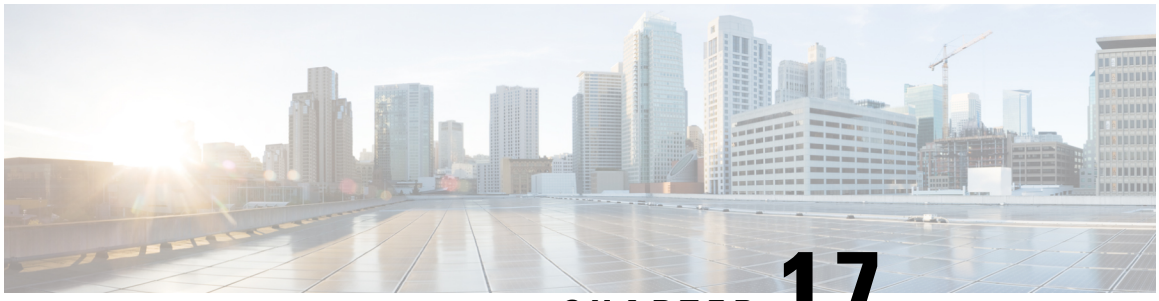
Procedure

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.



CHAPTER 17

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

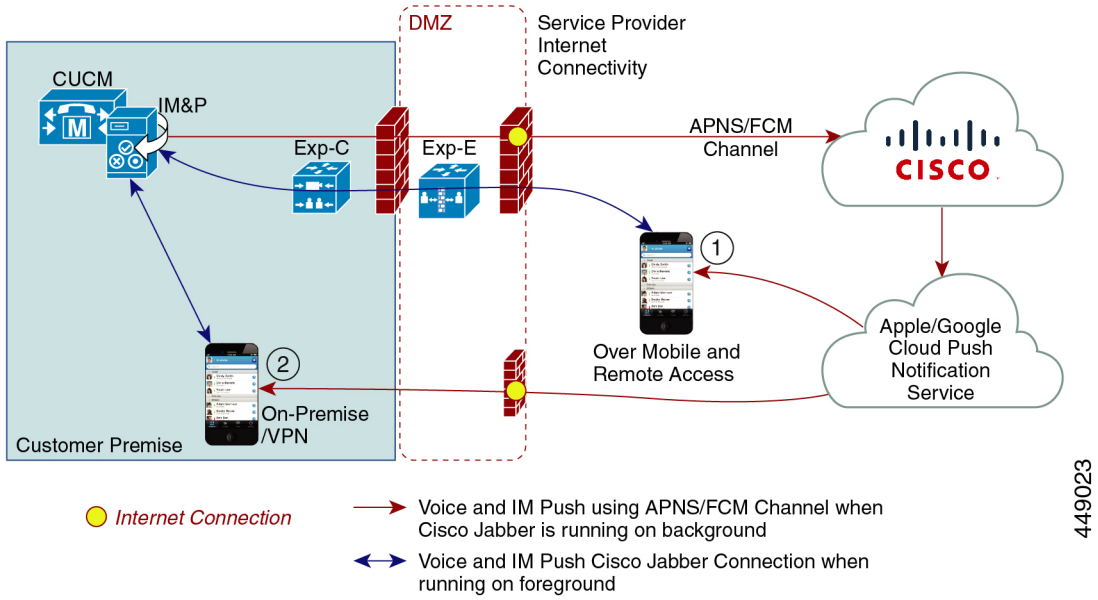
At startup, clients that are installed on Android and iOS platform devices register to Unified Communications Manager, the IM and Presence Service and to the Google and Apple cloud. With Mobile and Remote Access deployments, the clients registers to the on-premises servers through Expressway. So as long 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



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)

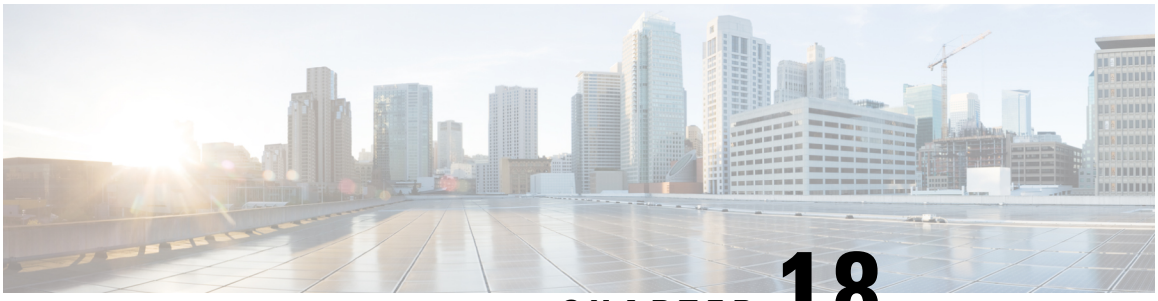
Client	OS	Platform Cloud	Cloud Service
Webex on Android	Android	Google	Android PNS Service

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.

PART II

Dial Plan



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 14: 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 175	Configure partitions to create a logical groupings of system resources with similar reachability characteristics.
Step 2	Configure Calling Search Spaces, on page 176	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 15: 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.

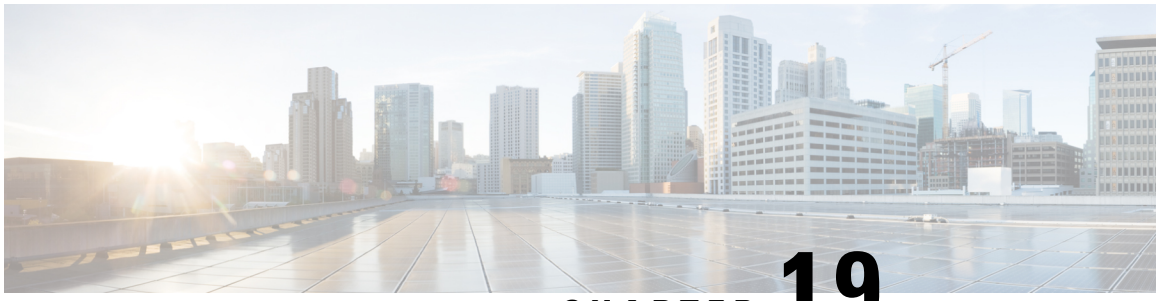
Step 7 (Optional) Change the priority of selected partitions by using the arrow keys to the right of the **Selected Partitions** box.

Step 8 Click **Save**.

Partition Interactions and Restrictions

Table 16: 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 180	**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 181	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 181	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 181

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

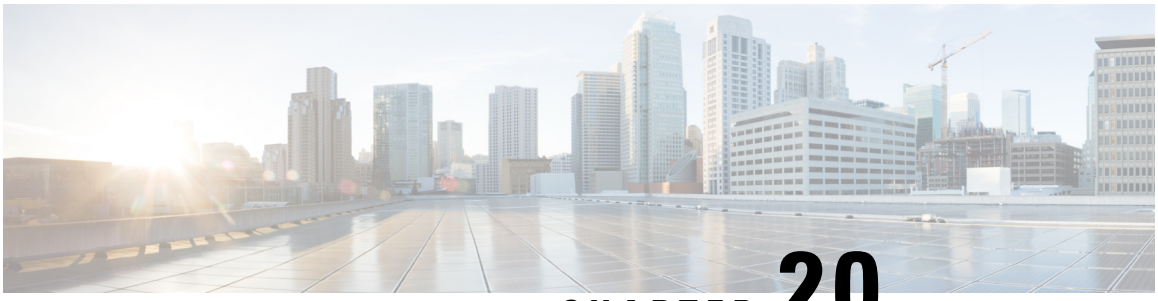
Procedure

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.

Translation Patterns

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, Unified CM 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 that is configured within the translation pattern.

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.

Transformation Patterns

Transformation patterns can be used to discard digits, add prefix digits, add a calling party transformation mask, and control the presentation of the calling party number before the system sends the call to the phone or to the PSTN.

Configure transformation patterns and associate them to a route partition, thereby assigning the pattern to the calling search space that contains the partition. You can assign the pattern to the call settings for a specific device, device pool, gateway, or trunk via the Calling Party Transformation CSS or Called Party Transformation CSS fields in the configuration windows.

You can configure the following transformation patterns:

- **Calling Party Transformation Patterns** — Allow the system to adapt the global form of the calling party's number into the local form required by off-cluster networks connected to the route group devices, such as gateways or trunks.

  Called Party Transformation Patterns — Allow the system to adapt the global form of the called party's number into the local form required by off-cluster networks connected to the route group devices.

Route Patterns

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 dial string and uses it to direct the call to a gateway or route list. You can assign route patterns to gateways, trunks, or to a route list that includes one or more route groups.
- **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.

Additional Call Routing

The route plan can also include the following optional components:

- **Local Route Groups** — If you have multiple sites, you can use local route groups so that Off-Net calls can be routed to a gateway as specified by the device pool rather than by the route pattern configuration. This allows you to use a single set of route patterns for multiple locations.
- **Route Filters** — Create route filters and add them to your route patterns or hunt pilots to restrict users from using the pattern. Route filters are mandatory is you are using a dial plan installer file, but are optional for manual dial plan configurations. For manual configurations, route filters apply only if your pattern uses the @ wildcard.
- **Automated Alternate Routing** — Automatically reroute calls through the PSTN or another network when the system blocks a call due to insufficient bandwidth.
- **Time-of-day Routing** — Create a time schedule that specifies when a given partition is available to receive incoming calls.

Call Routing Prerequisites

- Complete the tasks in the Partition Configuration Task Flow, on page 175.
- Ensure that you have the following information:
  - Internal number extensions
  - A plan listing the calls that route to each gateway

For detailed information on planning your call routing, refer to the *Call Control and Routing* topics in the *Cisco Collaboration System Solution Reference Network Design*.

Call Routing Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure Translation Patterns, on page 186	Configure translation patterns to specify how to complete digit translations for calls in a particular partition.
Step 2	Configure Calling Party Transformation Patterns, on page 186	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 3	Configure Called Party Transformation Patterns, on page 187	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 ten-digit calling number.
Step 4	Configure Local Route Groups, on page 187	**Optional**. Local route groups let you use a single set of route patterns for multiple locations. Unified CM assigns the gateway based on the calling device location rather than the route pattern.
Step 5	Configure Route Groups, on page 189	**Optional**. Configure route groups to set the selection order of the gateway devices. Route groups contain one or more devices.
Step 6	Configure Route Lists, on page 190	**Optional**. Route lists contain one or more route groups. Configure route lists to control the selection order of the route groups.
Step 7	Configure Route Filters, on page 190	**Optional**. Use route filters to restrict certain numbers that are otherwise allowed by a route pattern.
Step 8	Configure Route Patterns, on page 194	Configure route patterns to direct calls to specific devices and to include or exclude specific digit patterns.
Step 9	Enable Clusterwide Automated Alternate Routing, on page 198	**Optional**. Enable Automated Alternate Routing (AAR) to let the system reroute calls to the PSTN or other networks when calls are blocked due to insufficient bandwidth.

	Command or Action	Purpose
Step 10	Configure AAR Group, on page 198	**Optional**. Configure an AAR group with digit transformations to apply for Automated Alternate Routing.
Step 11	Configure Time of Day Routing, on page 199	**Optional**. Create a time schedule that specifies when a given partition is available to receive incoming calls.

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**.

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 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 188	**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 188	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 189	**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 191.

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 193.

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

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 17: Route Filter Tags

Tag	Description
AREA-CODE	This three-digit area code in the form [2-9]XX identifies the area code for long-distance calls.
COUNTRY CODE	These one-, two-, or three-digit codes specify the destination country for international calls.
END-OF-DIALING	This single character identifies the end of the dialed-digit string. The # character serves as the end-of-dialing signal for international numbers that are dialed within the NANP.
INTERNATIONAL-ACCESS	This two-digit access code specifies international dialing. Calls that originate in the U.S. use 01 for this code.
INTERNATIONAL-DIRECT-DIAL	This one-digit code identifies a direct-dialed international call. Calls that originate in the U.S. use 1 for this code.
INTERNATIONAL-OPERATOR	This one-digit code identifies an operator-assisted international call. This code specifies 0 for calls that originate in the U.S.
LOCAL-AREA-CODE	This three-digit local area code in the form [2-9]XX identifies the local area code for 10-digit local calls.
LOCAL-DIRECT-DIAL	This one-digit code identifies a direct-dialed local call. NANP calls use 1 for this code.
LOCAL-OPERATOR	This one-digit code identifies an operator-assisted local call. NANP calls use 0 for this code.
LONG-DISTANCE-DIRECT-DIAL	This one-digit code identifies a direct-dialed, long-distance call. NANP calls use 1 for this code.
LONG-DISTANCE-OPERATOR	These one- or two-digit codes identify an operator-assisted, long-distance call within the NANP. Operator-assisted calls use 0 for this code, and operator access uses 00.
NATIONAL-NUMBER	This tag specifies the nation-specific part of the digit string for an international call.
OFFICE-CODE	This tag designates the first three digits of a seven-digit directory number in the form [2-9]XX.
SATELLITE-SERVICE	This one-digit code provides access to satellite connections for international calls.

Tag	Description
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 18: 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.

Operator	Description
==	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 195
- Example of Pre-dot Digit Removal, on page 197
- Example of Digit Prefixing, on page 197
- Example of On-Net and Off-Net Patterns, on page 198
- Example of Block and Route Patterns, on page 198

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 19: 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.

Character	Description	Examples
!	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 91999999999999999999.
?	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 91999999999999999999.
+	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 91999999999999999999.
[ ]	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.

Character	Description	Examples
.	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.

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 211.

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 200	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.
Step 2	Configure a Time Schedule, on page 200	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 200	Associate time schedules with partitions to determine where calling devices search when

	Command or Action	Purpose
		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*.
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.

Troubleshooting with Dialed Number Analyzer

Dialed Number Analyzer installs as a feature service along with Cisco Unified Communications Manager. The tool allows you to test a Cisco Unified Communications Manager dial plan configuration before deploying it. You can also use the tool to analyze dial plans after the dial plan is deployed.

Because a dial plan can be complex, involving multiple devices, translation patterns, route patterns, route lists, route groups, calling and called party transformations, and device level transformations, a dial plan may contain errors. You can use Dialed Number Analyzer to test a dial plan by providing dialed digits as input. The tool analyzes the dialed digits and shows details of the calls. You can use these results to diagnose the dial plan, identify problems if any, and tune the dial plan before you deploy it.

For details on how to set up and use the Dialed Number Analyzer, refer to the document *Dialed Number Analyzer 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.

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.

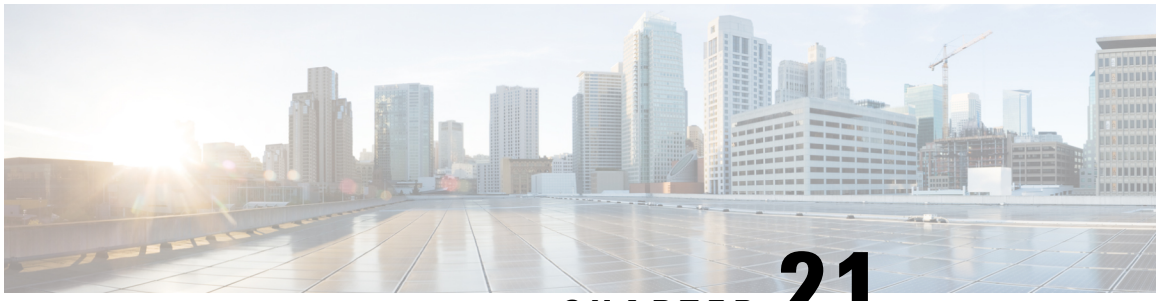
Procedure

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 212	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 212	Configure a hunt list with a prioritized order of line groups.
Step 3	Configure Hunt Pilots, on page 213	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 214.

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 20: 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 91999999999999999999.
?	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 9199999999999999999999.
+	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 9199999999999999999999.

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

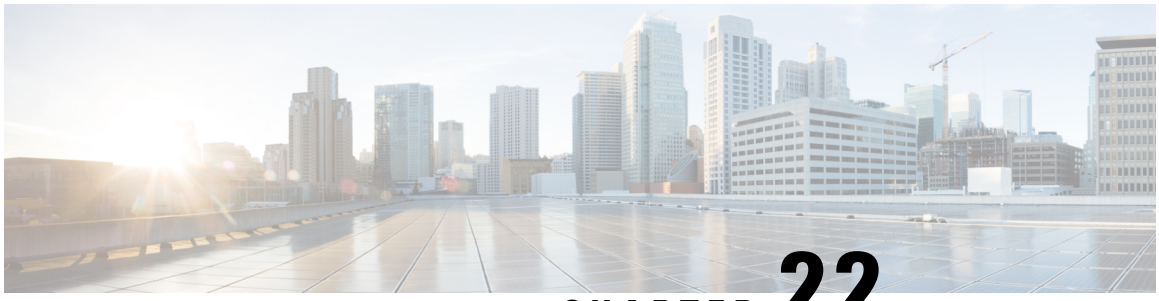
Feature	Interactions and Restrictions
Single Number Reach with Hunt Groups	If you have a hunt group configured and one or more of the directory numbers that the hunt group points toward also has Single Number Reach (SNR) enabled, the call does not extend to the SNR remote destinations unless all devices 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 21: 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 Intercluster Lookup Service

ILS Overview

The Cisco Intercluster Lookup Service (ILS) makes it easy to create a multi-cluster network of remote Cisco Unified Communications Manager clusters that share data.

ILS eliminates the need for an administrator having to configure connections between clusters manually. Once you have ILS configured on a hub cluster, you can connect new clusters by enabling ILS on the new cluster and pointing the new cluster to an existing hub. ILS connects the clusters automatically and lets both clusters know the topology of the larger ILS network.

ILS Network Components

An ILS network comprises the following components:

- **Hub clusters**—Hub clusters form the backbone of an ILS network using automesh functionality to create a full mesh topology with the other hub clusters. Hub clusters relay and share information across the ILS network for a variety of features.
- **Spoke clusters**—Spoke clusters connect only to their local hub cluster and never contact other hub or spoke clusters directly. Spoke clusters rely on their local hub to share and relay information across the network.
- **Global dial plan imported catalogs**—This optional component applies if you have Global Dial Plan Replication configured, and you are interoperating with a Cisco TelePresence Video Communications Server, or a third-party call control system. Import a directory URI or +E.164 number catalog manually from a CSV file that was exported from the other system, thereby allowing users in the ILS network to call users from the other system.

Cluster View

The remote cluster view functionality of ILS can be used to map the network. Each cluster exchanges update messages, called peer info vectors, that 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

Feature Support

Features such as Global Dial Plan Replication and Extension Mobility Roaming are dependent on ILS to create intercluster networks where the clusters share dial plan information. This lets you set up intercluster call networks with video calling, URI dialing, and intercluster mobility.

ILS is also used by Centralized Deployments of the IM and Presence Service if you are connecting the IM and Presence central cluster to multiple telephony clusters. ILS is used to create the connections between the IM and Presence central cluster and the telephony clusters.

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 20 spoke clusters per hub, up to a 200 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 20 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 Configuration Task Flow

Complete these tasks to set up your ILS network.

Before you begin

Make sure to plan our your ILS topology so that you know which clusters will be hub clusters and which will be spoke clusters.

Procedure

	Command or Action	Purpose
Step 1	Configure Cluster IDs, on page 221	Each cluster within the ILS network must have a unique Cluster ID
Step 2	Configure ILS, on page 221	Configure and activate ILS in the various clusters of your network.
Step 3	Verify that ILS is Running, on page 222	Confiirm that the ILS network is up and running.
Step 4	Configure Remote Cluster View, on page 223	Configure the remote cluster view for your ILS network.

Configure Cluster IDs

Each cluster within the ILS network must have a unique Cluster ID. ILS does not work if your remote clusters retain the default **StandAloneCluster** value for the cluster ID.

Procedure

Step 1 Log in to Cisco Unified CM Administration on the publisher node.

Step 2 Choose **System** > **Enterprise Parameters**.

Step 3 Set the value of the **Cluster ID** to a value that uniquely identifies the cluster.

Step 4 Click **Save**.

Step 5 Repeat this procedure on the publisher node of each cluster.

Configure ILS

Use this procedure to activate and configure the Intercluster Lookup Service (ILS) in your network.

Note The first cluster that you configure must be a hub cluster.

Procedure

Step 1 Log into Cisco Unified CM Administration on the publisher node.

Step 2 Choose **Advanced Features** > **ILS Configuration**.

Step 3 From the **Role** drop-down list box, select **Hub Cluster** or **Spoke Cluster** depending on which type of cluster you are setting up.

Step 4 If you want to enable Global Dial Plan Replication, check the **Exchange Global Dial Plan Replication Data with Remote Clusters** check box.

