Administration Guide for Cisco Unified Communications Manager and IM and Presence Service, Release 12.0(1)

First Published: 2017-08-23

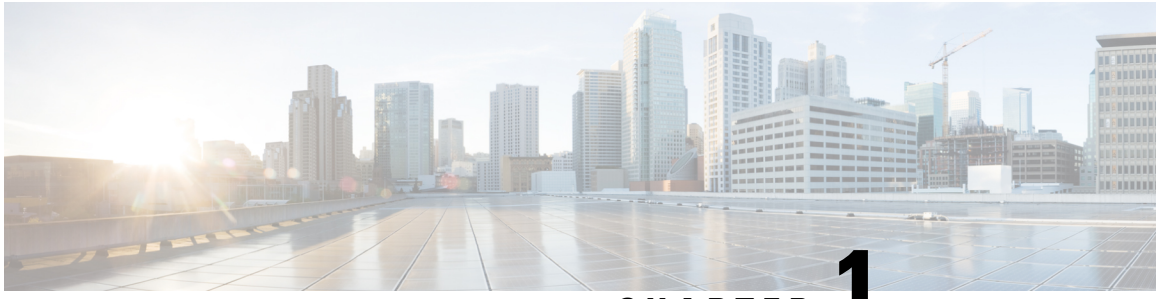
Last Modified: 2021-10-19

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

PART I

Administration Overview



CHAPTER 1

Administration Overview

Cisco Unified CM Administration Overview

Cisco Unified CM Administration, a web-based application, is the main administration and configuration interface for Cisco Unified Communications Manager. You can use Cisco Unified CM Administration to configure a wide range of items for your system including general system components, features, server settings, call routing rules, phones, end users, and media resources.

Configuration Menus

The configuration windows for Cisco Unified CM Administration are organized under the following menus:

- System—Use the configuration windows under this menu to configure general system settings such as server information, NTP settings, Date and Time groups, Regions, DHCP, LDAP integration, and enterprise parameters.
- Call Routing-—Use the configuration windows under this tab to configure items related to how Cisco Unified Communications Manager routes calls, including route patterns, route groups, hunt pilots, dial rules, partitions, calling search spaces, directory numbers, and transformation patterns.
- Media Resources—Use the configuration windows under this tab to configure items such as media resource groups, conference bridges, annunciators, and transcoders.
- Advanced Features—Use the configuration windows under this tab to configure features such as voice-mail pilots, message waiting, and call control agent profiles.
- Device—Use the configuration windows under this tab to set up devices such as phones, IP phone services, trunks, gateways, softkey templates, and SIP profiles.
- Application—Use the configuration windows under this tab to download and install plug-ins such as Cisco Unified JTAPI, Cisco Unified TAPI, and the Cisco Unified Real-Time Monitoring Tool.

- User Management—Use the configuration windows under the User Management tab to configure end users and application users for your system.
- Bulk Administration-—Use the Bulk Administration Tool to import and configure large numbers of end users or devices at a time.
- Help—Click this menu to access the online help system. The online help system contains documentation that will assist you in configuring settings for the various configuration windows on your system.

Operating System Administration Overview

Use Cisco Unified Communications Operating System Administration to configure and manage your operating system and perform the following administration tasks:

- Check software and hardware status
- Check and update IP addresses
- Ping other network devices
- Manage NTP servers
- Upgrade system software and options
- Manage node security, including IPsec and certificates
- Manage remote support accounts
- Restart the system

Operating System Status

You can check the status of various operating system components, including the following:

- Clusters and nodes
- Hardware
- Network
- System
- Installed software and options

Operating System Settings

You can view and update the following operating system settings:

- IP—Updates the IP addresses and DHCP client settings that ypu entered when the application was installed.
- NTP Server settings—Configures the IP addresses of an external NTP server; adds an NTP server.
- SMTP settings—Configures the simple mail transfer protocol (SMTP) host that the operating system will use for sending email notifications.

Operating System Security Configuration

You can manage security certificates and IPsec settings. From the **Security** menu, you can choose the following security options:

- Certificate Management—Manages certificates and certificate signing requests (CSRs). You can display, upload, download, delete, and regenerate certificates. Through certificate management, you can also monitor the expiration dates of the certificates on the node.

- IPsec Management—Displays or updates existing IPsec policies; sets up new IPsec policies and associations.

Software Upgrades

You can upgrade the software version that is running on the operating system or to install specific software options, including Cisco Unified Communications Operating System locale installers, dial plans, and TFTP server files.

From the **Install/Upgrade** menu option, you can upgrade system software from either a local disc or a remote server. The upgraded software is installed on the inactive partition, and you can then restart the system and switch partitions, so the system starts running on the newer software version. For more information, see the *Upgrade Guide for the Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html.

Note You must perform all software installations and upgrades through the software upgrade features that are included in the Cisco Unified Communications Operating System interface and the CLI. The system can upload and process only software that is Cisco Systems approved. You cannot install or use third-party or Windows-based software applications.

Services

The application provides the following operating system utilities:

- Ping—Checks connectivity with other network devices.
- Remote Support—Sets up an account that Cisco support personnel can use to access the system. This account automatically expires after the number of days that you specify.

CLI

You can access the CLI from the Operating System or through a secure shell connection to the server. For more information, see the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Authenticated Network Time Protocol Support

With Cisco Unified Communications Manager release 12.0 (1), the authenticated Network Time Protocol (NTP) capability for Unified Communications Manager is supported. This support is added to secure the NTP server connection to Unified Communications Manager. In the previous releases, the Unified Communications Manager connection to the NTP server was not secure.

This feature is based on symmetric key-based authentication and is supported by NTPv3 and NTPv4 servers. Unified Communications Manager supports only SHA1-based encryption. The SHA1-based symmetric key support is available from NTP version 4.2.6 and above.

- Symmetric Key
- No Authentication

You can check the authentication status of the NTP servers through administration CLI or **NTP Server List** page of the **Cisco Unified OS Administration** application.

Cisco Unified Serviceability Overview

Cisco Unified Serviceability is a web-based troubleshooting tool that provides a host of services, alarms, and tools that assist administrators in managing their systems. Among the features that Cisco Unified Serviceability offers to administrators are:

- Start and Stop Services—Administrators can set up an assortment of services that help administrators manage their systems. For example, you can start the Cisco CallManager Serviceability RTMT service thereby allowing administrators to use the Real-Time Monitoring Tool to monitor the health of your system.
- SNMP—SNMP facilitates the exchange of management information among network devices, such as nodes, routers, and so on. As part of the TCP/IP protocol suite, SNMP enables administrators to remotely manage network performance, find and solve network problems, and plan for network growth.
- Alarms—Alarms provide information on the runtime status and state of your system, so that you can troubleshoot problems that are associated with your system.
- Traces—Trace tools help you to troubleshooting issues with voice applications.
- Cisco Serviceability Reporter—The Cisco Serviceability Reporter generates daily reports in Cisco Unified Serviceability.
- SNMP—SNMP facilitates the exchange of management information among network devices, such as nodes, routers, and so on. As part of the TCP/IP protocol suite, SNMP enables administrators to remotely manage network performance, find and solve network problems, and plan for network growth.
- CallHome—Configure the Cisco Unified Communications Manager Call Home feature, allowing Cisco Unified Communications Manager to communicate and send the diagnostic alerts, inventory, and other messages to the Smart Call Home back-end server

Additional Administrative Interfaces

Using Cisco Unified Serviceability, you can start services that allow you to use the following additional administrative interfaces:

- Real-Time Monitoring Tool—The Real-Time Monitoring Tool is a web-based interface that helps you to monitor the health of your system. Using RTMT, you can view alarms, counters and reports that contain detailed information on the health of your system.
- Dialed Number Analyzer—The Dialed Number Analyzer is a web-based interface that helps administrators to troubleshoot issues with the dial plan.
- Cisco Unified CDR Analysis and Reporting—CDR Analysis and Reporting collects call details records showing the details of the calls that are placed on your system.

For details about how to use Cisco Unified Serviceability, 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.

Cisco Unified Reporting Overview

The Cisco Unified Reporting web application generates consolidated reports for troubleshooting or inspecting cluster data. You can access the application at the Unified Communications Manager and Unified Communications Manager IM and Presence Service consoles.