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.

Step 5 Configure **ILS Authentication Details** between the various clusters in the network:

- For TLS authentication, check the **Use TLS Certificates** check box. Note that if you choose this option, you must also exchange CA-signed certificates between the nodes in your cluster.
- For password authentication (regardless of whether TLS is used), check the **Use Password** check box and enter the password details.

Step 6 Click **Save**.

Step 7 In the **ILS Cluster Registration** popup, configure your registration details:

a) In the **Registration Server** text box, enter the publisher node IP address or FQDN for the hub cluster to which you want to connect this cluster. If this is the first hub cluster in your network, you can leave the field blank

b) Make sure that the **Activate the Intercluster Lookup Service** on the publisher in this cluster check box is checked.

c) Click **OK**.

Step 8 Repeat this procedure on the publisher node of each cluster that you want to add to the ILS network. Add the new cluster as a hub or spoke cluster.

Note Depending on the sync values that you configured, there may be a delay while the cluster information propagates throughout the network.

If you chose 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 of each cluster to a central location
- Consolidate exported certificates in the ILS network
- Import certificates onto the publisher node of each cluster in your network

For details, see the "Manage Certificates" chapter of the *Administration Guide for Cisco Unified Communications Manager*.

Verify that ILS is Running

Confirm that your ILS network is up and running.

Procedure

Step 1 Log in to the publisher node on any of your telephony clusters.

Step 2 From Cisco Unified CM Administration choose **Advanced Features** > **ILS Configuration**.

Step 3 Check the **ILS Clusters and Global Dial Plan Imported Catalogs** section. Your ILS network topology should appear.

Configure Remote Cluster View

Use this procedure to configure remote cluster view for the ILS network.

Procedure

Step 1 In Cisco Unified CM 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.

Step 4 Click **Save**.

ILS Interactions and Restrictions

ILS Interactions

Table 22: 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.

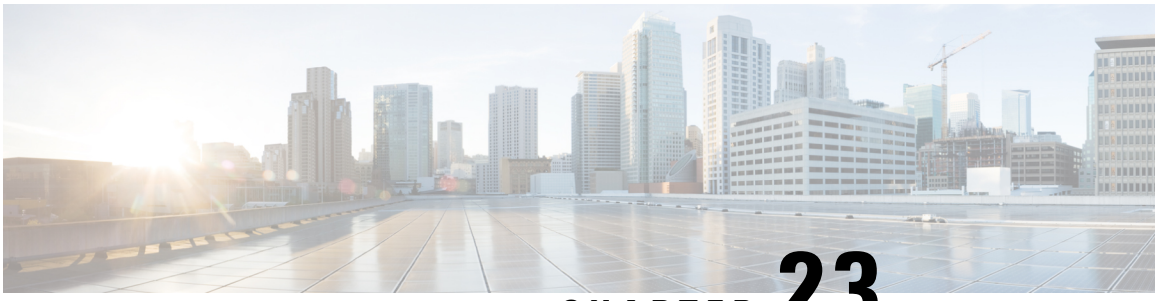
Feature	Interaction
Global Dial Plan Replication	When Global Dial Plan Replication is enabled across an ILS network, remote clusters in an ILS network share global dial plan data, including the following: • Directory URIs • Alternate numbers • Alternate number patterns • Route strings • PSTN failover 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 23: 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.

Restriction	Description
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 23

Configure Global Dial Plan Replication

Global Dial Plan Replication Overview

Global Dial Plan Replication makes it easy to set up an intercluster VoIP network with video calling that uses either URI dialing, enterprise numbers or E.164 numbers for dialing.

Global Dial Plan Replication leverages the Cisco Intercluster Lookup Service by replicating global dial plan data elements to the remote clusters in an ILS network. Each cluster in the ILS network learns the Global Dial Plan elements of the other clusters, along with the route string for the home cluster.

Advertised Globally via ILS

Global Dial Plan Replication advertises the following dial plan elements to the ILS network, replicating this data in remote clusters:

- **Directory URIs**—In the local cluster, provision email-style directory URIs (e.g. alice@cisco.com). URI dialing provides a user-centric method of placing calls. Global Dial Plan Replication lets you advertise the local catalog of directory URIs to the other clusters in the ILS network to enable intercluster URI dialing.
- **Enterprise and E.164 Alternate Numbers**—Alternate numbers are aliases of the original extension that are created by applying a mask with prepend digit instructions to the original directory number. Alternate numbers can be dialed from anywhere within an ILS network. There are two types of alternate numbers. You can provision alternate numbers in the local cluster and then either advertise each numbers to the ILS network or configure advertised number patterns that summarize a range of alternate numbers, and advertise the pattern to the ILS network.
- **Advertised patterns**—Advertised patterns summarize a range of enterprise alternate numbers or +E.164 alternate numbers. You can replicate the pattern throughout an ILS network, rather than individual alternate numbers in order to save database space in the remote cluster. Advertised patterns are only used from remote clusters in the ILS network—you cannot use these patterns to route local calls.
- **PSTN failover numbers**—This option lets you assign the Enterprise Alternate Number or E.164 Alternate Number as a PSTN failover number. If call routing to a global dial plan element fails via VoIP channels,

the failover number provides an alternate routing method. In the remote cluster, you must configure route patterns that route the PSTN failover to an appropriate gateway.

- **Route string**—Each cluster has a route string that gets replicated with along with the global dial plan catalog. The route string identifies the home cluster for a directory URI or alternate number. For intercluster calling, you must configure SIP route patterns in each remote cluster that route the route string back to its home cluster.
- **Learned Global Dial Plan Data**—To ensure that replicated data reaches all clusters in the ILS network, each cluster replicates its locally provisioned global dial plan data, along with catalogs that were learned from other clusters.
- **Imported Global Dial Plan Data**— If you are interoperating Cisco Unified Communications Manager with a Cisco TelePresence Video Communications Server, or a third-party call control system, export global dial plan data from the other system to a csv file, and then import that csv file into a hub cluster in the ILS network. Global Dial Plan Replication replicates the imported catalog to other clusters in the ILS network, allowing you to place calls to directory URIs and alternate numbers that are registered to the other system.

Sample Global Dial Plan Mapping

The following example shows sample Global Dial Plan data elements that map to phone extension 4001. Assuming call routing is configured correctly, dialing any of these numbers will ring extension 4001.

- Enterprise Alternate Number—A number mask of 5XXXX applied to extension 4001 creates an enterprise alternate number of 54001.
- E164 Alternate Number—A number mask of 1972555XXXX applied to extension 4001 creates an +E.164 alternate number of 19725554001.
- PSTN Failover—Assign the enterprise alternate Number or +E.164 alternate number as the PSTN failover and route the call to an appropriate gateway.
- Advertised Pattern—The pattern 54XXX can be used to summarize all Enterprise Alternate Numbers in the 54000-54999 range. You can create patterns for Enteprise and +E.164 alternate numbers.
- Directory URIs—alice@cisco.com

Note Directory URIs can be assigned to a directory number or to an end user. Directory URIs that are associated to an end user will also associate to the user's primary extension (a directory number) and will ring the primary extension, provided it is assigned.

URI Dialing

URI dialing is a subfeature of Global Dial Plan Replication that allows callers to place calls using directory URIs as the dial string. A directory URI is an alphanumeric text string that looks like an email addresses (for example, alice@cisco.com).

Although the URI resembles an email address, a directory URI is not a routable entity by itself. For local calling, calls to directory URIs can be routed so long as the directory URI is in a partition that is within the

caller's calling search space. For intercluster calls, the system pulls the cluster route string that was replicated with Global Dial Plan Replication and tries to match a SIP route pattern to the route string.

Directory URI Types

There are two types of directory URIs, with the type being determined by how you provision the directory URI:

- User-based URIs—The directory URI is assigned to a user in **End User Configuration**. All of these URIs get assigned automatically to the local directory URI partition, which is a local nondeletable partition. If the user also has a primary extension, the URI also appears in **Directory Number Configuration** as the Primary URI for that extension.
- Line-based URIs—Up to five additional directory URIs can be assigned directly to a directory number in the **Directory Number Configuration** window. For these URIs, you can assign any local partition.

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

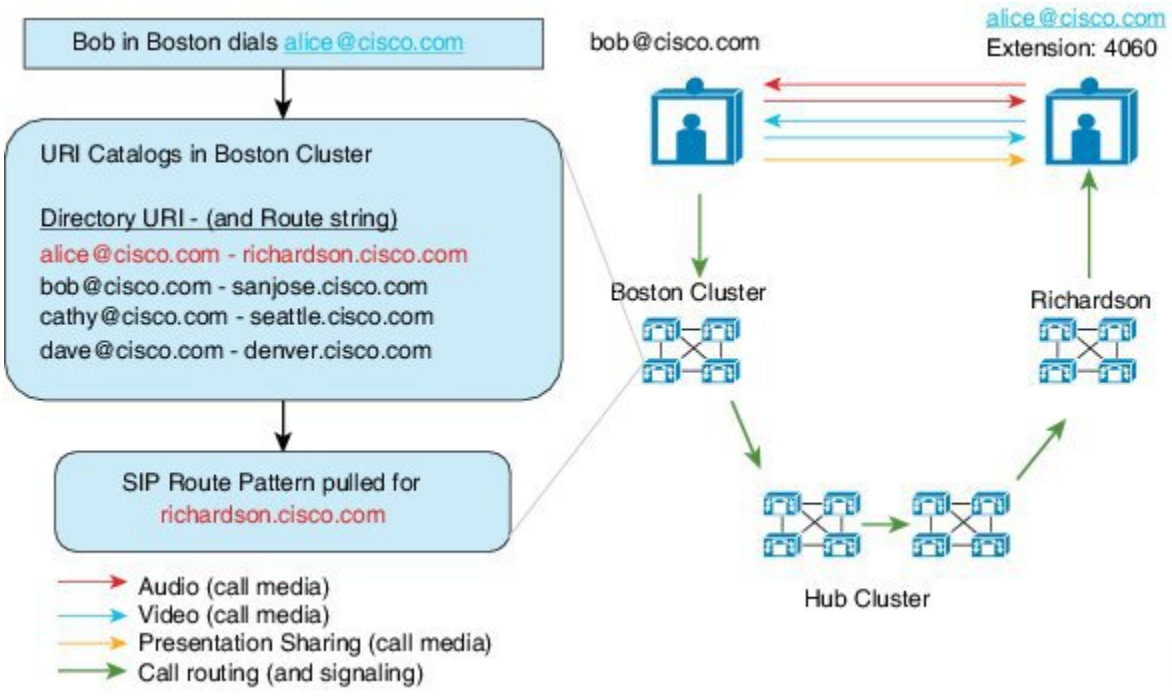
- Call-forwarding to URIs won't be possible from physical phones.
- Call-forward to a URI can only be configured through applications if that URI is already in the Unified Communications Manager database. If the URI is not in the database, then the application will error out "Call Forward Setting Failed /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".

Call Routing for Global Dial Plan Replication

For intracluster calling, Global Dial Plan Data is routed via partitions and calling search spaces. For calls to a local directory URI, enterprise alternate number or E.164 alternate number to work, the URI or number must be present in a partition that is in the calling search space that the calling party is using.

Intercluster calling uses the cluster route strings that Global Dial Plan Replication advertises to send the call to the called party's home cluster. When a caller places a call to a directory URI or alternate number that is homed in another cluster, the system pulls the associated route string, matches a SIP route pattern for the route string, and sends the call to the destination that the SIP route pattern specifies. For this to work, you must configure SIP route patterns in your remote clusters to route the route string back to its home cluster.

If call routing fails, the system can also use the associated PSTN failover number. However, you will need to configure route patterns in the remote cluster so that PSTN failover calls can be sent to the appropriate gateway.



Global Dial Plan Replication Prerequisites

You must:

- Configure the Cisco Intercluster Lookup Service (ILS)
- Plan how you are going to deploy your global dial plan:
  - Will you deploy URI dialing by provisioning directory URIs for your users? You can use Global Dial Plan Replication to replicate directory URIs across the ILS network.
  - Will you deploy alternate number dialing? Will you use enterprise alternate numbers or E.164 alternate numbers? Which will you use as the PSTN failover?
  - If you are deploying alternate numbers, plan your numbering plan. For large networks, you can save on database space and bandwidth by advertising number patterns to the ILS network rather than individual alternate numbers.

Global Dial Plan Replication Configuration Task Flow

Complete these tasks to configure Global Dial Plan Replication and URI dialing. You must complete these tasks in each cluster of the ILS network.

Procedure

	Command or Action	Purpose
Step 1	Enable ILS Support for Global Dial Plan Replication, on page 233	Enable support for Global Dial Plan Replication in the local cluster.
Step 2	Configure SIP Profiles, on page 233	Configure SIP settings that support Global Dial Plan Replication and URI Dialing.
Step 3	Configure SIP Trunks for URI Dialing, on page 233	For URI dialing, configure whether the system inserts a directory URI, directory number, or blended address in Contact headers.
Step 4	Configure SIP Route Patterns, on page 234	For intercluster routing, configure SIP route patterns in each cluster that route the learned route strings back to their home clusters.
Step 5	Set Database Limits for Learned Data, on page 235	Set the upper limit for the amount of data that ILS can write to the local database.
Step 6	Assign Partitions for Learned Numbers and Patterns, on page 236	Assign route partitions for enterprise alternate numbers, +E.164 alternate numbers, and learned number patterns.
Step 7	Set Up Advertised Pattern for Alternate Numbers, on page 236	Optional. Advertise a number pattern that summarizes a range of enterprise or +E.164 alternate numbers.
Step 8	Block a Learned Pattern, on page 237	Optional. Configure a pattern that blocks calls to a specific number or number pattern. This configuration is applied locally, and is not replicated to the ILS network.
Step 9	Import Global Dial Plan Data, on page 239	Optional. If you are interoperating with a Cisco TelePresence Video Communications Server or third-party call control system, import a catalog of directory URIs, +E.164 Numbers and PSTN failover numbers from the other system into a hub cluster in the ILS network.
Step 10	Provision Global Dial Plan Data, on page 237	Assign directory URIs, enterprise alternate numbers, and +E.164 alternate numbers to a directory number. **Note** For multiple users, use an LDAP directory sync or Bulk Administration to assign global dial plan data for a large number of users in a single operation. Refer to the Provisioning Users section of this guide.

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**.

Configure SIP Profiles

Use this procedure to edit the SIP Profiles in your network to support Global Dial Plan Replication and URI dialing.

Procedure

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

Step 2 Click **Find** and select an existing SIP Profile.

Step 3 From the **Dial String Interpretation** drop-down, configure the policy the system uses to determine whether to route calls as directory URIs or as directory numbers:

- Always treat all dial strings as URI addresses
- Phone number consists of characters 0–9, A–D, *, and + (others treated as URI addresses).
- Phone number consists of characters 0-9, *, and + (others treated as URI addresses)—This is the default option.

Step 4 Check the **Use Fully Qualified Domain Name in SIP Requests** check box.

Step 5 Optional. Under **Trunk-Specific Configuration**, check the **Send ILS Learned Destination Route String** check box if you want to be able to route intercluster calls across a Cisco Unified Border Element.

Step 6 Click **Save**.

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

For intercluster call routing with Global Dial Plan Replication and URI dialing, you must configure SIP route patterns that route the learned route strings back to their home clusters.

Procedure

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

Step 2 Click **Add New**.

Step 3 From the **Pattern Usage** drop-down, select **Domain Routing**.

Step 4 Depending on whether you are deploying IPv4 or IPv6, enter the route string in the **IPv4 Address** or **IPv6 Address** text box.

Step 5 Under **SIP Trunk/Route List**, select a SIP trunk or route list that leads to the next- hop cluster for the route back to the route string's home cluster.

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

Step 7 Click **Save**.

Step 8 Create SIP route patterns for each learned route string.

Step 9 Repeat these tasks for each cluster in the ILS network.

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 is 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

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.

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.

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**.

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**.

Provision Global Dial Plan Data

Use this procedure to add directory URIs, enterprise alternate numbers, +E.164 alternate numbers and PSTN failover rules to a directory number.

Note If you have a large number of users, configure universal line templates and apply them with provisioning tools such as LDAP sync or Bulk Administration to provision global dial plan data for a large number of users in a single operation. See the Provisioning Users section of this book.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Directory Number**.

Step 2 Do either of the following:

- Click **Find** and select an existing directory number for which you want to add global dial plan data.
- Click **Add New** to create a new directory number.

Step 3 If you are creating a new number, enter the **Directory Number** and click **Save**.

Step 4 To add an enterprise alternate number click the the **Add an Enterprise Alternate Number** button and do the following:

a) Enter a **Number Mask**. For example, 5XXXX as an alternate number for 4001. The resulting enterprise alternate number (54001) displays in the **Alternate Number** field.
b) Check the **Add to Local Route Partition** check box to add to a local route partition.
c) From the **Route Partition** drop-down, select the partition.
d) Check **Advertise Globally via ILS** if you want this alternate number to be advertised to the ILS network.

Note If you configure an advertised pattern where the enterprise alternate number or +E.164 alternate number falls within the range of the pattern, then you don't need to advertise the alternate numbers individually.

Step 5 To add an +E.164 Alternate Number, click the **Add an +E.164 Alternate Number** and do the following:

a) Enter a **Number Mask**. For example, 1972555XXXX as an alternate number for extension 4001. The resulting +E.164 alternate number (19725554001) displays in the **Alternate Number** field.
b) Check the **Add to Local Route Partition** check box to add to a local route partition.
c) From the **Route Partition** drop-down, select the partition.
d) Check **Advertise Globally via ILS** if you want this alternate number to be advertised to the ILS network.

Step 6 In the **Directory URIs** section, add directory URIs to this directory number:

a) In the **URI** field, enter the directory URI. For example, alice@cisco.com.
b) From the **Partition** drop-down, assign the directory URI to a local partition.
c) Check the **Advertise Globally via ILS** check box to include this directory URI in advertised catalogs.
d) Click **Add Row** to add additional directory URIs. You can add up to five directory URIs.

Step 7 In the **Advertised Failover Number** field, select either the Enterprise Alternate Number or +E.164 Alternate Number as a PSTN failover.

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

Step 9 Click **Save**.

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.

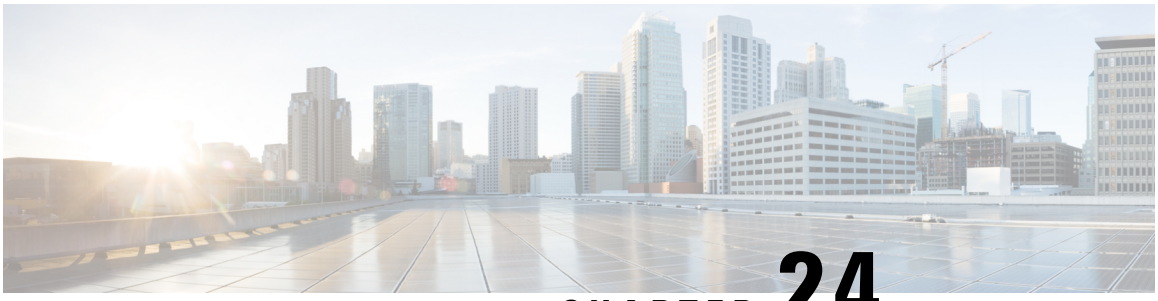
Global Dial Plan Replication Interactions and Restrictions

The following table summarizes some of the feature interactions for Global Dial Plan Replication and URI dialing.

Feature	Interactions and Restrictions
Export Directory URIs and +E.164 Patterns	You can also export all directory URIs and +E.164 number patterns that were configured in the local cluster, and export them to a csv file that you can import into another system. 1. In Cisco Unified CM Administration, choose **Bulk Adminstration** > **Directory URIs and Patterns** > **Export Local Directory URIs and Patterns**. 2. Click one of the following radio buttons to define the domain name that you want to attach to the export file: • **Organizational Top Level Domain**—Click this radio button to use the value of the Organizational Top Level Domain enterprise parameter for the export file domain name. • **Route String Domain**—Click this radio button to use the value of the Route String field, as configured in ILS Configuration, for the export file domain name. • **User Defined Domain**—Click this radio button to create a customized domain name to attach to the export file. If you choose this option, enter the domain name in the **Domain Name** text box. 3. Click the **Export Local Directory URIs and Patterns** button. 4. Save the CSV file to a local drive

Feature	Interactions and Restrictions
Partitioning with URI Dialing	Partitioning with directory URIs depends on how you provision the directory URI. • For user-based directory URIs that are assigned to an end user in **End User Configuration**, the local nondeletable Directory URI partition is assigned to the URI automatically. You cannot assign another partition, but you can use an administrator-managed partition as an alias for the local Directory URI partition by configuring the **Directory URI Alias Partition** enterprise parameter. • For line-based directory URIs where the URI is assigned directly to a directory number in **Directory Number Configuration**, you can assign each URI to a local partition separately. If you are using tools like LDAP sync and Bulk Administration to provision directory URIs: • Directory URIs that are provisioned via an LDAP sync are user-based and get assigned to the user in **End User Configuration**. These URIs are assigned to the local Directory URI partition. If the user has a primary extension, the URI also appears in **Directory Number Configuration** as the Primary URI. However, the assigned partition is the Directory URI partition. • For directory URIs that are provisioned via Bulk Administration, it depends on how your updates are applied. For example, if you use the `bat.xlt` spreadsheet to create a csv import file, the user will be a user-based URI if you use the **Users** or **Update Users** tabs on the spreadsheet to add the directory URI. However, if you add the directory URI via the **Line Fields** options that appear when you click **Create File Format**, you can assign the URI to a directory number and assign a local partition to the URI directly.
Directory URI Case Sensitivity	By default, the user portion of a directory URI (the portion before the @) is case sensitive. You can make the user portion case insensitive by editing the URI Lookup Policy enterprise parameter.
Calling Search Space	To be dialable, directory URIs, enterprise alternate numbers, and +E.164 alternate numbers must be in a partition that is available in the calling party's calling search space.

Feature	Interactions and Restrictions
Digit Transformations with URI dialing	If you use digit transformations, and you are deploying intercluster URI dialing, apply digit transformations against either the phone configuration or against the device pool that the phone uses. • For individual phones, apply the transformation to the **Calling Party Transformation CSS** field in the **Remote Number** section. • For device pools, you can apply the transformation against the **Calling Party Transformation CSS** field under **Device Mobility Related Information**. **Note** For roaming devices, the device pool setting overrides the phone configuration even if the **Use Device Pool Calling Party Transformation CSS** check box is unchecked in the **Phone Configuration** window.



CHAPTER 24

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 245	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 246	Set up your partitions and calling search spaces.
Step 4	Create Calling Party Transformation Patterns, on page 246	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 247	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 24: 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.

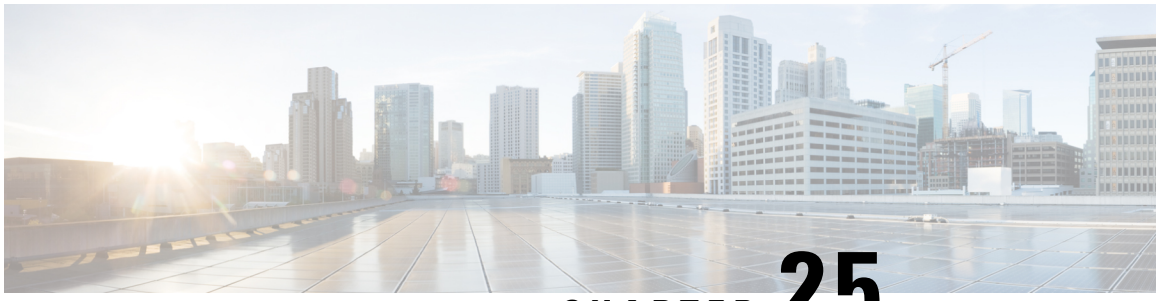
Calling Party Normalization Restrictions

The following table displays restrictions that the Calling Party Normalization feature has with certain features and system components of Cisco Unified Communications Manager.

Table 25: 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 25

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, 7970, and 7971

Dial Rules Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure Application Dial Rules, on page 254	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 255	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 255	Use SIP dial rules configuration to configure dial plans for phones that are running SIP.
Step 4	Reprioritize Dial Rule, on page 258	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 255
- Configure SIP Dial Rules, on page 255

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 255

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 257	Configure and update SIP dial rules and associate them with the phones that are running SIP.
Step 2	Reset SIP Dial Rule, on page 257	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 258	(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 256

Pattern Formats

Table 26: 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 257

Related Topics

Pattern Formats, on page 256

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 257

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 258

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 257

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, 7970, and 7971 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.

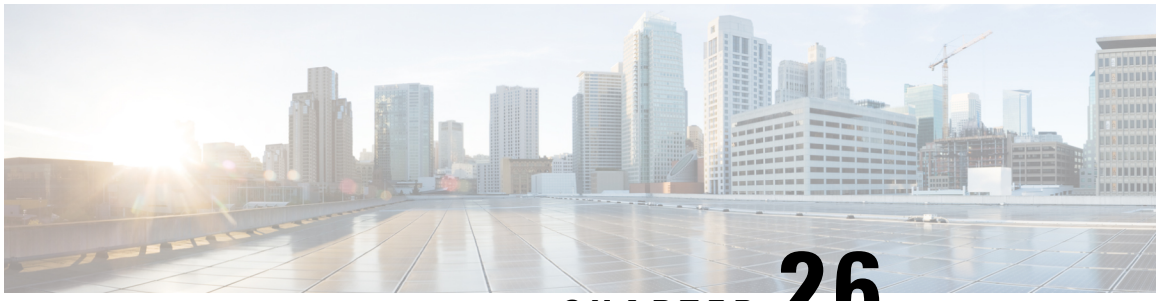
Directory Lookup Dial Rules Restrictions

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.

PART III

Integrate Applications



CHAPTER 26

Integrate Cisco Applications

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.

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

Cisco Expressway

Cisco Unified Communications Manager integrates with Cisco Expressway to provide Cisco Unified Communications Mobile and Remote Access. Cisco Unified Communications 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 provided by Cisco Unified Communications Manager (Unified CM) when the endpoint is not within the enterprise network. The Expressway provides secure firewall traversal and line-side support for Unified CM registrations.

The overall solution provides the following functions:

- Off-premises access—A consistent experience outside the network for Cisco 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.

For deployment details, refer to the *Mobile and Remote Access Through Cisco Expressway Deployment Guide* at https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html.

Cisco Emergency Responder

Cisco Emergency Responder (Emergency Responder) helps you manage emergency calls in your telephony network so that you can respond to these calls effectively and so that you can comply with local ordinances concerning the handling of emergency calls. In North America, these local ordinances are called “enhanced 911,” or E911. Other countries and locales have similar ordinances.

Because emergency call ordinances can differ from location to location within a country, region, state, or even metropolitan area, Emergency Responder gives you the flexibility to configure your emergency call configuration to specific local requirements. However, ordinances differ from location to location, and security requirements differ from company to company, so you must research your security and legal needs before deploying Emergency Responder.

For details on how to install Cisco Emergency Responder and integrate it with Cisco Unified Communications Manager, refer to *Cisco Emergency Responder Administration Guide* at https://www.cisco.com/c/en/us/support/unified-communications/emergency-responder/products-maintenance-guides-list.html

Feature Support from Cisco Unified Communications Manager

The following Cisco Unified Communications Manager features support integrations with Cisco Emergency Responder. For details on how to configure these features on Cisco Unified Communications Manager, refer to the *Feature Configuration Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

- Location Awareness
- Emergency Handler

Cisco Paging Server

Cisco Unified Communications Manager can be configured to integrate with Cisco Paging Server to provide basic paging services for Cisco IP Phones and a variety of endpoints. The Cisco Paging Server product is offered through the InformaCast Virtual Appliance and offers the following deployment options:

- Basic Paging—Provides phone-to-phone and group live audio paging to Cisco IP Phones. All users of the system can participate in making and receiving basic pages.
- Advanced Notifications—Provides a full-featured emergency notification solution that gives you the ability to reach an unlimited number of phones with text and live or pre-recorded audio messages

For more information and documentation on Cisco Paging Server, see https://www.cisco.com/c/en/us/products/unified-communications/paging-server/index.html.

Configuration

For details on how to configure Cisco Unified Communications Manager for Basic Paging or Advanced Notifications, see the "Paging" chapter of the *Feature Configuration Guide for Cisco Unified Communications Manager*.

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.

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.

Advanced QoS APIC-EM Controller

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.

Configuration Details

For additional details, including information on how to configure Cisco Unified Communications Manager to integrate with an APIC_EM Controller, refer to the "Configure QoS with APIC-EM Controller" chapter of the *Feature Configuration Guide for Cisco Unified Communications Manager*.

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.

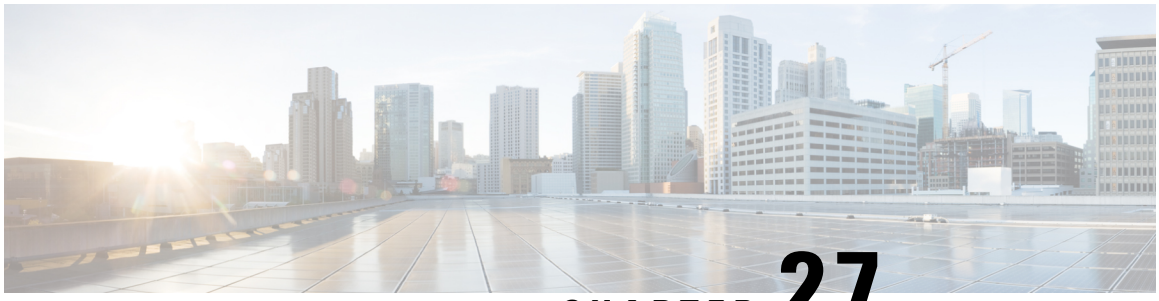
< None > indicates the WebDialer Server would apply to all nodes.

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 27

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 274	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 274	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 275 • Configure New Call Accept Timer, on page 275 • Configure Simultaneous Active Calls, on page 276 • Synchronize CTI Route Point, on page 276	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 277	Configure the directory number for the CTI device.
Step 5	Associate Devices with Groups, on page 277	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 277	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 279	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 275	Add a new, or modify an existing CTI route point.
Step 2	Configure New Call Accept Timer, on page 275	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 276	Configure the number of simultaneous active calls on the route point.
Step 4	**Optional**: Synchronize CTI Route Point, on page 276	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**.

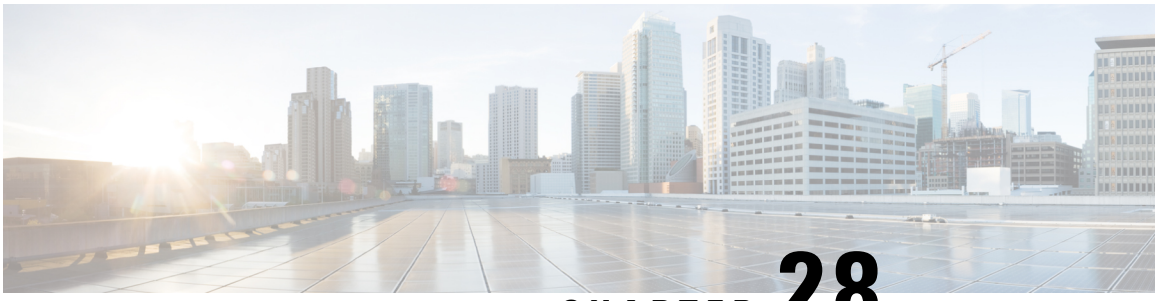
Step 5 In the **Application Heartbeat Minimum Interval** field, enter the time for the minimum interval. The default is 5.

Step 6 In the **Application Heartbeat Maximum Interval** field, enter the time for the maximum interval. The default is 3600.

Step 7 Click **Save**.

PART IV

Provisioning End Users



CHAPTER 28

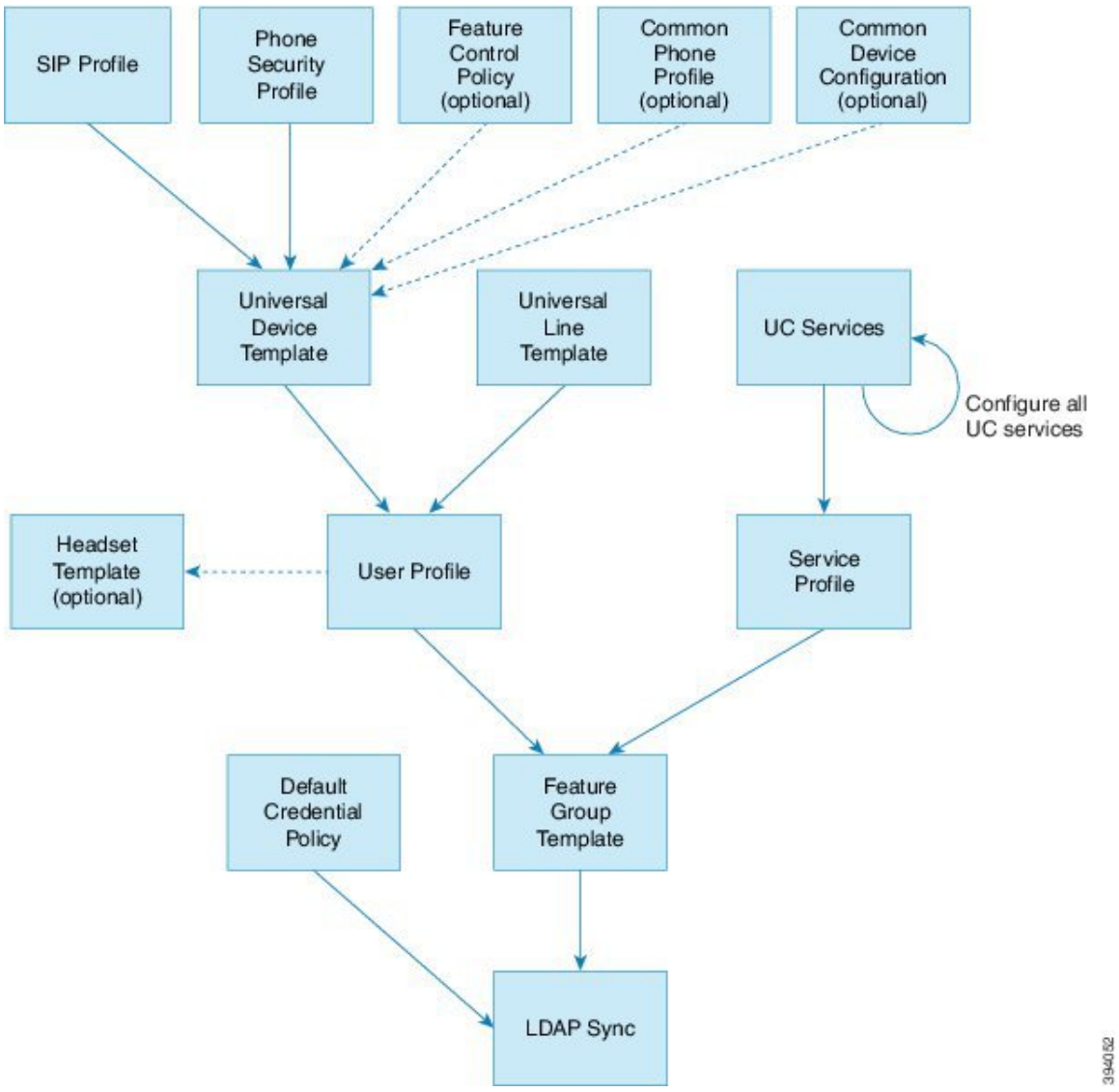
Configure Provisioning Profiles

Provisioning Profiles Overview

Unified Communications Manager contains a set of profiles and templates that you can assign to new users. If you set these profiles and common settings beforehand, when you provision new users, and assign devices, users and devices will be configured automatically based on the settings that are applied.

When you provision users, associate them to the User Profile and Service Profile that contain the settings they need. In addition, when you add devices for users, their device and directory number will be configured quickly using the Universal Line and Universal Device Templates that are associated to the user's User Profile.

You can use the following profiles and templates to apply common settings to users and endpoints based on the user needs.



Provisioning Profiles Task Flow

If you have a large number of users and devices to provision, you can simplify the configuration process by setting up user profiles and service profiles with templates and common settings that apply for users in a specific group (for example, customer support).

When you provision users, associate them to the User Profile and Service Profile that contain the settings they need. In addition, when you add devices for users, their device and directory number will be configured quickly using the Universal Line and Universal Device Templates that are associated to the user's User Profile.

You can use the following profiles and templates to apply common settings to users and endpoints based on the user needs.

Procedure

	Command or Action	Purpose
Step 1	Configure SIP Profile, on page 286	Set up common SIP settings that will be associated with the SIP endpoints that you deploy.
Step 2	Configure Phone Security Profile, on page 287	Configure security profiles that you will assign to provisioned endpoints. Assign settings such as TLS and TFTP encryption.
Step 3	Create a Feature Control Policy, on page 287	**Optional**. Use this policy to enable particular features and control the appearance of phone softkeys.
Step 4	Create a Common Phone Profile, on page 288	**Optional**. Use this profile to assign TFTP data and product-specific configuration defaults to a profile that you can assign to groups of endpoints.
Step 5	Configure Common Device Configuration, on page 289	**Optional**. Use this configuration to assign user-specific settings and IPv6 preferences to endpoints.
Step 6	Configure a Universal Device Template, on page 289	This template contains common settings that will be used to configure newly provisioned phones. You can also assign the profiles that you've configured to this template.
Step 7	Configure a Universal Line Template, on page 290	This template contains common settings that will used to configure newly provisioned extensions. You can also configure enterprise and E.164 numbers for your extensions.
Step 8	Configure a User Profile, on page 291	Set up a User Profile with the device templates, line templates, and common settings for newly provisioned users.
Step 9	Configure a Headset Template, on page 292	**Optional**. If you plan to use Cisco Headsets configure headset templates and assign them to the User Profiles that you've set up.
Step 10	Configure UC Services, on page 293	Configure UC Services such as the IM and Presence Service and a directory service.
Step 11	Configure a Service Profile, on page 294	Create a Service Profile that includes the UC services you want to assign to provisioned users.
Step 12	Configure a Feature Group Template, on page 294	For LDAP syncs, add your user profile and service profiles to a feature group template that you can assign to LDAP-synced users.

	Command or Action	Purpose
Step 13	Configure Default Credential Policy, on page 295	Configure the credential policy that you will assign to newly provisioned users.

What to do next

- Set up your LDAP sync in order to provision new users
- If you are not deploying LDAP, you can use Bulk Administration to provision users by bulk.

Configure SIP Profile

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

Procedure

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

Step 2 Perform one of the following steps:

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

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

Step 4 If you are deploying URI dialing, configure the **Dial String Interpretation** to instruct the system on whether to handle calls as directory URIs or phone numbers.

Step 5 Under **Parameters Used in Phone**, complete the DSCP settings to define QoS handling for types of calls that use this profile.

Step 6 (Optional) If you need to assign a Normalization Script, select one of the default scripts from the Normalization Script drop-down list.

Note You can also create your own scripts. For details, see the *Feature Configuration Guide for Cisco Unified Communications Manager*.

Step 7 If you want this profile to support both IPv4 and IPv6 stacks simultaneously, check the **Enable ANAT** check box.

Step 8 Check the **Allow Presentation Sharing using BFCP** check box if you want your users to be able to share presentations.

Step 9 Complete the remaining fields in the SIP Profile Configuration window. For help with the fields and their settings, see the online help.

Step 10 Click **Save**.

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**.

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**.

Create a Common Phone Profile

A common phone profile is an optional profile that can be used to configure TFTP data and Product-Specific Configuration defaults for the phones that use the profile.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device > Device Settings > Common Phone Profile** menu path to configure common phone profiles.

Step 2 Click **Add New**.

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

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

Step 5 If you set up a **Feature Control Policy** to phones that use this profile, select the policy from the drop-down list.

Step 6 Complete the remaining fields in the **Common Phone Profile Configuration** window. For help with the fields and their settings, see the online help.

Step 7 Configure fields under Product-Specific Configuration Layout. For field descriptions, click the (?) to see field-specific help.

Step 8 (Optional) If you want to enable Interactive Connectivity Establishment (ICE) for Mobile and Remote Access phones:

a) Set the ICE drop-down to **Enabled**.

b) Set the **Default Candidate Type** to one of the following:

- **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. Often, 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.

c) Configure the remaining ICE fields.

Step 9 Click **Save**.

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 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 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 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.
c) Check the **Allow Provisioning of a phone already assigned to a different End User** check box to determine whether the user who is associated with this profile has the permission to migrate or reassign a device that is already owned by another user. By default, this check box is unchecked.

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 If you want the users in this user profile to set the maximum login time for Extension Mobility or Extension Mobility Cross Cluster through Cisco Unified Communications Self Care Portal, check the **Allow End User to set their Extension Mobility maximum login time** check box.

Note By default **Allow End User to set their Extension Mobility maximum login time** check box is unchecked.

Step 10 Click **Save**.

Configure a Headset Template

Use this procedure to configure a headset template with customized settings that you can apply to Cisco headsets. You can create a customized template or use the system-defined Standard Default Headset Template.