This tool provides an easy way to take a snapshot of cluster data. The tool gathers data from existing sources, compares the data, and reports irregularities. When you generate a report in Cisco Unified Reporting, the report combines data from one or more sources on one or more servers into one output view. For example, you can view the following reports to help you administer your system:

- Unified CM Cluster Overview—View this report to get a snapshot of your cluster, including Cisco Unified Communications Manager and IM and Presence Service versions, server hostnames, and hardware details.
- Phone Feature List—View this report if you are configuring features. This report provides a list of which phones support which Cisco Unified Communications Manager features.
- Unified CM Phones Without Lines—View this report to see which phones in your cluster do not have a phone line.

For a full list of reports offered through Cisco Unified Reporting, as well as instructions on how to use the application, see the *Cisco Unified Reporting Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Disaster Recovery System Overview

The Disaster Recovery System (DRS), which can be invoked from Cisco Unified Communications Manager Administration, provides full data backup and restore capabilities. The Disaster Recovery System allows you to perform regularly scheduled automatic or user-invoked data backups.

DRS restores its own settings (backup device settings and schedule settings) as part of the platform backup/restore. DRS backs up and restores the `drfDevice.xml` and `drfSchedule.xml` files. When the server is restored with these files, you do not need to reconfigure DRS backup device and schedule.

The Disaster Recovery System includes the following capabilities:

- A user interface for performing backup and restore tasks.
- A distributed system architecture for performing backup and restore functions.
- Scheduled backups.
- Archive backups to a physical tape drive or remote SFTP server.

Bulk Administration Tool Overview

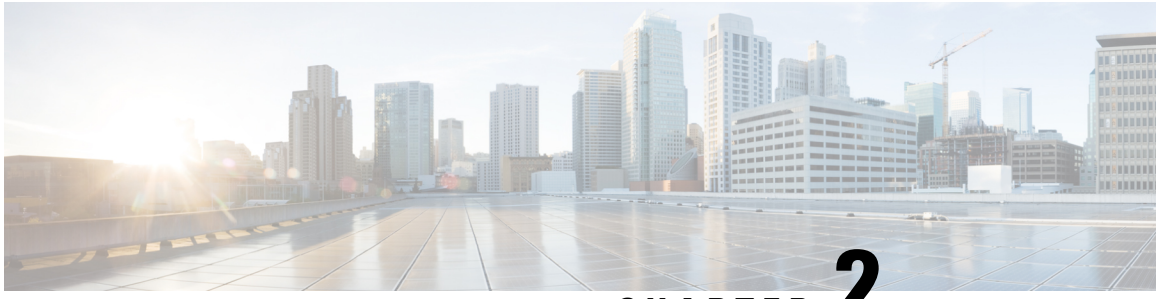
In Cisco Unified CM Administration, uses the Bulk Administration menu and submenu options to configure entities in Unified Communications Manager through use of the Bulk Administration Tool.

The Unified Communications Manager Bulk Administration Tool (BAT), a web-based application, lets administrators perform bulk transactions to the Unified Communications Manager database. BAT lets you add, update, or delete a large number of similar phones, users, or ports at the same time. When you use Cisco Unified CM Administration, each database transaction requires an individual manual operation, while BAT automates the process and achieves faster add, update, and delete operations.

You can use BAT to work with the following types of devices and records:

- Add, update, and delete Cisco IP Phones, gateways, phones, computer telephony interface (CTI) ports, and H.323 clients
- Add, update, and delete users, user device profiles, Cisco Unified Communications Manager Assistant managers and assistants
- Add or delete Forced Authorization Codes and Client Matter Codes
- Add or delete call pickup groups
- Populate or depopulate the Region Matrix
- Insert, delete, or export the access list
- Insert, delete, or export remote destinations and remote destination profiles
- Add Infrastructure Devices

For details on how to use the Bulk Administration Tool, refer to the *Bulk Administration Guide for Cisco Unified Communications Manager*.



CHAPTER 2

Getting Started

Sign In to Adminstrative Interfaces

Use this procedure to sign in to any of the administrative interfaces in your system.

Procedure

Step 1 Open the Unified Communications Manager interface in your web browser.

Step 2 Choose the administration interface from the **Navigation** drop-down list.

Step 3 Click **Go**.

Step 4 Enter your username and password.

Step 5 Click **Login**.