Note The Standard Default Headset Configuration Template is a system-defined template. You can assign new User Profiles to the Standard Default Headset Template but you can't edit the template. By default, all user profiles are assigned to this template. To disassociate a user profile from this template, you must assign the profile to a new template.

Procedure

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

Step 2 Do either of the following:

- To edit an existing template, select the template.
- To create a new template, select any existing template and click **Copy**. The existing settings are applied to your new template.

Step 3 Add a **Name** and **Description** for the template.

Step 4 Under **Model and Firmware Settings**, assign any customized headset settings that you want to apply to this template. To add a new setting, click the **Add** button and configure the settings.

Step 5 Use the up and down arrows to move the User Profiles that you want to assign to this template to the **Assigned Users Profiles** list box. All users whom are assigned to those profiles will also be assigned to this headset template.

Step 6 Click **Save**.

Step 7 Use the **Set to Default** button to return to the default template settings.

Step 8 Click **Apply Config**.

For a Standard Default Headset Configuration Template, the **Apply Config** button takes effect for the following:

- Devices owned by users you added to the Assigned User Profile list

- Anonymous devices

For a Customized Headset Configuration Template, the **Apply Config** button takes effect only for devices owned by users you added to the **Assigned User Profiles** list.

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**.

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.

Configure Default Credential Policy

Use this procedure to configure clusterwide default credential policies that get applied to newly provisioned users. You can apply a separate credential policy for each of the following credential types:

- Application User Passwords
- End User Passwords
- End User PINs

Procedure

Step 1 Configure settings for a credential policy:

a) From Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Credential Policy**.

b) Do either of the following:

- Click **Find** and select an existing credential policy.
- Click **Add New** to create a new credential policy.

c) If you want the system to check for easily hacked passwords such as ABCD or 123456, check the **Check for Trivial Passwords** check box.

d) Complete the fields in the **Credential Policy Configuration** window. For help with the fields and their settings, see the online help.

e) Click **Save**.

f) If you want to create a different credential policy for one of the other credential types, repeat these steps.

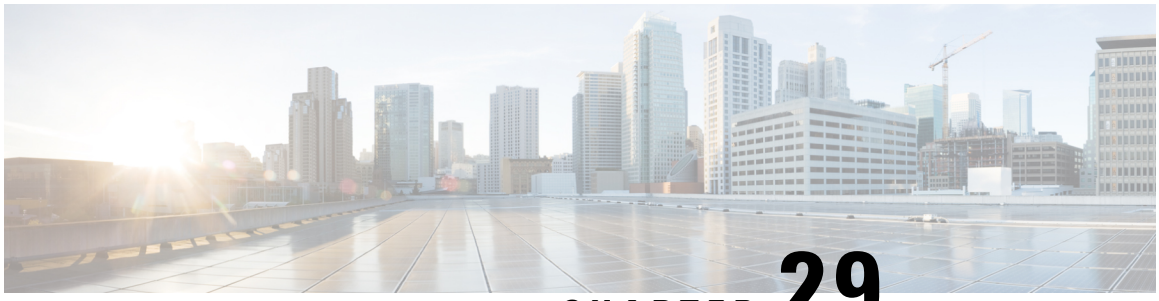
Step 2 Apply the credential policy to one of the credential types:

a) From Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Credential Policy Default**.

b) Select the credential type to which you want to apply your credential policy.

c) From the **Credential Policy** drop-down, select the credential policy that you want to apply for this credential type. For example, you might select the credential policy that you created.
d) Enter the default passwords in both the **Change Credential** and **Confirm Credential** fields. Users have to enter these passwords at next login.
e) Configure the remaining fields in the **Credential Policy Default Configuration** window. For help with the fields and their settings, see the online help.
f) Click **Save**.
g) If you want to assign a credential policy for one of the other credential types, repeat these steps.

Note For individual users, you can also assign a policy to a specific user credential from the **End User Configuration** window or **Application User Configuration** window for that user. Click the **Edit Credential** button that is adjacent to the credential type (password or PIN) to open the **Credential Configuration** settings for that user credential.



CHAPTER 29

Configure LDAP Synchronization

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 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 299	Log in to Cisco Unified Serviceability and activate the Cisco DirSync service.
Step 2	Enable LDAP Directory Synchronization, on page 300	Enable LDAP directory synchronization in Unified Communications Manager.
Step 3	Create an LDAP Filter, on page 300	**Optional**. Create an LDAP filter if you want Unified Communications Manager to synchronize only a subset of users from your corporate LDAP directory.
Step 4	Configure LDAP Directory Sync, on page 301	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 303	**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 303	**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 304	**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**.

Note To search conference rooms represented as Room objects in OpenLDAP Server, configure the custom filter as (| (objectClass=intOrgPerson)(objectClass=rooms)). This allows Cisco Jabber client to search conference rooms by their name and dial the number associated with the room.

Conference rooms are searchable provided **givenName** or **sn** or **mail** or **displayName** or **telephonenumber** attribute is configured in the OpenLDAP server for a room object.

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 304

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

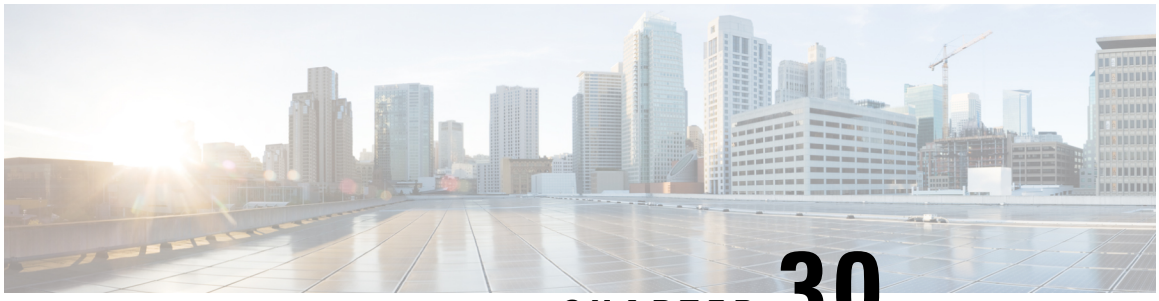
Step 1 From Cisco Unified CM Administration, choose **System** > **Service Parameters**.

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**.



CHAPTER 30

Provisioning Users and Devices Using Bulk Administration Tool

Bulk Administration Tool Overview

The Bulk Administration Tool (BAT) is a web-based application that you can use to perform bulk transactions to the Unified Communications Manager database. You can use BAT to add, update, or delete a large number of similar phones, users, or ports at the same time.

Note The Bulk Administration menu is visible only on the first node of Unified Communications Manager server.

The Cisco Bulk Provisioning Service (BPS) administers and maintains all jobs that are submitted through the Bulk Administration menu of Cisco Unified CM Administration. You can start this service from Cisco Unified Serviceability. You need to activate the Cisco Bulk Provisioning Service only on the first node of Unified Communications Manager.

You can use BAT to perform the following:

- Add, update, or delete large numbers of phones in batches
- Define the common phone attributes to add a group of new phones
- Creates new BAT phone templates
- Adds a group of new users and to associate users to phones and other IP Telephony devices
- Creates User CSV Data File From BAT Spreadsheet
- Creates CSV data file for adding phones and users in batches
- Adds a group of phones and users to the Unified Communications Manager database and directory

Bulk Administration Tool Prerequisites

- Configure User and Service Profiles

Bulk Administration Tool Task Flow

Procedure

	Command or Action	Purpose
Step 1	Add Phones to Database, on page 307	You use BAT to add phones and other IP telephony devices in bulk to the Unified Communications Manager database.
Step 2	Create New BAT Phone Template, on page 307	You can create new BAT phone templates.
Step 3	Create Phone CSV Data File Using BAT Spreadsheet, on page 312	You can add new phones or IP telephony devices to the system using the .xls spreadsheet that was designed for use with BAT.
Step 4	Create Custom Phone File Format Using Text Editor, on page 314	You can use a text editor to create a custom phone file format for the text-based CSV data file.
Step 5	Insert Phones Into Unified Communications Manager, on page 315	You can add phones, Cisco VGC Phones, CTI ports, or H.323 clients into the Unified Communications Manager database.
Step 6	Add Users, on page 317	You can use BAT to add a group of new users and to associate users to phones and other IP Telephony devices.
Step 7	Create User CSV Data File From BAT Spreadsheet, on page 317	You can provide details for adding new users to the Unified Communications Manager database in the BAT spreadsheet and then convert it in to a CSV data file.
Step 8	Insert Users in Unified Communications Manager Database, on page 318	You can add a group of users to the Unified Communications Manager database using a CSV data file.
Step 9	Add Phone and User File Format, on page 320	You can add the phone and user file format with a text-based CSV data file. After the CSV data file is created, you need to associate the file format with the text-based CSV data file.
Step 10	Insert Phones with Users Into Unified Communications Manager, on page 320	You can add a group of phones and users to the Unified Communications Manager database and directory.

Add Phones to Database

When you use BAT to add phones and other IP telephony devices in bulk to the Unified Communications Manager database, you can add multiple lines, services, and speed dials for each phone. You can also add CTI ports and H.323 clients.

You have two options for creating a CSV data file for phones:

- Use the BAT spreadsheet (BAT.xlt) and export the data to the CSV format
- Use a text editor to create a text file in CSV format (for experienced users)

Procedure

Step 1 Choose **Bulk Administration** > **Phones** > **Phone Template**.

The **Find and List Phone Templates** window displays.

Step 2 Create a CSV data file to insert the phone templates.

Perform one of the following options:

a) Create a CSV data file using the BAT spreadsheet.
b) Create a CSV data file using a text editor as follows:

1. Choose **Bulk Administration** > **Phones** > **Phone File Format** > **Create File Format**.
2. Use a text editor and create the CSV data file for phones that follows the file format that you want to use.
3. Choose **Bulk Administration** > **Phones** > **Phone File Format** > **Add File Format** to associate the text-based file format with the CSV data file.

Step 3 Choose **Bulk Administration** > **Phones** > **Validate Phones**.

Step 4 Choose **Bulk Administration** > **phones** > **Insert phones** to insert phone records into the Unified Communications Manager database.

Create New BAT Phone Template

You can create new BAT phone templates. After you create a phone template, you can add lines, services, and speed dials.

Procedure

Step 1 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 displays with fields and default entries for the chosen device type.

Step 5 In the **Template Name** field, enter a name for the template.

The name can contain up to 50 alphanumeric characters.

Step 6 In the Device Information area, enter the phone settings that this batch has in common.

Some phone models and device types do not have all the attributes that the table lists. See, the phone model documentation for information on all the attributes.

Step 7 After you have entered all the settings for this BAT phone template, click **Save**.

When the status indicates that the transaction has completed, you can add line attributes.

Add or Update Phone Lines in BAT Template

You can add one or more lines to the BAT template or to update existing lines. The button template in use for the BAT template determines the number of lines that you can add or update. You can create a primary phone template that has multiple lines. Then, you can use the standard template to add phones with a single line or up to the number of lines in the standard template. All phones or user device profiles in this batch will use the settings that you choose.

Cisco recommends that you use alphanumeric characters for the line template value, so if numbers are given, a chance exists of this conflicting with an actual directory number. This would also avoid conflicts with features such as Call Pickup group number and Call Park number.

The maximum number of lines that display for a BAT template depends on the model and button template that you chose when you created the BAT phone template. For some CiscoUnifiedIPPhone models, you can also add CiscoUnifiedIPPhone services and speed dials to the template.

Procedure

Step 1 Find the Phone Template to which you want to add the line.

Step 2 In the **Phone Template Configuration** window, click **Line [1] Add a new DN**, in the **Associated Information** area.

The **Line Template Configuration** window displays.

Step 3 Enter or choose the appropriate values for the line settings.

Step 4 Click **Save**.

Step 5 To add settings for any additional lines, repeat Step 2, on page 308 through Step 4, on page 308.

If you choose Back to Find/List from the **Related Links** drop-down list box in the upper, right, corner of the **Line Template Configuration** window, the **Find and List Line Template** window displays.

a) To find existing line template, enter the appropriate search criteria and click **Find**.

b) To add a new line template, click **Add New**.

Add or Update IP Services in BAT Template

You can subscribe CiscoUnifiedIPPhone services to the CiscoUnifiedIPPhone models that include this feature directly in the BAT template. To bulk subscribe users or phones to IP services, the IP services must have common service parameters and be subscribed through a phone template. You can not bulk subscribe IP services that have unique service parameters. For services with unique parameters, use the CSV file.

Procedure

Step 1 Find the Phone Template to which you want add an IP service.

Step 2 From the **Phone Template Configuration** window, click **Add a new SURL** in the **Associated Information** area.
A popup window displays. In this window, you can subscribe to CiscoUnifiedIPPhone services that are available.

Step 3 In the **Select a Service** drop-down list box, choose a service to which you want all phones to be subscribed. The **Service Description** box displays details about the service that you choose.

Step 4 Click **Next**.

Step 5 In the **Service Name** field, modify the name of the service, if required.

Step 6 Associate the selected services or add more services to the template.

a) To associate these phone services to the phone template, click **Save**.
b) To add more services, repeat Step 3, on page 309 through Step 6, on page 309.
c) To add all the services to the template, click **Update**.

After you are done adding or updating services for the selected template, proceed to the next step.

Step 7 Close the popup window.

Add or Update Speed Dials in BAT Template

You can add and update speed dials in the BAT template for phones and Cisco VGC phones if the Phone Button Template provides speed-dial buttons. The Phone Button Template in use for the BAT template determines the number of available speed-dial buttons.

Procedure

Step 1 Find the Phone Template to which you want to add speed dials.

Step 2 From the **Phone Template Configuration** window, do one of the following:

a) Click **Add a new SD** in the **Associated Information** area.
b) Choose Add/Update Speed Dials from the **Related Links** drop-down list box in the upper, right-hand corner of the window.

A popup window displays. In this window, you can designate speed-dial buttons for CiscoUnifiedIPPhones and expansion modules.

Step 3 In the **Speed Dial Settings** area, enter the phone number, including any access or long-distance codes, in the **Number** field.

Note When you enter the phone number, it can be followed by Forced Authorized Code (FAC)/Client Matter Code (CMC) if applicable. You can enter the Phone number, FAC, CMC either in sequence or separated by a comma (,). The Speed dial may include any PIN, Password or any other digits to be sent as DTMF digits after the call is connected. If you require a pause while connecting through speed dial, you can enter one or more comma (,) where each comma represents a pause of 2 seconds. DTMF digits will be sent after the call is connected and the appropriate pause duration corresponding to the number of commas is entered.

Step 4 In the **Label** field, enter a label that corresponds to the speed-dial number.

Step 5 In the **Abbreviated Dial Settings** area, you can set abbreviated speed dials for applicable IP phone models. Repeat Step 3, on page 309.

Step 6 Click **Save**.
BAT inserts the speed-dial settings in the template and the popup window closes.

Add or Update Busy Lamp Field in BAT Template

You can add and update busy lamp filed speed dials in the BAT template for phones and Cisco VGC phones if the Phone Button Template provides speed-dial buttons. The Phone Button Template in use for the BAT template determines the number of available BLF SD buttons.

Procedure

Step 1 Find the Phone Template to which you want to add speed dials.

Step 2 In the **Phone Template Configuration** window, do one of the following:

a) Click **Add a new BLF SD** in the **Associated Information** area.

b) Choose Add/Update Busy Lamp Field Speed Dials from the **Related Links** drop-down list in the upper, right-hand corner of the window.

A popup window displays. In this window, you can designate busy lamp field speed-dial (BLF SD) buttons for CiscoUnifiedIPPhones and expansion modules.

Step 3 In the **Speed Dial Settings** area, enter the destination, including any access or long-distance codes, in the **Destination** field.

Step 4 Choose the directory number from the drop-down list. You can click **Find** to search for directory numbers.

Step 5 In the **Label** field, enter a label that corresponds to the BLF SD number.

Step 6 Click **Save**.
BAT inserts the BLF SD settings in the template, and the popup window closes.

Add or Update Busy Lamp Field Directed Call Park in BAT Template

You can add and update busy lamp field (BLF) directed call park in the BAT template for phones and Cisco VGC phones if the Phone Button Template provides speed-dial buttons. The Phone Button Template in use for this BAT template determines the number of available BLF Directed Call Park buttons.

Procedure

Step 1 Find the Phone Template to which you want to add BLF speed directed call park.

Step 2 In the **Phone Template Configuration** window, do one of the following:

a) Click **Add a new BLF Directed Call Park** in the **Associated Information** area.

b) Choose **Add/Update BLF Directed Call Park** from the **Related Links** drop-down list box in the upper, right-hand corner of the window.

A popup window displays. In this window, you can designate BLF Directed Call Park buttons for CiscoUnifiedIPPhones and expansion modules.

Step 3 In the **Unassigned Busy Lamp Field/Directed Call Park Settings** area, choose the directory number from the drop-down list. You can click **Find** to search for directory numbers.

Step 4 In the **Label** field, enter a label that corresponds to the BLF Directed Call Park number.

Step 5 Click **Save**.
BAT inserts the BLF Directed Call Park settings in the template, and the popup window closes.

Add or Update Intercom Template in BAT Template

You can add one or more Intercom templates to the BAT template, or update existing Intercom templates in the BAT template The button template in use for the BAT template determines the number of lines that you can add or update. You can create a standard phone template that has multiple lines. Then, you can use the standard template to add phones with a single line or up to the number of lines in the standard template. All phones or user device profiles in this batch will use the settings that you choose for the intercom template.

We recommend that you use alphanumeric characters for intercom template, so if numbers are given, a chance exists of this conflicting with an actual directory number. This would also avoid conflicts with features such as Call Pickup group number and Call Park number.

The maximum number of lines that display for a BAT template depends on model and button template that you chose when you created the BAT phone template. For some CiscoUnifiedIPPhone models, you can also add CiscoUnifiedIPPhone services and speed dials to the template.

Procedure

Step 1 Find the Phone Template to which you want to add the intercom template.

Step 2 In the **Phone Template Configuration** window, click **Intercom [1] - Add a new Intercom** in the **Associated Information** area.
The **Intercom Template Configuration** window displays.

Step 3 Enter or choose the appropriate values for the intercom template settings.

Step 4 Click **Save**.
BAT adds the intercom template to the phone template configuration.

Step 5 To add settings for any additional intercom templates, repeat Step 2, on page 311 through Step 4, on page 311.

If you choose Back to Find/List from the **Related Links** drop-down list box in the upper, right, corner of the **Intercom Template Configuration** window, the **Find and List Intercom Directory Number** window displays.

Note If you choose Back to Find/List from the **Related Links** drop-down list box in the upper, right, corner of the **Intercom Template Configuration** window, the **Find and List Intercom Directory Number** window displays.

a) Click **Find** and enter the appropriate search criteria and to find existing Intercom directory numbers.
b) In the **Find and List Intercom Directory Number** window, click **Add New** to add a new intercom directory number.

Create Phone CSV Data File Using BAT Spreadsheet

Use the BAT spreadsheet to create the CSV data file. You can define the file format within the spreadsheet, and the BAT spreadsheet uses the data file formats to display the fields for the CSV data file.

Note If you enter a comma in one of the fields, BAT.xlt encloses that field entry in double quotes when you export to BAT format.

If you enter a blank row in the BAT spreadsheet, the system treats the empty row as the end of the file and does not convert data that is entered after a blank line to the BAT format.

You can use the dummy MAC address option when adding CTI ports. This option gives a unique device name to each CTI port in the form of dummy MAC addresses that you can manually update later using the Cisco Unified Communications Manager Administration or the UnifiedCM Auto-Register phone Tool. Do not use the dummy MAC address option for H.323 clients, VGC phones, or VGC virtual phones.

The dummy MAC address option automatically generates dummy MAC addresses in the following format:

XXXXXXXXXXXX

where X represents any 12-character, hexadecimal (0-9 and A-F) number.

Attention The number of lines and speed dials that you define for phones in the BAT spreadsheet must not exceed the numbers that are defined in the BAT phone template, otherwise, an error occurs when you attempt to insert the CSV data file and BAT template.

After you have finished editing all the fields in the BAT spreadsheet, you can export the content to a CSV formatted data file. A default filename is assigned to the exported CSV formatted data file:

`<tabname>-<timestamp>.txt`

where `<tabname>` represents the type of input file that you created, such as phones, and `<timestamp>` represents the precise date and time that the file was created.

You can rename the CSV formatted data file after you save the exported file to your local workstation.

Note You cannot upload a CSV filename that contains a comma (for example, abcd,e.txt) to the Unified Communications Manager server.

Procedure

Step 1 To open the BAT spreadsheet, locate and double-click the BAT.xlt file

Step 2 When prompted, click **Enable Macros** to use the spreadsheet capabilities.

Step 3 To display the phones options, click the **Phones** tab at the bottom of the spreadsheet.

Step 4 Choose the radio button for one of the following device types:

The device type that you select determines the validation criteria for data in the BAT spreadsheet.

- Phones
- CTI Port
- H.323 Client
- VGC Phones
- VGC Virtual Phones
- Cisco IP Communicator Phone

The spreadsheet displays options that are available for the chosen device. For example, when you choose phones, fields for the number of phone lines and the number of speed dials display.

Step 5 Choose the device and line fields to appear in the BAT spreadsheet for each phone. Do the following:

a) Click **Create File Format**.

b) To choose the device fields, click a device field name in the **Device Field** box and then click the arrow to move the field to the **Selected Device Fields** box.

A CSV data file must include **MAC Address/Device Name** and **Description**; therefore, these fields always remain selected.

Tip To select a range of items in the list, hold down the **Shift** key. To select random field names, hold down the **Ctrl** key and click field names.

c) Click a line field name in the **Line Field** box and click the arrow to move the field to the **Selected Line Fields** box.

Tip To change the order of the items in the **Selected Line** and **Device** boxes, choose an item and use the up and down arrows to move the field up or down in the list.

d) A message asks whether you want to overwrite the existing CSV format. Click **Create** to modify the CSV data file format.

e) Click **OK**.
New columns for the selected fields display in the BAT spreadsheet in the order that you specified.

Step 6 Scroll to the right to locate the **Number of Phone Lines** box and enter the number of lines for the phone.

Note The number of lines you enter must not exceed the number of lines that are configured in the BAT template.

Step 7 For phones, you must enter the number of speed-dial buttons in the **Maximum Number of Speed Dials** box.

Note The number of speed dials you enter must not exceed the number of speed dials that are configured in the BAT template.

After you enter the number, columns display for each speed-dial number.

Step 8 Enter the number of Busy Lamp Field (BLF) speed-dial buttons in the **Maximum Number of BLF Speed Dials** box.
After you enter the number, columns display for each BLF speed-dial number.

Step 9 Enter data for an individual phone on each line in the spreadsheet.

Complete all mandatory fields and any relevant, optional fields. Each column heading specifies the length of the field and whether it is required or optional. See online help for phone field descriptions.

Step 10 If you did not enter the MAC address for each phone, check the **Create Dummy MAC Address** check box.

Attention Do not use the dummy MAC address option for H.323 clients, VGC phones, or VGC virtual phones.

Step 11 To transfer the data from the BAT Excel spreadsheet into a CSV formatted data file, click **Export to BAT Format**.

Tip For information on how to read the exported CSV data file, click the link to **View Sample File** in the **Insert phones** window in BAT.

The system saves the file with the default filename: `<tabname>-<timestamp>.txt` to your choice of a folder on your local workstation.

Create Custom Phone File Format Using Text Editor

You can use a text editor to create a custom phone file format for the text-based CSV data file.

Procedure

Step 1 Choose **Bulk Administration** > **Phones** > **Phone File Format** > **Create File Format**.

Step 2 Click **Add New**.

Step 3 In the **Format Name** field, enter a name for this custom format.

Step 4 Choose the fields to appear in the custom file format. Do the following:

a) To choose the device fields, click a device field name in the **Device Field** box and then click the arrow to move the field to the **Selected Device Fields** box.

A CSV data file must include **MAC Address/Device Name** and **Description**; therefore, these fields always remain selected.

Tip To select a range of items in the list, hold down the **Shift** key. To select random field names, hold down the **Ctrl** key and click field names.

b) Click a line field name in the **Line Field** box and click the arrow to move the field to the **Selected Line Fields** box.

c) Click the intercom DN field names in the **Intercom DN Fields** box and click the arrow to move the fields to the **Selected Intercom DN Fields Order** box.

Tip You can change the order of the items in the **Selected Line Fields**, **Selected Device Fields**, and **Selected Intercom DN Fields Order** boxes. Choose an item and use the up and down arrows to move the field up or down in the list.

Step 5 In the **IP Phone Services Maximums** area, enter the maximum values for the following fields:

- Maximum Number of Speed Dials
- Maximum Number of BLF Speed Dials
- Maximum Number of BLF Directed Call Parks

- Maximum Number of IP Phone Services
- Maximum Number of IP Phone Service Parameters

Step 6 Click **Save**.
The name of the custom file format displays in the **File Format Names** list in the **Find and List Phone File Formats** window.

Insert Phones Into Unified Communications Manager

When you insert phone records into the Unified Communications Manager database, you define the target CSV data file and how the phone records get inserted. Select any combination of the listed actions to overwrite the existing phone records, or you can choose to insert the records during upload:

- Delete all existing Speed Dials before adding new one
- Delete all existing BLF Speed Dials before adding new one
- Delete all existing BLF Directed Call Parks before adding new one
- Delete all existing Subscribed Services before adding new one

Note Phone records must be validated before insertion.

Note BAT expects Directory Number URI fields for directory numbers in the following format:

URI 1 on Directory Number 1, URI 1 Route Partition on Directory Number 1, URI 1 is Primary on Directory Number 1.

You can use the dummy MAC address option. When adding CTI ports, this option gives a unique device name to each CTI port in the form of dummy MAC addresses that you can manually update later using the Unified Communications Manager Administration or the UnifiedCM Auto-Register Phone Tool. Do not use the dummy MAC address option for H.323 clients, VGC phones, or VGC virtual phones.

The dummy MAC address option automatically generates dummy MAC addresses in the following format:

XXXXXXXXXXXX

where X represents any 12-character, hexadecimal (0-9 and A-F) number.

Before you begin

- You must have a Unified Communications Manager Bulk Administration (BAT) phone template for the devices that you are adding. You can choose the target and method of the data file upload. Phone records must be validated before insertion.
- You must have a data file in comma separated value (CSV) format that contains the unique details for the phones or other IP telephony devices.

Procedure

Step 1 Choose **Bulk Administration** > **Phones** > **Insert Phones**.

Step 2 Specify the file format type for the phone record that you are uploading.

a) To insert phone records that use a customized file format, click **Insert Phones Specific Details** radio button and continue with Step 3, on page 316 and Step 5, on page 316.

b) To insert phone records from an exported phone's file that was generated using the All Details option, click **Insert phones All Details** radio button.

Step 3 In the **File Name** drop-down list box, choose the CSV data file that you created for this specific bulk transaction. Next, check the **Allow Update Phone with Custom File** check box to allow updating the phone with the chosen custom file.

Step 4 Check the **Override the existing configuration** check box to overwrite the existing phone settings with the information that is contained in the file that you want to insert. Next, check the check boxes beside the upload action(s) to perform during the upload.

The following upload actions get enabled for selection after you have checked the **Override the existing configuration** check box.

- Delete all existing Speed Dials before adding new one.
- Delete all existing BLF Speed Dials before adding new one.
- Delete all existing BLF Directed Call Parks before adding new one.
- Delete all existing Subscribed Services before adding new one.

Note Leave the check boxes clear to append those records to the existing records in the CSV data file during the upload.

Step 5 For the Specific Details option, in the **Phone Template Name** drop-down list, choose the BAT phone template that you created for this type of bulk transaction.

Attention If you did not enter individual MAC addresses in the CSV data file, you must check the **Create Dummy MAC Address** check box. You can update this information manually later. Skip to Step 8, on page 316. If you supplied MAC addresses or device names in the data input file, do not choose this option.

If you do not know the MAC address of the phone that is assigned to the user, then choose this option. When the phone is plugged in, a MAC address registers for that device.

Step 6 In the **Job Information** area, enter the Job description.

Step 7 Choose an insert method. Do one of the following:

a) Click **Run Immediately** to insert the phone records immediately.

b) Click **Run Later** to insert the phone records later.

Step 8 Click **Submit** to create a job for inserting the phone records.

Use the **Job Configuration** window to schedule or activate this job.

What to do next

If the phones inserted are of the type Cisco Unified Mobile Communicator, then you must reset the devices after the insert job is completed. You can reset the phones using the **Bulk Administration** > **Phones** > **Reset/Restart Phones** option.

Add Users

You must create a CSV data file to add new users in bulk to the Unified Communications Manager database using the BAT spreadsheet. For users who have applications that require a CTI port, such as CiscoIPSoftPhone, BAT can associate CTI ports to existing users.

Procedure

Step 1 Create a comma separated values (CSV) data file to define individual values for each user that you want to add.

Step 2 Use BAT to insert the users in the Unified Communications Manager database.

Create User CSV Data File From BAT Spreadsheet

You can provide details for adding new users to the Unified Communications Manager database in the BAT spreadsheet and then convert it in to a CSV data file.

Note If you enter a blank row in the BAT spreadsheet, the system treats the empty row as the end of the file and does not convert data that is entered after a blank line to the BAT format.

After you have finished editing the fields to add users in the BAT spreadsheet, you can export the content to a CSV formatted data file. A default filename is assigned to the exported CSV formatted data file:

`<tabname>-<timestamp>.txt`

where `<tabname>` represents the type of input file that you created, such as phones, and `<timestamp>` represents the precise date and time that the file was created.

You can rename the CSV formatted data file after you save the exported file to your local workstation. If you enter a comma in one of the fields, BAT.xlt encloses that field entry in double quotes when you export to BAT format.

Note You cannot upload a CSV filename that contains a comma (for example, abcd,e.txt) to the Unified Communications Manager server.

Procedure

Step 1 To open the BAT spreadsheet, locate and double-click BAT.xlt file.

Step 2 When prompted, click **Enable Macros** to use the spreadsheet capabilities.

Step 3 To add users, click the **Users** tab at the bottom of the spreadsheet.

Step 4 Complete all mandatory fields and any relevant optional fields. Each column heading specifies the length of the field and whether it is required or optional.

In each row, provide the information as described in the online help files.

- If a user has multiple devices, the device name field should be repeated, once for each device.
- To enter additional device names that will be associated to a new user, enter a value in the **Number of Controlled Devices** text box.

Note You can associate all devices, including CTI ports, ATA ports, and H.323 clients, with a user.

Step 5 To enter additional device names that will be associated to a new user, enter a value in the **Number of Controlled Devices** text box.

Step 6 Click **Export to BAT Format** to transfer the data from the BAT Excel spreadsheet into a CSV formatted data file.

The system saves the file to C:\XLSDataFiles with the default file name <tabname>-<timestamp>.txt , or uses **Browse** to save the file to another existing folder.

Tip For information on how to read the exported CSV data file, click the link to **View Sample File** in the **Insert Users** window in BAT.

What to do next

You must upload the CSV data file to the first node of Unified Communications Manager database server so that BAT can access the data file.

Insert Users in Unified Communications Manager Database

You can add a group of users to the Unified Communications Manager database using a CSV data file. The field values that you enter in the CSV file for inserting users override the values provided in the user template.

Attention If the credential policy has “check for trivial password” enabled, and the password in the user template is the user ID, inserting users through BAT may fail if the user ID does not satisfy the necessary criteria for the trivial password.

Users can be inserted using BAT with primary extension configured without any devices selected for controlled devices. To do so, you must pre-populate the DN in Unified Communications Manager before inserting the users using BAT. The following steps outline the process of pre-populating the DN:

1. Create range of DNs to be associated for primary extension for users in the DN page.

2. Create a BAT template with primary extension configured (which should be the same DN's pre-populated).
3. Insert the users using BAT (as shown in the following procedure)

Before you begin

You must have a CSV data file that is saved in the UTF-8 encoding format and that contains the usernames, controlled device names, and directory numbers. You can create the CSV data file by using one of these methods:

- BAT spreadsheet that is converted to CSV format
- Export utility that produces an export file of user data

Note When you are inserting users by using an exported BAT file, you might get errors stating "User ID already exists" for some users that were exported in more than one file. For example, a list of first line managers and a list of users might both include the same manager user ID.

Procedure

Step 1 Choose **Bulk Administration** > **Users** > **Insert Users**.

Step 2 In the **File Name** field, choose the CSV data file that you created for this bulk transaction.

Step 3 If the CSV data file was created by using the export utility, check the **File created with Export Users** check box.

Step 4 From the **User Template Name** drop-down list, choose the user template you want to use for this insert.

Note The User Profile, Controlled Device Name, and Directory Number should exist in the Unified Communications Manager database. The controlled device name should be entered in full. If it contains only MAC Address, then BAT displays a non-existing device error.

Step 5 In the **Job Information** area, enter the Job description.

Step 6 Choose an insert method. Do one of the following:

a) Click **Run Immediately** to insert the user records immediately.
b) Click **Run Later** to insert the user records at a later time.

Step 7 To create a job for inserting the user records, click **Submit**.

To schedule and/or activate this job, use the Job Scheduler option in the **Bulk Administration** main menu.

Add Phones with Users Using the BAT Spreadsheet

Create a CSV data file for adding phones and users in bulk.

Procedure

Step 1 To open the BAT spreadsheet, locate and double-click BAT.xlt file.

You can download a BAT.xlt file.

Step 2 When prompted, click **Enable Macros** to use the spreadsheet capabilities.

Step 3 At the bottom of the spreadsheet, click the **Phones-Users** tab.

Step 4 Follow steps 4 through 10 in Create Phone CSV Data File Using BAT Spreadsheet, on page 312.

Add Phone and User File Format

You can add the phone and user file format with a text-based CSV data file. After the CSV data file is created, you need to associate the file format with the text-based CSV data file. After associating the file format with the CSV file, the names for each field display as the first record in the CSV data file. You can use this information to verify that you entered the values for each field in the correct order.

Before you begin

You must create a CSV data file that defines individual values for each user that you want to update.

When you use a text editor to create the CSV data file, you create a file format for entering values in the text-based file. You enter values in the text file in the order that the file format specifies.

Procedure

Step 1 Choose **Bulk Administration** > **Phones and Users** > **Phones & Users File Format** > **Assign File Format**. The **Add File Format Configuration** window displays.

Step 2 In the **File Name** field, choose the text-based CSV file that you created for this transaction.

Step 3 In the **Format File Name** field, choose the file format that you created for this type of bulk transaction.

Step 4 To create a job for associating the matching file format with the CSV data file, click **Submit**.

Step 5 To schedule and/or activate this job, use the Job Scheduler option in the **Bulk Administration** main menu.

Note The user fields get added automatically when you add the file format.

Insert Phones with Users Into Unified Communications Manager

You can add a group of phones and users to the Unified Communications Manager database and directory.

Note Phone records must be validated before insertion.

You can use the dummy MAC address option. When adding CTI ports, this option gives a unique device name to each CTI port in the form of dummy MAC addresses that you can manually update later using the Unified Communications Manager Administration or the UnifiedCM Auto-Register phone Tool. Do not use the dummy MAC address option for H.323 clients, VGC phones, or VGC virtual phones.

The dummy MAC address option automatically generates dummy MAC addresses in the following format:

XXXXXXXXXXXX

where X represents any 12-character, hexadecimal (0-9 and A-F) number.

Before you begin

1. Create a comma-separated values (CSV) data file to define individual values for each phone with users that you want to insert. You can create the CSV data file using the BAT spreadsheet (BAT.xlt) to add phones with users, or create a custom text file in CSV format to add phones with users combinations.
2. Associate file format with the CSV data file.
3. Validate phones with users records.

Procedure

Step 1 Choose **Bulk Administration** > **Phones & Users** > **Insert Phones with Users**.

Step 2 In the **File Name** field, choose the CSV data file that you created for this bulk transaction.

Step 3 In the **Phone Template Name** field, choose the BAT phone template that you used for this transaction.

Attention If you did not enter individual MAC addresses in the CSV data file, you must check the **Create Dummy MAC Address** check box. You can update this information manually later. If you supplied MAC addresses or device names in the data input file, do not choose this option.

If you do not know the MAC address of the phone that is assigned to the user, choose this option. When the phone is plugged in, a MAC address registers for that device.

Step 4 In the **User Template Name** field, choose the BAT user template that you used for this transaction

Step 5 In the **Job Information** area, enter the Job description.

Step 6 Choose an insert method. Do one of the following:

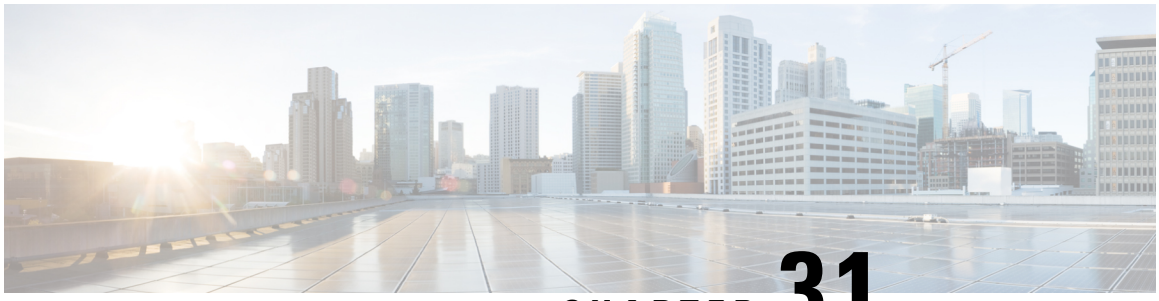
a) Click **Run Immediately** to insert the phones with users immediately.
b) Click **Run Later** to insert the phones with users at a later time.

Step 7 To create a job for inserting the phones and user records, click **Submit**.

To schedule and activate this job, use the Job Scheduler option in the **Bulk Administration** main menu.

PART V

Provisioning Endpoints



CHAPTER 31

Configure Endpoints

Endpoint Provisioning Defaults

Use the information in this part to configure endpoint devices, and how to associate users with endpoints.

Unified Communications Manager contains a set of device defaults that you can provision prior to adding endpoints. If you set these device default settings beforehand, when you provision new users and devices will be configured automatically based on the settings that are applied.

Following are the two default configurations for endpoints provisioning:

- Configure Device Defaults
- Configure Enterprise Phone Settings

Endpoint Provisioning Default Prerequisites

Confirm the ports that are configured for endpoint registrations. From Cisco Unified CM Administration, go to **System** > **Cisco Unified CM**, select the server and confirm the configured port settings.

Note In most cases, there is no need to change the ports from their default settings.

Endpoint Provisioning Defaults Task Flow

Complete the following task flows to configure devices for your system.

Procedure

	Command or Action	Purpose
Step 1	Configure Device Defaults, on page 326	You can change the default settings that are applied to devices that auto-register with a Unified Communications Manager node. Each type of device has a specific set of defaults.
Step 2	Configure Device Profile, on page 329	**Optional**. You can configure a device profile comprises the set of attributes that associate with a particular device for a user.
Step 3	Configure Default Device Profiles, on page 327	You can configure a default device profile that a phone takes whenever a user logs into a phone for which that user does not have a user device profile.
Step 4	Configure a Softkey Template on the Default Device Profile, on page 327	**Optional**. You can add the default device profile to a softkey template.
Step 5	Configure Enterprise Phone, on page 329	You can configure the basic enterprise phone settings that apply to all phones in the same cluster.

Configure Device 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 or activation codes.

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.

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 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

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 Enterprise Phone

Configure Enterprise Phone Settings

Use this procedure to configure default Product-Specific Configuration field settings that can be used by the phones in your network.

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

Procedure

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

Step 2 Enter the required fields in the **Product Specific Configuration Layout** section.

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

Step 3 Complete the remaining fields in the Enterprise Phone Configuration window. For help with the fields and their settings, see the online help.

Configure a Phone

Perform these steps to manually add the phone to the Unified Communications Manager database. You do not have to perform these steps if you are using autoregistration. If you opt for autoregistration, Unified Communications Manager automatically adds the phone and assigns the directory number.

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**.

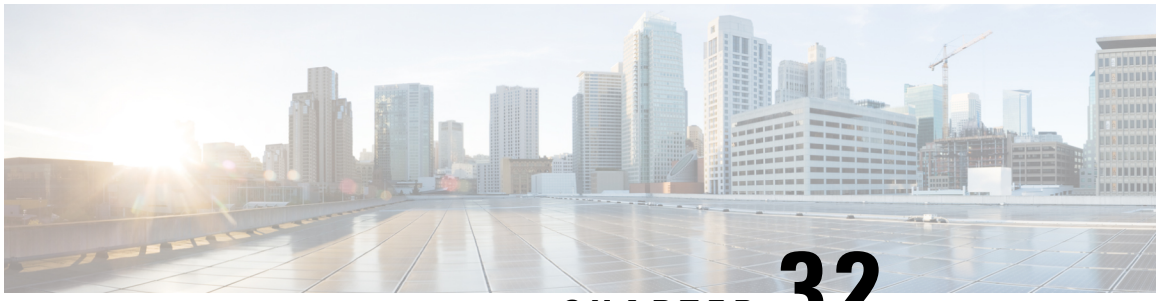
Self Care Portal

The Self Care Portal can be used as part of the deployment process for provisioning and configuring new phones:

- End users can use the portal to customize features and settings for their phones.
- With Device Activation Code Onboarding, users have the option to use the portal to activate their phones.