Reset the Administrator or Security Password

If you lose the administrator password and cannot access your system, use this procedure to reset the password.

Note For password changes on IM and Presence nodes, stop the Cisco Presence Engine service in all IM and Presence nodes before resetting the administrator password. After the password reset, restart the Cisco Presence Engine service in all the nodes. Make sure that you perform this task during maintenance because you may face presence issues when the PE is stopped.

Before you begin

- You require physical access to the node on which you perform this procedure.

- At any point, when you are requested to insert CD or DVD media, you must mount the ISO file through the vSphere client for the VMWare server. See "Adding DVD or CD Drives to a Virtual Machine" https://www.vmware.com/support/ws5/doc/ws_disk_add_cd_dvd.html for guidance.
- The security password on all nodes in a cluster must match. Change the security password on all machines, or the cluster nodes will not communicate.

Procedure

Step 1 Sign in to the CLI on the publisher node with the following username and password:

a) Username: **`pwrecovery`**

b) Password: **`pwreset`**

Step 2 Press any key to continue.

Step 3 If you have a valid CD/DVD in the disk drive or you mounted an ISO file, remove it from the VMWare client.

Step 4 Press any key to continue.

Step 5 Insert a valid CD or DVD into the drive or mount the ISO file.

Note For this test, you must use a disk or ISO file that is data only.

Step 6 After the system verifies the last step, you are prompted to enter one of the following options to continue:

- Enter **a** to reset the administrator password.
- Enter **s** to reset the security password.

Note You must reset each node in a cluster after you change its security password. Failure to reboot the nodes causes system service problems and problems with the administration windows on the subscriber nodes.

Step 7 Enter the new password, and then reenter it to confirm.

The administrator credentials must start with an alphabetic character, be at least six characters long, and can contain alphanumeric characters, hyphens, and underscores.

Step 8 After the system verifies the strength of the new password, the password is reset, and you are prompted to press any key to exit the password reset utility.

If you want to set up a different administrator password, use the CLI command **set password**. For more information, see the *Command Line Interface Reference Guide for CiscoUnified Solutions* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Shut Down or Restart the System

Use this procedure if you need to shut down or restart your system, for example, after you make a configuration change.

Before you begin

If the server is forced to shutdown and restart from your virtual machine, the file system may become corrupted. Avoid a forced shutdown; instead, wait for the server to shutdown properly after this procedure or after you run **utils system shutdown** from the CLI.

Note If you force shutdown or restart the virtual machine from VMware administration tools (vCenter or Embedded Host Client):

Procedure

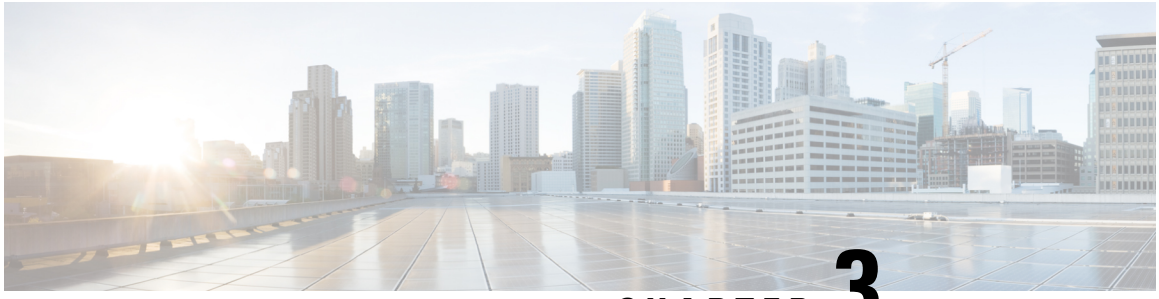
Step 1 From Cisco Unified OS Administration, choose **Settings** > **Version**.

Step 2 Perform one of the following actions:

- Click **Shutdown** to stop all processes and shut down the system.
- Click **Restart** to stop all processes and restart the system.

PART II

Manage Users



CHAPTER 3

Manage User Access

User Access Overview

Manage user access to Cisco Unified Communications Manager by configuring the following items:

- Access Control Groups
- Roles
- User Rank

Access Control Group Overview

An access control group is a list of users and the roles that are assigned to those users. When you assign an end user, application user, or administrator user to an access control group, the user gains the access permissions of the roles that are associated to the group. You can manage system access by assigning users with similar access needs to an access control group with only the roles and permissions that they need.