- Users can also use the portal to self-provision their own Single Number Reach remote destinations.

End users need to be set up with access before they can use the portal. For details on how to set up the portal, go to the “Self Care Portal’ chapter of the *Feature Configuration Guide for Cisco Unified Communications Manager*.



CHAPTER 32

Configure CAPF

Certificate Authority Proxy Function (CAPF) Overview

The Cisco Certificate Authority Proxy Function (CAPF) is a Cisco proprietary service that issues Locally Significant Certificates (LSCs) and authenticates Cisco endpoints. The CAPF service runs on Unified Communications Manager and performs the following tasks:

- Issues LSCs to supported Cisco Unified IP Phones.
- Authenticates phones when mixed mode is enabled.
- Upgrades existing LSCs for phones.
- Retrieves phone certificates for viewing and troubleshooting.

CAPF Running Modes

You can configure CAPF to operate in the following modes:

- Cisco Authority Proxy Function—The CAPF service on Unified Communications Manager issues LSCs that are signed by CAPF service itself. This is the default mode.
- Online CA—Use this option to have an external online CA signed LSC for phones. The CAPF service connects automatically to the external CA. When a CSR is submitted, the CA signs and returns the CA-signed LSC automatically.
- Offline CA—Use this option if you want to use an offline external CA to sign LSC for phones. This option requires you to manually download the LSC, submit them to the CA, and then upload the CA-signed certificates after they are ready.

Note Cisco recommends that if you want to use a third-party CA to sign LSC, use the **Online CA** option instead of **Offline CA** as the process is automated, much quicker, and less likely to encounter problems.

CAPF Service Certificate

When Unified Communications Manager is installed, CAPF service is installed automatically and a CAPF-specific system certificate is generated. When security is applied, Cisco CTL Client copies the certificate to all cluster nodes.

Phone Certificate Types

Cisco uses the following X.509v3 certificate types for phones:

- Locally Significant Certificates (LSC)—A certificate that installs on supported phones after you perform the necessary configuration tasks that are associated with the Cisco Certificate Authority Proxy Function (CAPF). The LSC secures the connection between Unified Communications Manager and the phone after you configure the device security mode for authentication or encryption.

Note For Online CA, the LSC validity is based on the CA and can be used as long as the CA allows it.

- Manufacture Installed Certificates (MIC)—Cisco Manufacturing installs MICs automatically in supported phone models. Manufacturer-installed certificates authenticate to Cisco Certificate Authority Proxy Function (CAPF) for LSC installation. You cannot overwrite or delete manufacture-installed certificate.

Note Cisco recommends that you use Manufacturer Installed Certificates (MICs) for LSC installation only. Cisco supports LSCs to authenticate the TLS connection with Unified Communications Manager. Since MIC root certificates can be compromised, customers who configure phones to use MICs for TLS authentication or for any other purpose do so at their own risk. Cisco assumes no liability if MICs are compromised.

LSC Generation via CAPF

After you configure CAPF, add the configured authentication string on the phone. The keys and certificate exchange occurs between the phone and CAPF and the following occurs:

- The phone authenticates itself to CAPF using the configured authentication method.
- The phone generates its public-private key pair.
- The phone forwards its public key to CAPF in a signed message.
- The private key remains in the phone and never gets exposed externally.
- CAPF signs the phone certificate and sends the certificate to the phone in a signed message.

Note Be aware that the phone user can abort the certificate operation or view the operation status on the phone.

Note Key generation set at low priority allows the phone to function while the action occurs. Although the phone functions during certification generation, additional TLS traffic may cause minimal call-processing interruptions with the phone. For example, audio glitches may occur when the certificate is written to flash at the end of the installation

CAPF Prerequisites

Before configuring the Certificate Authority Proxy Function for LSC generation, perform the following:

- If you want to use a third-party CA to sign your LSCs, configure your CA externally.
- Plan how you are going to authenticate your phones.
- Before you generate LSCs, ensure that you have the following:
  - Unified Communications Manager Release 12.5 or later.
  - Endpoints that use CAPF for certificates (includes Cisco IP Phones and Jabber).
  - Microsoft Windows Server 2012 and 2016.
  - Domain Name Service (DNS) is configured.
- You must upload the CA root and HTTPS certificates before generating LSCs. During a secure SIP connection, HTTPS certificate goes through the CAPF-trust and the CA root certificate goes through the CAPF-trust and the CallManager-trust. The Internet Information Services (IIS) hosts the HTTPS certificate. The CA root certificate is used to sign the Certificate Signing Requests (CSR).

  Following are the scenarios when you have to upload the certificates:

Table 27: Upload Certificate Scenarios

Scenarios	Results
CA root and HTTPS certificates are same.	Upload the CA root certificate.
CA root and HTTPS certificates are different and if HTTPS certificates are issued by the same CA root certificate.	Upload the CA root certificate.
The intermediate CA and HTTPS certificates are different and are issued by the CA root certificate.	Upload the CA root certificate.
CA root and HTTPS certificates are different and are issued by the same CA root certificate.	Upload CA root and HTTPS certificate.

Note Cisco strongly recommends that you use CAPF during a scheduled maintenance window because generating multiple certificates simultaneously may cause call-processing interruptions.

Certificate Authority Proxy Function Configuration Task Flow

Complete these tasks to configure the Certificate Authority Proxy Function (CAPF) service to issue LSCs for endpoints:

Note You don't have to restart the CAPF service after regenerating or uploading the new CAPF certificate.

Procedure

	Command or Action	Purpose
Step 1	Upload Root Certificate for Third-Party CAs	If you want your LSCs to be third-party CA-signed, upload the CA root certificate chain to the CAPF-trust store. Otherwise, you can skip this task.
Step 2	Upload Certificate Authority (CA) Root Certificate , on page 337	Upload the CA root certificate to the Unified Communications Manager Trust store.
Step 3	Configure Online Certificate Authority Settings, on page 338	Use this procedure to generate phone LSC certificates.
Step 4	Configure Offline Certificate Authority Settings	Use this procedure to generate phone LSC certificates using an Offline CA.
Step 5	Activate or Restart CAPF Services	After you configure the CAPF system settings, activate essential CAPF services.
Step 6	Configure CAPF settings in Unified Communications Manager using one of the following procedures: • Configure CAPF Settings in a Universal Device Template, on page 340 • Update CAPF Settings via Bulk Admin, on page 341 • Configure CAPF Settings for a Phone, on page 342	Add the CAPF settings to Phone Configuration using one of the following options: • If you haven't synced your LDAP directory, add CAPF settings to a Universal Device Template and apply settings through the initial LDAP sync. • Use Bulk Administration Tool to apply CAPF settings to many phones in a single operation. • You can apply CAPF settings on a phone-by-phone basis.

	Command or Action	Purpose
Step 7	Set KeepAlive Timer, on page 343	(Optional) Set a keepalive value for the CAPF-Endpoint connection so that it's not timed out by a firewall. The default value is 15 minutes.

Upload Root Certificate for Third-Party CAs

Upload the CA root certificate to the CAPF-trust store and the Unified Communications Manager trust store to use an external CA to sign LSC certificates.

Note Skip this task if you don't want to use a third-party CA to sign LSCs.

Procedure

Step 1 From Cisco Unified OS Administration choose **Security** > **Certificate Management**.
Step 2 Click **Upload Certificate/Certificate chain**.
Step 3 From the **Certificate Purpose** drop-down list, choose **CAPF-trust**.
Step 4 Enter a **Description** for the certificate. For example, **Certificate for External LSC-Signing CA**.
Step 5 Click **Browse**, navigate to the file, and then click **Open**.
Step 6 Click **Upload**.
Step 7 Repeat this task, uploading certificates to **callmanager-trust** for the **Certificate Purpose**.

Upload Certificate Authority (CA) Root Certificate

Note Ensure that the intermediate or root CA certificate doesn't contain the 'CAPF−' substring in the Common Name. The 'CAPF−' common name is reserved for CAPF certificates.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.
Step 2 Click **Upload Certificate/Certificate chain**.
Step 3 From the **Certificate Purpose** drop-down list, choose **callmanager-trust**.
Step 4 Enter a **Description** for the certificate. For example, **Certificate for External LSC-Signing CA**.
Step 5 Click **Browse**, navigate to the file, and then click **Open**.

Configure Online Certificate Authority Settings

Use this procedure in Unified Communications Manager to generate phone LSCs using Online CAPF.

Note FIPS enabled mode doesn't support Online CAPF and CAPFv3.

Procedure

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

Step 2 From the **Server** drop-down list, choose a node where you activated the Cisco Certificate Authority Proxy Function (Active) service.

Step 3 From the **Service** drop-down list, choose **Cisco Certificate Authority Proxy Function (Active)**. Verify that the word "Active" is displayed next to the service name.

Step 4 From the **Certificate Issuer to Endpoint** drop-down list, choose **Online CA**. For CA-signed certificates, we recommend using an Online CA.

Step 5 In the **Duration Of Certificate Validity (in days)** field, enter a number between 1 and 1825 to represent the number of days that a certificate issued by CAPF is valid.

Step 6 In the **Online CA Parameters** section, set the following parameters in order to create the connection to the Online CA section.

- Online CA Hostname—The subject name or the Common Name (CN) should be the same as the Fully Qualified Domain Name (FQDN) of HTTPS certificate.

  Note The hostname configured is the same as the Common Names (CN) of the HTTPs certificate hosted by Internet Information Services (IIS) running on Microsoft CA.

- Online CA Port—Enter the port number for Online CA. For example, 443
- Online CA Template—Enter the name of the template. Microsoft CA creates the template.
- Online CA Type—Choose the default type, Microsoft CA.
- Online CA Username—Enter the username of the CA server.
- Online CA Password—Enter the password for the username of the CA server.

Step 7 Complete the remaining CAPF service parameters. Click the parameter name to view the service parameter help system.

Step 8 Click **Save**.

Step 9 Restart **Cisco Certificate Authority Proxy Function** for the changes to take effect. It automatically restarts the Cisco Certificate Enrollment service.

Current Online CA limitations

- The Online CA feature does not work if the CA server uses any other language apart from English. The CA server should respond only in English.
- The Online CA feature does not support mTLS authentication with CA.

- While using Online CA for LSC operation if LSC certificate is not provided with 'Digital signature' and 'key encipherment' key usage Device secure registration will fail.
- Device secure registration fails if LSC certificate is not provided with 'Digital signature' and 'key encipherment' while using Online CA for LSC operation.

Configure Offline Certificate Authority Settings

Follow this high-level process if you decide to generate phone LSC certificates using an Offline CA.

Note The offline CA option is more time-consuming than online CAs, involving numerous manual steps. Restart the process if there are any issues (for example, a network outage or phone reset) during the certificate generation and transmission process.

Procedure

Step 1 Download the root certificate chain from the third-party certificate authority.

Step 2 Upload the root certificate chain to the required trusts (CallManager trust CAPF trust) in Unified Communications Manager.

Step 3 Configure Unified Communications Manager to use Offline CAs by setting the **Certificate Issue to Endpoint** service parameter to Offline CA.

Step 4 Generate **CSR**s for your phone LSCs.

Step 5 Send the **CSR**s to the certificate authority.

Step 6 Obtain the signed certificates from the **CSR**.

For more detailed example on how to generate phone LSCs using an Offline CA, see CUCM Third-Party CA-Signed LSCs Generation and Import Configuration.

Activate or Restart CAPF Services

Activate the essential CAPF services after you configure the CAPF system settings. Restart if the CAPF service is already activated.

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 From the **Security Services** pane, check the services that apply:

- **Cisco Certificate Enrollment Service**—Check this service if you're using an Online CA else leave it unchecked.

- **Cisco Certificate Authority Proxy Function**—Check this service if unchecked (Deactivated). Restart if the service is already activated.

Step 4 Click **Save** if you modified any settings.

Step 5 If the **Cisco Certificate Authority Proxy Function** service was already checked (Activated), restart it:

a) From the **Related Links** drop-down list, select **Control Center - Feature Services** and click **Go**.

b) From **Security Settings** pane, check the **Cisco Certificate Authority Proxy Function** service and click **Restart**.

Step 6 Complete one of the following procedures to configure CAPF settings against individual phones.

a) Configure CAPF Settings in a Universal Device Template, on page 340

b) Update CAPF Settings via Bulk Admin, on page 341

c) Configure CAPF Settings for a Phone, on page 342

Configure CAPF Settings in a Universal Device Template

Use this procedure to configure CAPF settings to a Universal Device Template. Apply the template against an LDAP directory sync through the feature group template configuration. The CAPF settings in the template apply to all synced devices that use this template.

Note You can only add the Universal Device Template to an LDAP directory that hasn't been synced. If your initial LDAP sync has occurred, use Bulk Administration to update phones. For details, see Update CAPF Settings via Bulk Admin, on page 341.

Procedure

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

Step 2 Do either of the following:

- Click **Find** and **Select** an existing template.
- Click **Add New**.

Step 3 Expand the **Certificate Authority Proxy Function (CAPF) Settings** area.

Step 4 From the **Certificate Operation** drop-down list, select **Install/Upgrade**.

Step 5 From the **Authentication Mode** drop-down list menu, select an option for the device to authenticate itself.

Step 6 If you chose to use an authentication string, enter the **Authentication String** in the text box, or click **Generate String** to have the system generate a string for you.

Note Authentication fails if this string isn't configured on the device itself.

Step 7 From the remaining fields, configure the key information. For help with the fields, see the online help.

Step 8 Click **Save**.

Note Make sure you have configured the devices that use this template with the same authentication method that you assigned in this procedure. Otherwise, device authentication fails. See your phone documentation for details on how to configure authentication for phones.

Step 9 Apply the template settings to devices that use this profile.

a) Add the Universal Device Template to a Feature Group Template Configuration.
b) Add the Feature Group Template to an LDAP Directory Configuration that isn't synced.
c) Complete an LDAP sync. The CAPF settings get applied to all synced devices.

For details on configuring feature group templates and LDAP directories, see the "Configure End Users" section of System Configuration Guide for Cisco Unified Communications Manager.

Update CAPF Settings via Bulk Admin

Use **Update Phones** query of Bulk Administration to configure CAPF settings and LSC certificates for many existing phones in a single operation.

Note If you haven't provisioned the phones, use **Insert Phones** menu of the Bulk Administration to provision new phones with CAPF settings from a CSV file. See the "Phones Insertions" section of Bulk Administration Guide for Cisco Unified Communications Manager for details on how to insert phones from CSV files.

Make sure you have configured your phones with the same string and authentication method that you plan to add in this procedure. Else, your phones don't authenticate to CAPF. See your *Phone Documentation* for details on how to configure authentication on the phone.

Procedure

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

Step 2 Use filter options to limit the search to the phones that you want to update and click **Find**.

For example, use **Find phones where** drop-down list to select all phones, where LSC expires before a specific date or in a specific Device Pool.

Step 3 Click **Next**.

Step 4 From the **Logout/Reset/Restart** section, choose the **Apply Config** radio button. When the job runs, the CAPF updates get applied to all updated phones.

Step 5 Under **Certification Authority Proxy Function (CAPF) Information**, check the **Certificate Operation** check box.

Step 6 From the **Certificate Operation** drop-down list, choose **Install/Upgrade** to have CAPF install a new LSC certificate on the phone.

Step 7 From the **Authentication Mode** drop-down list, choose how you want the phone to authenticate itself during the LSC installation.

Note Configure the same authentication method on the phone.

Step 8 Complete one of the following steps if you selected **By Authentication String** as the **Authentication Mode**:

- Check **Generate unique authentication string for each device** if you want to use a unique authentication string for each device.
- Enter the string in **Authentication String** text box, or click **Generate String** if you want to use the same authentication string for all devices.

Step 9 Complete the remaining fields in the **Certification Authority Proxy Function (CAPF) Information** section of the **Update Phones** window. For help with the fields and their settings, see the online help.

Step 10 From the **Job Information** section, select **Run Immediately**.

Note Select **Run Later** if you want run the job at a scheduled time. For details on scheduling jobs, see the "Manage Scheduled Jobs" section in Bulk Administration Guide for Cisco Unified Communications Manager.

Step 11 Click **Submit**.

Note Apply configurations in the **Phones Configuration** window for all updated phones if you didn't select the **Apply Config** option in this procedure.

Configure CAPF Settings for a Phone

Use this procedure to configure CAPF settings for LSC certificates on an individual phone.

Note Use Bulk Administration or sync LDAP directory to apply CAPF settings to a large number of phones.

Configure your phone with the same string and authentication method that you plan to add in this procedure. Else, the phone doesn't authenticate itself to CAPF. See your *Phone Documentation* for details on how to configure authentication on the phone.

Procedure

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

Step 2 Click **Find** and select an existing phone. The **Phone Configuration** page appears.

Step 3 Navigate to the **Certification Authority Proxy Function (CAPF) Information** pane.

Step 4 From the **Certificate Operation** drop-down list, choose **Install/Upgrade** for CAPF to install a new LSC certificate on the phone.

Step 5 From the **Authentication Mode** drop-down list, choose how you want the phone to authenticate itself during the LSC installation.

Note The phone should be configured to use the same authentication method.

Step 6 Enter a text string or click **Generate String** to generate a string for you if you selected **By Authentication String**.

Step 7 Enter the details in the remaining fields in the **Certification Authority Proxy Function (CAPF) Information** pane of the **Phone Configuration** page. For help with the fields and their settings, see the online help.

Step 8 Click **Save**.

Set KeepAlive Timer

Use this procedure to set the clusterwide keepalive timer for the CAPF–Endpoint connection so that the connection doesn't get timed out by a firewall. The timer has a default value of 15 minutes. After each interval, the CAPF service sends a keepalive signal to the phone to keep the connection open.

Procedure

Step 1 Use the Command Line Interface to login to the publisher node.

Step 2 Run the `utils capt set keep_alive` CLI command.

Step 3 Enter a number between 5 and 60 (minutes) and click **Enter**.

CAPF Administration Tasks

After you configure CAPF and issue LSC certificates, use the following tasks to administer LSC certificates on an ongoing basis.

Certificate Status Monitoring

You can configure the system to monitor certificate status automatically. The system will email you when certificates are approaching expiration, and then revoke the certificates after expiration.

For details on how to configure certificate monitoring checks, see the Certificate Monitoring and Revocation Task Flow in the "Manage Certificates" chapter.

Run Stale LSC Report

Use this procedure to run a Stale LSC report from Cisco Unified Reporting. Stale LSCs are certificates that were generated in response to an endpoint CSR, but were never installed because a new CSR was generated by the endpoint before the stale LSC was installed.

Note You can also obtain a list of stale LSC certificates by running the `utils capf stale-lsc list` CLI command on the publisher node.

Procedure

Step 1 From Cisco Unified Reporting, choose **System Reports**.

Step 2 In the left navigation bar, choose **Stale LSCs**.

Step 3 Click **Generate a new Report**.

View Pending CSR List

Use this procedure to view a list of pending CAPF CSR files. All CSR files are timestamped.

Procedure

Step 1 Use the Command Line Interface to login to the publisher node.

Step 2 Run the `utils capf csr list` CLI command.
A timestamped list of pending CSR files displays.

Delete Stale LSC Certificates

Use this procedure to delete stale LSC certificates from the system.

Procedure

Step 1 Use the Command Line Interface to login to the publisher node.

Step 2 Run the `utils capf stale-lsc delete all` CLI command
The system deletes all stale LSC certificates from the system.

CAPF System Interactions and Restrictions

Feature	Interaction
Authentication String	CAPF authentication method for the phone, you must enter the same authentication string on the phone after the operation, or the operation will fail. If TFTP Encrypted Configuration enterprise parameter is enabled and you fail to enter the authentication string, the phone may fail and may not recover until the matching authentication string is entered on the phone
Cluster Server Credentials	All servers in the Unified Communications Manager cluster must use the same administrator username and password, so CAPF can authenticate to all servers in the cluster

Feature	Interaction
Migrating secure phone	If a secure phone gets moved to another cluster, the Unified Communications Manager will not trust the LSC certificate that the phone sends because it was issued by another CAPF, whose certificate is not in the CTL file. To enable the secure phone to register, delete the existing CTL file. You can then use the Install/Upgrade option to install a new LSC certificate with the new CAPF and reset the phone for the new CTL file (or use the MIC). Use the Delete option in the CAPF section on the Phone Configuration window to delete the existing LSC before you move the phones.
Cisco Unified IP Phones 6900 series, 7900 series, 8900 series, and 9900	Cisco recommends upgrading Cisco Unified IP Phones 6900 series, 7900 series, 8900 series, and 9900 series to use LSCs for TLS connection to Unified Communications Manager and removing MIC root certificates from the CallManager trust store to avoid possible future compatibility issues. Be aware that some phone models that use MICs for TLS connection to Unified Communications Manager may not be able to register. Administrators should remove the following MIC root certificates from the CallManager trust store: • CAP-RTP-001 • CAP-RTP-002 • Cisco_Manufacturing_CA • Cisco_Root_CA_2048
Power Failures	The following information applies when a communication or power failure occurs. • If a communication failure occurs while the certificate installation is taking place on the phone, the phone will attempt to obtain the certificate three more times in 30-second intervals. You cannot configure these values. • If a power failure occurs while the phone attempts a session with CAPF, the phone will use the authentication mode that is stored in flash; that is, if the phone cannot load the new configuration file from the TFTP server after the phone reboots. After the certificate operation completes, the system clears the value in flash.

Feature	Interaction
Certificate Encryption	Beginning from Unified Communications Manager Release 11.5(1) SU1, all the LSC certificates issued by CAPF service are signed with SHA-256 algorithm. Therefore, IP Phones 7900/8900/9900 series models supports SHA-256 signed LSC certificates and external SHA2 identity certificates (Tomcat, CallManager, CAPF, TVS and so on). For any other cryptographic operation that require validation of signature, only SHA-1 is supported. **Note** If you use phone models, which are in End of Software Maintenance or End of Life, we strongly recommend using the Unified Communications Manager before 11.5(1) SU1 release.

CAPF Examples with 7942 and 7962 Phones

Consider the following information about how CAPF interacts with the Cisco Unified IP Phone 7962 and 7942 when the phone is reset by a user or by Unified Communications Manager.

Note In the following examples, if the LSC does not already exist in the phone and if **By Existing Certificate** is chosen for the CAPF Authentication Mode, the CAPF certificate operation fails.

Example-Nonsecure Device Security Mode

In this example, the phone resets after you configure the Device Security Mode to **Nonsecure** and the CAPF Authentication Mode to **By Null String** or **By Existing Certificate (Precedence...)**. After the phone resets, it immediately registers with the primary Unified Communications Manager and receives the configuration file. The phone then automatically initiates a session with CAPF to download the LSC. After the phone installs the LSC, configure the Device Security Mode to Authenticated or Encrypted.

Example-Authenticated/Encrypted Device Security Mode

In this example, the phone resets after you configure the **Device Security Mode** to **Authenticated** or **Encrypted** and the CAPF Authentication Mode to **By Null String** or **By Existing Certificate (Precedence...)**. The phone does not register with the primary Unified Communications Manager until the CAPF session ends and the phone installs the LSC. After the session ends, the phone registers and immediately runs in authenticated or encrypted mode.

You cannot configure **By Authentication String** in this example because the phone does not automatically contact the CAPF server; the registration fails if the phone does not have a valid LSC.

CAPF Interaction with IPv6 Addressing

CAPF can issue and upgrade certificates to a phone that uses an IPv4, an IPv6, or both types of addresses. To issue or upgrade certificates for phones that are running SCCP that use an IPv6 address, you must set the Enable IPv6 service parameter to **True** in Unified Communications Manager Administration.

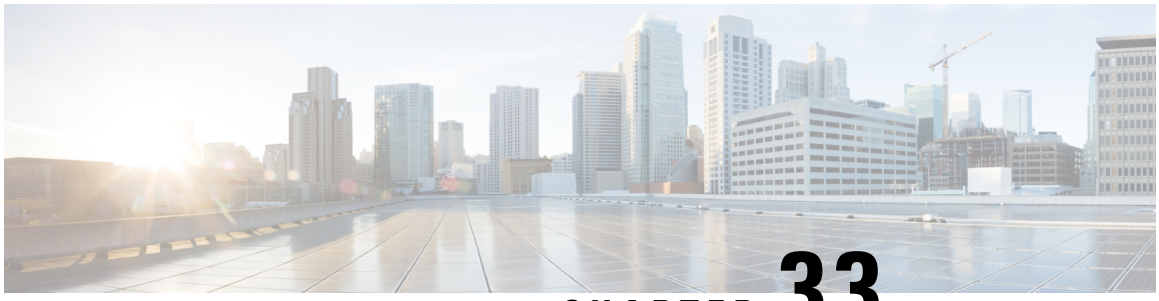
When the phone connects to CAPF to get a certificate, CAPF uses the configuration from the Enable IPv6 enterprise parameter to determine whether to issue or upgrade the certificate to the phone. If the enterprise parameter is set to **False**, CAPF ignores/rejects connections from phones that use IPv6 addresses, and the phone does not receive the certificate.

The following table describes how a phone that has an IPv4, IPv6, or both types of addresses connects to CAPF.

Table 28: How IPv6 or IPv4 Phone Connects to CAPF

IP Mode of Phone	IP Addresses on Phone	CAPF IP Address	How Phone Connects to CAPF
Two stack	IPv4 and IPv6 available	IPv4, IPv6	Phone uses an IPv6 address to connect to CAPF; if the phone cannot connect via an IPv6 address, it attempts to connect by using an IPv4 address.
Two stack	IPv4	IPv4, IPv6	Phone uses an IPv4 address to connect to CAPF.
Two stack	IPv6	IPv4, IPv6	Phone uses an IPv6 address to connect to CAPF. If the attempt fails, the phone uses an IPv4 address to connect to CAPF.
Two stack	IPv4	IPv4	Phone uses an IPv4 address to connect to CAPF.
Two stack	IPv4 and IPv6 available	IPv6	Phone uses and IPv6 address to connect to CAPF.
Two stack	IPv4 and IPv6 available	IPv4	Phone uses an IPv4 address to connect to CAPF.
Two stack	IPv4	IPv6	Phone cannot connect to CAPF.
Two stack	IPv6	IPv4	Phone cannot connect to CAPF.
Two stack	IPv6	IPv6	Phone uses an IPv6 address to connect to CAPF.
IPv4 stack	IPv4	IPv4, IPv6	Phone uses an IPv4 address to connect to CAPF.
IPv6 stack	IPv6	IPv4, IPv6	Phone uses an IPv6 address to connect to CAPF.
IPv4 stack	IPv4	IPv4	Phone uses an IPv4 address to connect to CAPF.
IPv4 stack	IPv4	IPv6	Phone cannot connect to CAPF.
IPv6 stack	IPv6	IPv6	Phone uses an IPv6 address to connect to CAPF.

IP Mode of Phone	IP Addresses on Phone	CAPF IP Address	How Phone Connects to CAPF
IPv6 stack	IPv6	IPv4	Phone cannot connect to CAPF.



CHAPTER 33

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.

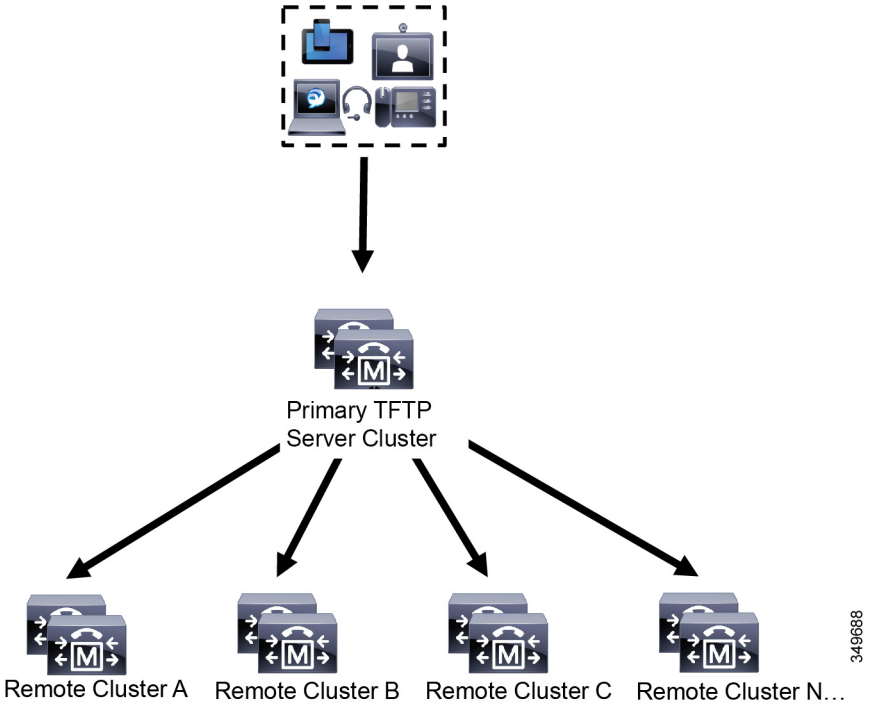
Proxy TFTP

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 7: 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 353 • Configure TFTP Server Manually, on page 353	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 354	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 355	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 355	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.

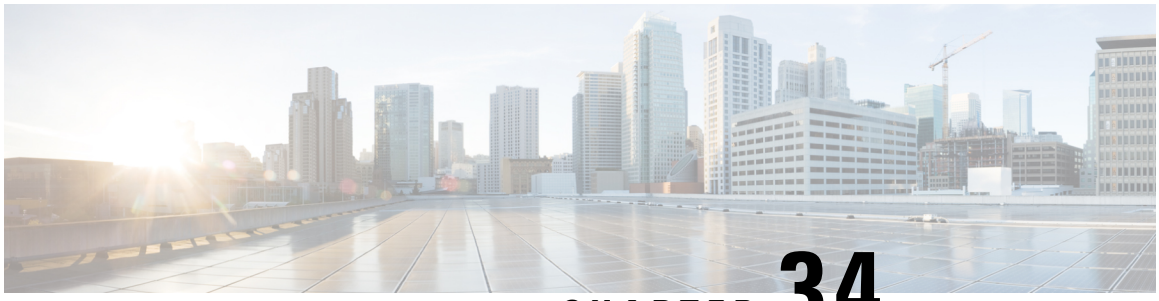
Step 3 Select the TFTP service in the **CM Services** area and click **Stop**.

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 34

Device Onboarding via Activation Codes

Activation Codes Overview

Activation codes make onboarding newly provisioned phones easy. An activation code is a single-use, 16-digit value that a user must enter on a phone while registering the phone. Activation codes provide a simple method for provisioning and onboarding phones without requiring an administrator to collect and input the MAC Address for each phone manually. This method is a simple alternative to autoregistration that you can use this method to provision a large number of phones, a single phone, or even to re-register existing phones.

You can also use Mobile and Remote Access-compliant devices to easily and securely register over Mobile and Remote Access using an activation code.

Activation Code Device Onboarding works in the following modes:

- On premise
- Mobile Remote Access (MRA)

Activation codes provide the following benefits:

- Onboarding using activation codes ensures that all newly provisioned phones or untrusted phones have their Manufacturing Installed Certificate (MIC) assessed and verified by Unified Communications Manager.

Note Cisco Manufacturing Root certificates must be present in the CallManager-trust store to perform onboarding activity.

- No need to manually enter actual MAC addresses. Administrators can use dummy MAC addresses and the phone updates the configuration automatically with the real MAC address during registration.

- No need to deploy an IVR, such as TAPS, to convert phone names from BAT to SEP.

Phone users can obtain their activation codes via the Self-Care Portal, provided the **Show Phones Ready to Activate** enterprise parameter is set to **`True`**. Otherwise, administrators must provide the codes to phone users.

Note When you provision with BAT MAC addresses, activation codes are tied to the phone model. BAT MAC is a reference to the device name that starts with 'BAT' and is followed by a random 12 hexidecimal digits that look like a MAC address. When saving a device configuration page with a blank MAC Address field, a random name with this format is created for you.You must enter an activation code that matches the phone model in order to activate the phone.

For added security, you can provision the phone with the actual MAC address of the phone. This option involves more configuration because the administrator must gather and input each phone's MAC address during provisioning, but provides greater security because users must enter the activation code that matches the actual MAC address on their phone.

Onboarding Process Flow in On-Premise Mode

Following is the process flow for onboarding new phones via activation codes :

1. Administrator sets the configuration to require the user to enter an activation code for onboarding.
2. Administrator provisions and configures the phone. If BAT MAC addresses are being used, the administrator does not enter the actual MAC address.
3. Phone gets an IP address for TFTP via a DHCP opt 150, or from an alternate TFTP as configured in Phone settings. The phone downloads the XMLDefault file, and detects that an activation code is in use.
4. The user enters the activation code on the phone.
5. The Phone authenticates to Cisco Unified Communications Manager via the activation code and manufacturer-installed certificate.
6. The Phone requires the TVS service when the activation code is used for onboarding phones. The ITL file provides this TVS function which contains the certificate of the TVS service that runs on the Unified CM server TCP port 2445.
7. Cisco Unified Communications Manager updates the device configuration with the actual MAC address. The TFTP server sense the device configuration to the phone, allowing the phone to register. Note that device registration can be up to five minutes.

Note It's recommended to add an additional subscriber to the default communication manager group for on-premise activation code onboarding. Else, when the node in the default communication manager group goes down, you may face onboarding issues.

Onboarding Process Flow in Mobile and Remote Access Mode

Following is the process flow for onboarding new phones via activation codes when you use the Mobile and Remote Access mode:

1. Administrator configures Cloud/Hybrid communication to Enable Activation Code Onboarding with Cisco Cloud and specifies the Mobile and Remote Access Activation Domain.
2. Administrator configures additional Mobile and Remote Access Service Domains, if required.
3. Administrator creates a full-device configuration without specifying MAC address (BAT, AXL, GUI). The device name will be a random BAT MAC address.
4. Administrator requests activation code for this device. Device Activation Service requests the code from the cloud-based device activation service.
5. The user can get the code from the self-care portal or the administrator can send it to the user.
6. The user powers up the phone and enters the activation code.
7. Phone learns from the cloud the location of Expressway and authenticates to Mobile and Remote Access/Cisco Unified Communications Manager.
8. Device activation service updates device configuration in the database with the phone's MAC address.

   The phone can now register and get its phone-specific configuration file from TFTP like normal Mobile and Remote Access, and register with Cisco Unified Communications Manager.

Note To provide secure solution for work from home remote users, Expressway's Mobile and Remote Access is the recommended solution and not TRP.

Activation Code Prerequisites

As of Release 12.5(1), the following Cisco IP Phone models support onboarding via activation codes: 7811, 7821, 7832, 7841, 7861, 8811, 8841, 8845, 8851, 8851NR, 8861, 8865, and 8865NR.

Additionally, Release 12.5(1)SU1 supports the following Cisco IP Phone models: 8832 and 8832NR

Self Care Portal

If you plan to have your users use the Self Care Portal to onboard their phones, you need to set the portal up beforehand so that your users will have access. For details, go to "Self Care Portal" chapter of the *Feature Configuration Guide for Cisco Unified Communications Manager*.

Device Onboarding with Activation Codes Task Flow in On-Premise Mode

Complete these tasks to onboard new phones using activation codes.

Procedure

	Command or Action	Purpose
Step 1	Activate the Device Activation Service, on page 360	The **Cisco Device Activation Service** must be running in Cisco Unified Serviceability.
Step 2	Set Registration Method to use Activation Codes, on page 360	Under Device Defaults, set the default registration method to use Activation Codes for supported phone models.
Step 3	Provision phones with activation code requirement. Following are two provisioning example options: • Add Phone with Activation Code Requirement, on page 361 • Add Phones with Activation Codes via Bulk Administration, on page 362	Cisco Unified Communications Manager has a variety of provisioning methods, including the options on the left. Whichever method you choose, make sure the **Requires Activation Code for Onboarding** check box is checked within that phone's **Phone Configuration**.
Step 4	Activate Phones, on page 365	Distribute activation codes to users. Users must enter the code on the phone in order to use the phone.

Activate the Device Activation Service

To use activation codes, the **Cisco Device Activation Service** must be running in Cisco Unified Serviceability. Use this procedure to confirm the service is running.

Procedure

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

Step 2 From the **Server** drop-down, choose the Unified Communications Manager publisher node and click **Go**.

Step 3 Under **CM Services**, confirm that the **Status** of the **Cisco Device Activation Service** says **Activated**.

Step 4 If the service is not running, check the adjacent check box and click **Save**.

What to do next

Set Registration Method to use Activation Codes, on page 360

Set Registration Method to use Activation Codes

Use this procedure to configure the system defaults so that phones of a specific model type will use activation codes to register with Unified Communications Manager.

Note This procedure applies for the onboarding of on-premise endpoints only. The Onboarding Method setting under **Device Defaults** does not apply for onboarding of Mobile and Remote Access endpoints using activation codes.

Procedure

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

Step 2 In the **Device Defaults Configuration** window, select the device type that will use activation codes for registration in the **Dual Bank Information** section, and change **On-Premise Onboarding Method** from **Auto Registration** to **Activation Code**.

Step 3 Click **Save**.

Note When device default is set to Activation Code, and if Auto Registration is earlier used for phone types, subsequent addition of new phones should follow Activation Code Onboarding or Manual Configuration of Phone (Using MAC address) and Registration.

For more information, see Add Phone with Activation Code Requirement and Add Phones with Activation Codes via Bulk Administration section to provision new phones.

Add Phone with Activation Code Requirement

Use this procedure if you want to provision a new phone with an activation code requirement.

Before you begin

Configure Universal Device and Line Templates with the settings that you want to apply as it makes the provisioning process faster.

Note If you choose not to use templates, you can add a new phone and configure settings manually, or add settings via a BAT Template. In each case, the **Requires Activation Code for Onboarding** check box must be checked in the **Phone Configuration** window.

Procedure

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

Step 2 Click **Add New From Template** to add settings from a universal line or device template.

Step 3 From the **Phone Type** drop-down menu, select the phone model.

Step 4 In the **MAC Address** field, enter a MAC address. With activation codes, you can use a dummy MAC address or the phone's actual MAC address.

You can modify the MAC address of a phone in the following scenarios:

- **BAT{mac}->SEP{mac}**: You should know the exact device name for prefix to change from `?BAT? to ?SEP?` upon **Save**.
- **SEP{mac}->BAT{mac}:** You can blank out the MAC address for prefix to change from `?SEP? to ?BAT?` and a new device name with a prefix of `?BAT?`.

Step 5 From the **Device Template** drop-down, select a template such as an existing Universal Device Template with the settings ou want to apply.

Step 6 From the **Directory Number** field, select an existing directory number, or click New and do the following:

a) In the **Add New Extension** popup, enter a new directory number and a Line Template that contains the settings you want to apply.

b) Click **Save** and then click **Close**.
The new extension appears in the **Directory Number** field.

Step 7 Optional. From the **User** field, select the User ID that you want to apply to this phone.

Step 8 Click **Add**.

Step 9 Check the **Requires Activation Code for Onboarding** check box. In case of Mobile and Remote Access mode, check the **Allow Activation Code via Mobile and Remote Access** check box.

Step 10 Configure any other settings that you want to apply. Refer to the online help for help with the fields and their settings.

Step 11 Click **Save**, and then click **OK**.
The **Phone Configuration** generates the new activation code. Click **View Activation Code** if you want to view the code.

What to do next

Activate Phones, on page 365

Add Phones with Activation Codes via Bulk Administration

This optional task flow contains a provisioning example using Bulk Administration Tool's Insert Phones feature to provision a large number of phones in a single operation. These phones will use activation codes for registration.

Procedure

	Command or Action	Purpose
Step 1	Configure BAT Provisioning Template, on page 363	Configure a BAT Template that contains the settings that you want to apply to provisioned phones.
Step 2	Create CSV File with New Phones, on page 363	Create a CSV file that contains the new phones that you want to add.
Step 3	Insert Phones, on page 364	Use Bulk Administrations's Insert Phones function to add the new phones to the database.

Configure BAT Provisioning Template

Use this procedure to create a phone template with common settings that you can apply via Bulk Administration to newly provisioned phones of a specific phone model.

Before you begin

This procedure assumes that your users are already deployed on the system and that you have already set up device pools, SIP profiles, and phone security profiles that meet your needs.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Bulk Administration** > **Phones** > **Phone Template**.

Step 2 Click **Add New**.

Step 3 From the **Phone Type** drop-down, select the phone model for which you want to create a template.

Step 4 Enter a **Template Name**.

Step 5 Check the **Require Activation Code for Onboarding** check box. In case of Mobile and Remote Access mode, check the **Allow Activation Code via Mobile and Remote Access** check box.

Step 6 Configure values for the following mandatory fields:

- Device Pool
- Phone Button Template
- Owner User ID
- Device Security Profile
- SIP Profile

Step 7 Complete any remaining fields in the **Phone Template Configuration** window. For help with the fields and their settings, refer to the online help.