There are two types of access control groups:

- Standard Access Control Groups—These are predefined default groups with role assignments that meet common deployment needs. You cannot edit the role assignments in a standard group. However, you can add and delete users, in addition to editing the User Rank requirement. For a list of standard access control groups, and their associated roles, see Standard Roles and Access Control Groups, on page 23.
- Custom Access Control Groups—Create your own access control groups when none of the standard groups contain the role permissions that meet your needs.

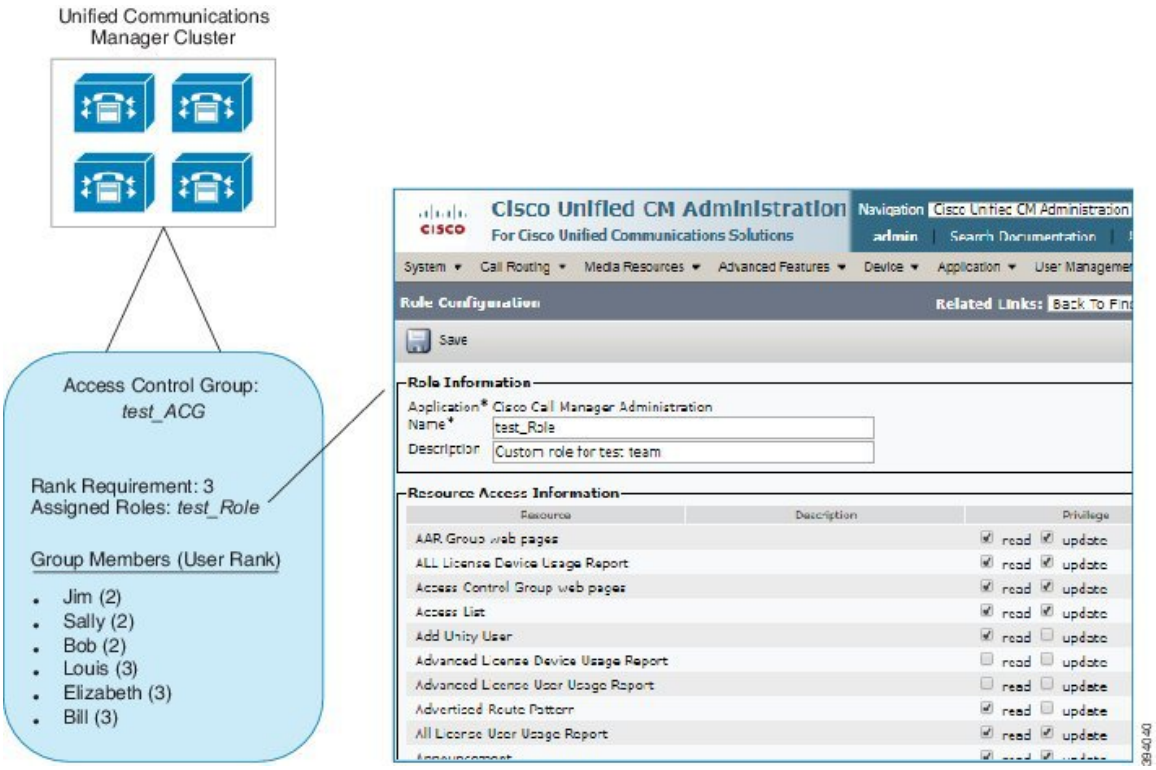
The User Rank framework provides a set of controls over the access control groups to which a user can be assigned. To be assigned to an access control group, a user must meet the minimum rank requirement for that group. For example, end users whom have a User Rank of 4 can be assigned only to access control groups

with minimum rank requirements between 4 and 10. They cannot be assigned to groups with a minimum rank of 1.

Example - Role Permissions with Access Control Groups

The following example illustrates a cluster where the members of a testing team are assigned to access control group **test_ACG**. The screen capture on the right displays the access settings of test_Role, which is the role that is associated to the access control group. Also note that the access control group has a minimum rank requirement of 3. All of the group members must have a rank between 1-3 to be able to join the group.

Figure 1: Role Permissions with Access Control Groups



Roles Overview

Users obtain system access privileges via the roles that are associated to the access control group of which the user is a member. Each role contains a set of permissions that is attached to a specific resource or application, such as Cisco Unified CM Administration or CDR Analysis and Reporting. For an application such as Cisco Unified CM Administration, the role may contain permissions that let you view or edit specific GUI pages in the application. There are three levels of permissions that you can assign to a resource or application:

- Read—Allows a user to view settings for a resource.
- Update—Allows a user to edit settings for a resource.
- No Access—If a user has neither Read or Update access, the user has no access to view or edit settings for a given resource.

Role Types

When provisioning users, you must decide what roles you want to apply and then assign users to an access control group that contains the role. There are two main types of roles in Cisco Unified Communications Manager:

- Standard roles—These are preinstalled default roles that are designed to meet the needs of common deployments. You cannot edit permissions for standard roles.
- Custom roles—Create custom roles when no standard roles have the privileges you need.

User Rank Overview

The User Rank hierarchy provides a set of controls over which access control groups an administrator can assign to an end user or application user.

When provisioning end users or application users, administrators can assign a user rank for the user. Administrators can also assign a user rank requirement for each access control group. When adding users to access conttrol groups, administrators can assign users only to the groups where the user's User Rank meets the group's rank requirement. For example, an administrator can assign a user whom has a User Rank of 3 to access control groups that have a User Rank requirement between 3 and 10. However, an administrator cannot assign that user to an access control group that has a User Rank requirement of 1 or 2.

Administrators can create their own user rank hierarchy within the **User Rank Configuration** window and can use that hierarchy when provisioning users and access control groups. Note that if you don't configure a user rank hierarchy, or if you simply don't specify the User Rank setting when provisioning users or access conrol groups, all users and access control groups are assigned the default User Rank of 1 (the highest rank possible).

User Access Prerequisites

Make sure to review your user needs so that you know what level of access your users require. You will want to assign roles that have the access privileges your users require, but which do not provide access to systems that they should not be able to access.

Before you create new roles and acess control groups, review the list of standard roles and access control groups to verify whether an existing access control group has the roles and access permissions that you need. For details, see Standard Roles and Access Control Groups, on page 23.

User Access Configuration Task Flow

Complete the following tasks to configure user access.

Before you begin

If you want to use default roles and access control groups then you can skip tasks for creating customized roles and access control groups. You can assign your users to the existing default access control groups.

Procedure

	Command or Action	Purpose
Step 1	Configure User Rank Hierarchy, on page 16	Set up the user rank hierarchy. Note that if you skip this task, all users and access control groups get assigned the default user rank of 1 (the highest rank).
Step 2	Create a Custom Role, on page 16	Create custom roles if the default roles don't have the access permissions you need.
Step 3	Create Access Control Group, on page 17	Create custom access control groups if the default groups don't have the role assignments you need.
Step 4	Assign Users to Access Control Group, on page 18	Add or delete users from a standard or custom access control group.
Step 5	Configure Overlapping Privilege Policy for Access Control Groups, on page 19	Optional. This setting is used if users are assigned to multiple access control groups with conflicting permissions.

Configure User Rank Hierarchy

Use this procedure to create a custom user rank hierarchy.

Note If you don't configure a user rank hierarchy, all users and access control groups get assigned a user rank of 1 (the highest possible rank) by default.

Procedure

Step 1 From Cisco Unified CM Administration, choose**User Management** > **User Settings** > **User Rank**.

Step 2 Click **Add New**.

Step 3 From the **User Rank** drop-down menu, select a rank setting between 1–10. The highest rank is 1.

Step 4 Enter a **Rank Name** and **Description**.

Step 5 Click **Save**.

Step 6 Repeat this procedure to add additional user ranks.
You can assign the user rank to users and access control groups to control which groups a user can be assigned to.

Create a Custom Role

Use this procedure to create a new role with customized privileges. You may want to do this if there are no standard roles with the exact privileges that you need. There are two ways to create a role:

- Use the **Add New** button to create and configure the new role from scatch.
- Use the **Copy** button if an existing role has access privileges that are close to what you need. You can copy the privileges of the existing role to a new role that is editable.