Step 8 Click **Save**.

What to do next

Create CSV File with New Phones, on page 363

Create CSV File with New Phones

Use this procedure to create a new csv file with your new phones.

Note You can also create your csv file manually.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Bulk Administration** > **Upload/Download Files**.

Step 2 Click **Find**.

Step 3 Select and download the **bat.xlt** spreadsheet.

Step 4 Open the spreadsheet and go to the **Phones** tab.

Step 5 Add your new phone details to the spreadsheet. If you are using dummy MAC addresses, leave the MAC Address field empty. Check the **Require Activation Code for Onboarding** check box. In case of Mobile and Remote Access mode, check the **Allow Activation Code via Mobile and Remote Access** check box.

Step 6 When you are done, click **Export to BAT Format**.

Step 7 From Cisco Unified CM Administration, choose **Bulk Administration** > **Upload/Download Files**.

Step 8 Upload the csv file.

a) Click **Add New**.
b) Click **Choose File** and select the csv file for uploading.
c) Select **Phones** as the target.
d) Select **Insert Phones - Specific Details** for the transaction type.
e) Click **Save**.

What to do next

Insert Phones, on page 364

Insert Phones

Use this procedure to insert new phones from a csv file.

Procedure

Step 1 Select **Bulk Administration** > **Phones** > **Insert Phones**.

Step 2 From the **File Name** drop-down, select your csv file.

Step 3 From the **Phone Template Name** drop-down, select the provisioning template that you created.

Step 4 Check the **Create Dummy MAC Address** check box.

Note For added security, you can add actual MAC addresses to the csv file such that the activation code works only for the phone with the matching MAC address. In this instance, leave this check box unchecked.

Step 5 Check the **Run Immediately** check box to run the job right away. If you choose to run the job later, you must schedule the job in the Bulk Administration Tool's Job Scheduler.

Step 6 Click **Submit.**

What to do next

Activate Phones, on page 365

Activate Phones

After provisioning, distribute activation codes to your phone users so that they can activate their phones. Following are two options for gathering and distributing activation codes:

- Self-Care Portal—Phone users can log in to the Self-Care Portal in order obtain the activation code that applies to their phone. They can either input the code on the phone manually, or use their phone's video camera to scan the barcode that displays in Self-Care. Either method will work. To use Self-Care to activate the phone, the **Show Phones Ready to Activate** enterprise parameter must be set to **True** in Cisco Unified Communications Manager (this is the default setting).

Note For additional requirements on how to configure user access for the Self-Care portal, see the "Self-Care Portal" chapter of the *Feature Configuration Guide for Cisco Unified Communications Manager*.

- CSV File—You can also export the list of outstanding users and activation codes to a csv file, which you can then distribute to your users. For a procedure, see Export Activation Codes, on page 365.

Registration Process

Phone users must enter the activation code on their phone in order to use their phones. After a phone user enters the correct activation code on the phone, the following occurs:

- Their phone authenticates with Cisco Unified Communications Manager.
- The phone configuration in Cisco Unified Communications Manager updates with the actual MAC address of the phone.
- The phone downloads the configuration file and any other relevant files from the TFTP server and registers with Cisco Unified Communications Manager.

What to do Next

The phone is now ready to use.

Export Activation Codes

Use this procedure to export a csv file of activation codes along with their corresponding phones and users. You can use this file to distribute activation codes to your users.

Procedure

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

Step 2 From **Related Links**, select **Export Activation Codes** and click **Go**.

Device Onboarding Task Flow (Mobile and Remote Access Mode)

Complete these tasks to onboard new phones using activation codes, in Mobile and Remote Access mode.

Before you begin

The **Cisco Device Activation Service** must be running in Cisco Unified Serviceability (the service is running by default). To verify that the service is running, go to Activate the Device Activation Service, on page 360.

Procedure

	Command or Action	Purpose
Step 1	Enable Cisco Cloud Onboarding via Mobile and Remote Access, on page 367	Under **Cloud Onboarding**, generate voucher, enable Activation Code Onboarding and specify the Mobile and Remote Access activation domain.
Step 2	Mobile and Remote Access Service Domain Configuration (Optional), on page 367	Onboard the cluster to the cloud to allow remote Mobile and Remote Access device onboarding to a specific Mobile and Remote Access Activation Domain.
Step 3	Upload Custom Certificate (Optional), on page 367	Optional. If you want to use your own custom certificates, remote Mobile and Remote Access endpoints will be able to download them from the cloud and use them to connect to Expressway.
Step 4	Provision phones with activation code requirement. Following are two provisioning sample options: • Add Phone with Activation Code Requirement, on page 361 • Add Phones with Activation Codes via Bulk Administration, on page 362	You must provision the phone in the Unified CM database. Unified CM has a variety of provisioning methods that you can use, including these sample options.
Step 5	Activate Phones, on page 365	Distribute activation codes to users. Users must enter the code on the phone in order to use the phone.

Enable Cisco Cloud Onboarding via Mobile and Remote Access

Procedure

Step 1 To authorize the cluster (CCMAct service) to connect to the cloud-based device activation service, generate the voucher by clicking the **Generate Voucher** button.

Step 2 Specify an Mobile and Remote Access Activation Domain. (This is copied to the Mobile and Remote Access Service Domain list automatically.)

Step 3 Enable activation code onboarding by checking the 'Enable the Activation Code Onboarding' and 'Allow Mobile and Remote Access Onboarding' checkboxes. If you configured device defaults onboarding using 'Auto Registration', then the 'Allow Mobile and Remote Access Onboarding' checkbox is disabled and automatically checked as it can only work for phones in Mobile and Remote Access mode. If you configured device defaults onboarding using 'Activate Code', then both the check boxes are available.

Step 4 Click **Save**.

Mobile and Remote Access Service Domain Configuration (Optional)

To configure Mobile and Remote Access Service Domain for your phone, use the following procedure:

Procedure

Step 1 Choose **Advanced Features** > **Mobile and Remote Access Service Domain** to access the Mobile and Remote Access Service Domain window.

Step 2 Enter the Mobile and Remote Access Service Domain name.

Step 3 Enter the SRV record for the Expressway-E that is used for activation.

Step 4 Choose the default Mobile and Remote Access Service Domain by checking the **Default** check box next to the selected domain. This is the domain that is used when you choose '< None >' at the device pool level.

Step 5 Access the Dependency Records using the link on the row of that record that also lists the number of dependencies.

Upload Custom Certificate (Optional)

To upload custom certificates, use the following procedure:

Procedure

Step 1 Upload the certificates to the Expressway. Do not remove any other certificates.

Step 2 Upload the new certificates to Unified Communications Manager using the path **CUCM OS Administration**> **Certificate Management** . Use the “Phone-Edge-trust” type. (Unified Communications Manager sends these to the cloud and then to the phone to access the Expressway.)

Step 3 Remove any other “Phone-Edge-trust” type certificates, as desired, so that the custom certificates are the only ones in use.

Additional Tasks for Activation Code

The following table lists additional tasks that you may need for activation codes.

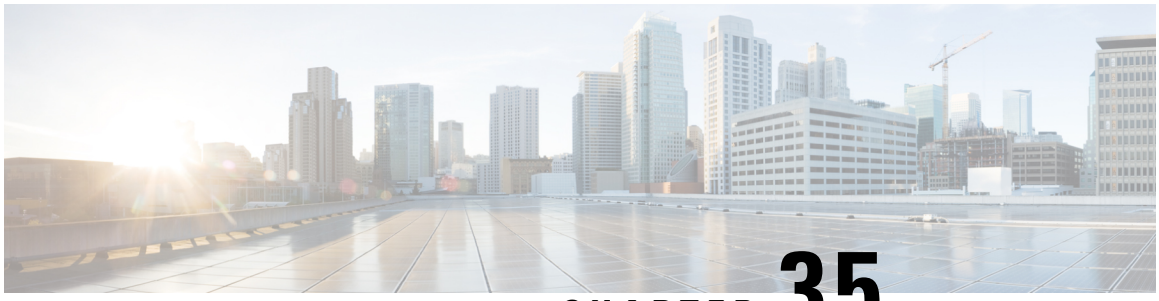
Task	Procedure
Generate activation codes for registered phones	If you want to generate an activation code for an already-registered phone: **1.** From Cisco Unified CM Administration, choose **Device** > **Phone**. **2.** Search for and open the **Phone Configuation** for the phone for which you want to generate an activation code. **3.** Check the **Requires Activation Code for Onboarding** check box and click **Save**.
Regenerate activation codes for unregistered phones	To generate a new activation code for an unregistered phone, such as may be required if the activation process for a new phone fails, do the following: **1.** From Cisco Unified CM Administration, choose **Device** > **Phone**. **2.** Search for and open the **Phone Configuation** for the phone for which you want to generate an activation code. **3.** Click **Release Activation Code** **4.** Click **Generate New Activation Code** and click **Save**.
Set Optional Activation Code Parameters	If you want to configure optional service parameters for activation codes. **1.** From Cisco Unified CM Administration, choose **System > Service Parameters**. **2.** From the **Server** drop-down, select the publisher node. **3.** From the **Service** drop-down, select **Cisco Device Activation Service**. **4.** Configure a value for the following optional service parameters. For help with the settings, refer to the context-sensitive help • **Activation Time to Live (Hours)**—The number of hours that an activation code remains active. The default is 168 • **Enable Mobile and Remote Access Activation**—Set this to True (the default setting) to enable Mobile and Remote Access activation. • **Mobile and Remote Access Activation Domain**—The domain where Mobile and Remote Access device activation takes place. **5.** Click **Save**.

Activation Code Use Cases

The following table highlights sample use cases with device onboarding via activation codes.

Use Case	Description
Replace an existing phone	Activation codes make it easy to replace existing phones. For example, let's say that a remote worker needs a new phone as their phone is damaged. • The administrator opens the **Phone Configuration** settings for the damaged phone in Unified Communications Manager. • The administrator blanks out the **MAC Address**, checks the **Requires Activation Code for Onboarding** check box, and clicks **Save**. • The user acquires a new phone of the same phone model, and plugs their phone into the network. • The user logs in to Self-Care to get their activation code, and inputs the code on the phone. The phone onboards successfully. **Note** In this scenario, the user can onboard any new phone so long as it is the same phone model as the damaged phone. In a more secure environment, the administrator may need to provision a replacement phone to replace the old phone (see below).
Secure shipping of new phone with activation codes	In a more secure environment where you can ensure that phone shipping process is secure by ting the activation code to a specific MAC address as follows: • The administrator provisions a new phone in Unified Communications Manager. • In the **Phone Configuration** settings for the new phone, the administrator enters the phone's actual **MAC Address** and checks the **Requires Activation Code for Onboarding** check box. • The administrator packages the phone and ships the phone to the user. • The user plugs the new phone into the network. • The user logs in to Self-Care to get the activation code, enters the code on the phone. The phone onboards successfully. **Note** In this scenario, the user can onboard only that specific phone.

Use Case	Description
Secure shipping of new phone (autoregistration)	As an alternative to activation codes, you can also use autoregistration and TAPS to securely ship phones to a remote worker: • In the **Device Defaults Configuration**, the administrator makes sure that the **Onboarding Method** for the phone model is **Autoregistration**. • The administrator provisions a new phone in Unified Communications Manager. In the **Phone Configuration** for the new phone, the administrator blanks out the phone's actual **MAC Address**. • The administrator packages the phone and ships the phone to the user. • The user plugs the new phone into the network, and lets it autoregister. • The user uses TAPS to map the autoregistered record back to the old record. **Note** This scenario requires you to configure both autoregistration and TAPS.
Re-onboarding phones via autoregistration	You can switch onboarding methods for specific phone models between Activation Codes and Autoregistration via the **On-Premise Onboarding Method** field in the **Device Defaults Configuration** window. **Note** If you want to re-onboard an existing phone via autoregistration, you must delete the existing record from the database for autoregistration to work.
Onboarding On-Premise phones for Use in Mobile and Remote Access mode	You can onboard the phones on-premise, and then mark the phone for onboarding again in Mobile and Remote Access mode to leverage the security provided by OAuth connection to Expressway and trusted connection from Expressway to Cisco Unified Communications Manager. In this scenario, with 'Allow Activation Code via Mobile and Remote Access' enabled, the phone onboards on-premise, validates the OAuth access token that it received, and switches to Mobile and Remote Access mode and initiates communication with the Expressway. If your internal network does not allow communication with the Expressway from on-premise, the phone does not register, but is ready to contact the Expressway when it is powered up off-premise. **Note** The off-premise phones that are unregistered cannot update their firmware load.This scenario is useful with out-of-the-box phones that need to be on premise to download the latest firmware and use the Activation Code feature.



CHAPTER 35

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, 7970, and 7971) 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 372	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 373	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 374	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 375	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 375	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 377	Disable autoregistration for the node as soon as you are finished registering new devices.
Step 7	Reuse Autoregistration Numbers, on page 378	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 373

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 372

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 374

Related Topics

Class of Service, on page 174

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 373

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 375

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 374

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 375

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 375

- 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 375

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 378.

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.

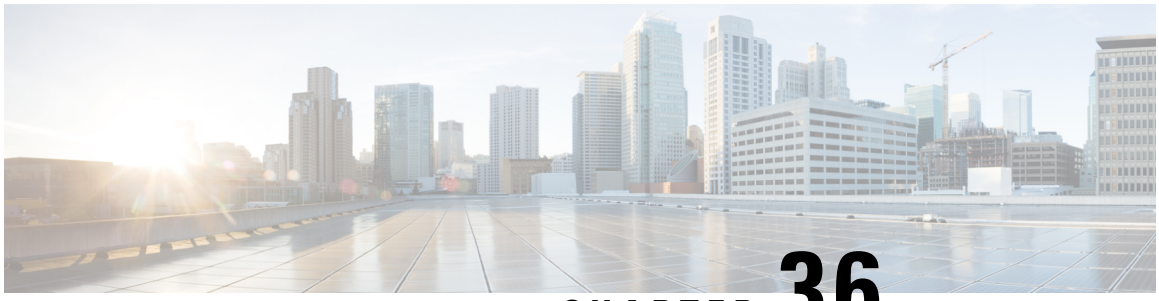
Step 3 Write down the current settings in the **Starting Directory Number** and **Ending Directory Number** fields.

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 36

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 Analog FXS Ports

You can enable self-provisioning on analog FXS ports so that the users can call the self-provisioning IVR and assign their associated DN to that analog port. In addition, for the provisioned phones, the user can unassign the DN associated with the analog voice gateway port and assign it to another user.

Procedure

1. Plugin the analog phone in the gateway's FXS voice port. Since the port is auto-registered or pre configured (manually), the phone will automatically get DN from the auto-registered pool or assigned DN.
2. Call Self-Provision IVR from the auto-registered analog device.
3. Enter Self-Service ID and PIN.

Note Upon confirmation, the analog device is provisioned using the End User Primary Extension. The auto-registered DN is released to the pool.

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 381	In Cisco Unified Serviceability, activate the **Self-Provisioning IVR** and **CTI Manager** services.
Step 2	Enable Autoregistration for Self-Provisioning, on page 382	Enable autoregistration parameter for self-provisioning
Step 3	Configure CTI Route Point, on page 382	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 383	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 383	Configure an application user for the self-provisioning IVR. Associate the CTI route point to the application user.
Step 6	Configure the System for Self-Provisioning, on page 384	Configure self-provisioning settings for your system, including associating the application user and CTI route point to the self-provisioning IVR.
Step 7	Enable Self-Provisioning in a User Profile, on page 384	Enables the users to Self-Provision phones in the user profile to which they are assigned.

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.

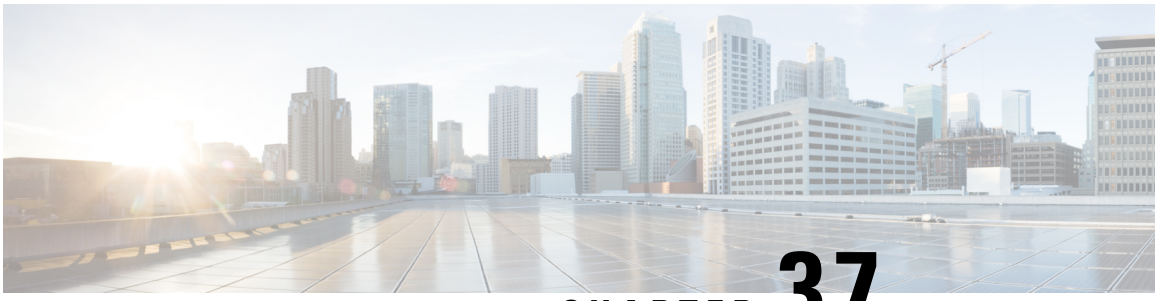
Step 4 Configure user settings for Self-Provisioning:

- 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.
- If you want users to be able to use self-provisioning to reassign a previously assigned phone, check the **Allow Provisioning of a phone that is already assigned to a different End User** setting in the user profile page associated with the end user of old device. Users can reassign a previously assigned phone only if this check box is enabled in the User Profile that is associated to the old device.

Step 5 Click **Save**.

PART VI

Reference Information



CHAPTER 37

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 29: 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 Tra 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 Un 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 30: 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 31: 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 32: 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 Transp (HTTP)
Browser	Unified Communications Manager	443, 8443 / TCP	Hypertext Transp over SSL (HTTPS

Web Requests From Cisco Unified Communications Manager to Phone

Table 33: 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 Transp (HTTP)

Signaling, Media, and Other Communication Between Phones and Cisco Unified Communications Manager

Table 34: 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	Phones use this port number to use the Headset Management feature.
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 35: 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 c 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 P (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) R
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 b syste the ty gatew For IC the H range 1100
Unified Communications Manager	Gateway		
Gateway	Unified Communications Manager	2000 / TCP	Skinny Client Co (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 us Real-Time Transp (RTP) and Real-T Control Protocol (for audio, video a channel when Cis Communications not have ports for
Gateway	Unified Communications Manager	5060 / TCP and UDP	Session Initiation 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 36: 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 Attendar (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 Attendar (AC) clients regis AC server for line state information.
Unified Communications ManagerAttendant Console	Unified Communications Manager	4321 / UDP	Cisco Unified Co Manager Attendar (AC) clients regis server for call co
Unified Communications Manager with SAF/CCD	IOS Router running SAF image	5050 / TCP	Multi-Service IOS 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 API programmatic rea writes to the Cisc Communications database that thir as billing or telepl management appl

Communication Between CTL Client and Firewalls

Table 37: 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 38: 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 39: 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 Manageme 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

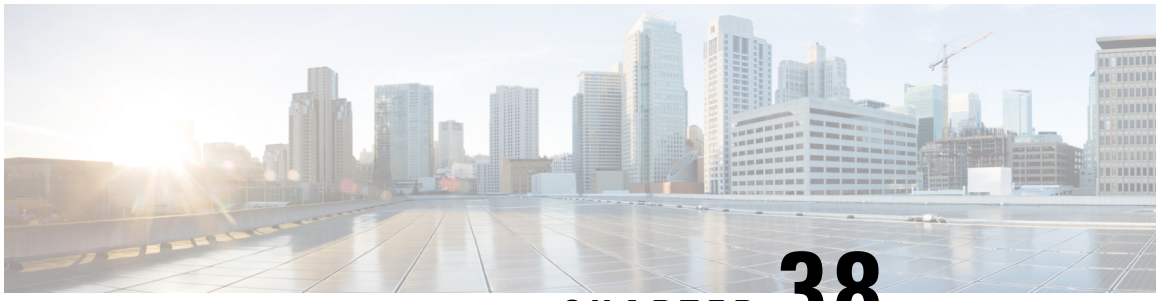
http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_design_guidance09186a00801f8e30.html

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 38

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 40: 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 41: 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 42: 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 43: 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 44: 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 45: 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 46: 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 47: 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 48: 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 49: 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 50: 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 51: 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 52: 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 53: 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 54: 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 55: 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 56: 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 57: 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 58: 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 59: 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 60: 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 61: 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 62: 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[1]	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

[1] This is the default port, however you can configure the PostgreSQL database to listen on any port.

Table 63: 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 64: 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 65: 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 66: 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 67: 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 68: 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) number carries ec traffic. It does not port as indicated i heading.
IM and Presence	Endpoint/IM and Presence		

Table 69: 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 70: 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 71: MS-SQL DB Configuration

From (Sender)	To (Listener)	Source Port	Destination Port	Protocol
IM and Presence Publisher	Database	[37240 – 61000]	7	TCP

Table 72: MS-SQL Persistent Chat Configuration

From (Sender)	To (Listener)	Source Port	Destination Port	Protocol
IM and Presence Publisher	Database	37240 – 61000	1433	TCP

Table 73: 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.