Procedure

Step 1 In Cisco Unified CM Administration, click **User Management** > **User Settings** > **Role**.

Step 2 Do either of the following:

- To create a new role, click **Add New**. Choose the **Application** with which this role associates, and click **Next**.
- To copy settings from an existing role, click **Find** and open the existing role. Click **Copy** and enter a name for the new role. Click **OK**.

Step 3 Enter a **Name** and **Description** for the role.

Step 4 For each resource, check the boxes that apply:

- Check the **Read** check box if you want users to be able to view settings for the resource.
- Check the **Update** check box if you want users to be able to edit setttings for the resource.
- Leave both check boxes unchecked to provide no access to the resource.

Step 5 Click **Grant access to all** or **Deny access to all** button to grant or remove privileges to all resources that display on a page for this role.

Note If the list of resources displays on more than one page, this button applies only to the resources that display on the current page. You must display other pages and use the button on those pages to change the access to the resources that are listed on those pages.

Step 6 Click **Save**.

Create Access Control Group

Use this procedure if you need to create a new access control group. You may want to do this if no standard group has the roles and access privileges you need. There are two ways to create a customized group:

- Use the **Add New** button to create and configure the new access control group from scatch.
- Use the **Copy** button if an existing group has role assignments that are close to what you need. You can copy the settings from the existing group to a new and editable group.

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Access Control Groups.**

Step 2 Do either of the following:

- To create a new group from scratch, click **Add New**.

- To copy settings from an existing group, click **Find** and open the existing access control group. Click **Copy** and enter a name for the new group. Click **OK**.

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

Step 4 From the **Available for Users with User Rank as** drop-down, select the minimum User Rank a user must meet to be assigned to this group. The default user rank is 1.

Step 5 Click **Save**.

Step 6 Assign roles to the access control group. The roles you select will be assigned to group members:

a) From **Related Links**, select **Assign Role to Access Control Group**, and click **Go**.
b) Click **Find** to search for existing roles.
c) Check the roles that you want to add and click **Add Selected**.
d) Click **Save**.

What to do next

Assign Users to Access Control Group, on page 18

Assign Users to Access Control Group

Add or delete users from a standard or custom access control group. .

Note You can add only those users whose user rank is the same or higher than the minimum user rank for the access control group.

Note If you are syncing new users from a company LDAP Directory, and your rank hierarchy and access control groups are created with the appropriate permissions, you can assign the group to synced users as a part of the LDAP sync. For details on how to set up an LDAP directory sync, see the *System Configuration Guide for Cisco Unified Communications Manager.*

Procedure

Step 1 Choose **User Management** > **User Settings** > **Access Control Group**.

The **Find and List Access Control Group** window appears.

Step 2 Click **Find** and select the access control group for which you want to update the list of users.

Step 3 From the **Available for Users with User Rank as** drop-down, select the rank requirement that users must meet to be assigned to this group.

Step 4 In the **User** section, click **Find** to display the list of users.

Step 5 If you want to add end users or application users to the access control group, do the following:

a) Click **Add End Users to Access Control Group** or **Add App Users to Access Control Group**.
b) Select the users whom you want to add.

c) Click **Add Selected**.

Step 6 If you want to delete users from the access control group:

a) Select the users whom you want to delete.

b) Click **Delete Selected**.

Step 7 Click **Save**.

Configure Overlapping Privilege Policy for Access Control Groups

Configure how Cisco Unified Communications Manager handles overlapping user privileges that can result from access control group assignments. This is to cover situations where an end user is assigned to multiple access control groups, each with conflicting roles and privilege settings.

Procedure

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

Step 2 Under **User Management Parameters**, configure one of the following values for the **Effective Access Privileges For Overlapping User Groups and Roles** as follows:

- **Maximum**—The effective privilege represents the maximum of the privileges of all the overlapping access control groups. This is the default option.
- **Minimum**—The effective privilege represents the minimum of the privileges of all the overlapping access control groups.

Step 3 Click **Save**.

View User Privilege Report

Perform the following procedure to view the User Privilege report for either an existing end user or an existing application user. The User Privilege report displays the access control groups, roles, and access privileges that are assigned to an end user or application user.

Procedure

Step 1 In Cisco Unified CM Administration, perform either of the following steps:

- For end users, choose **User Management** > **End User**.
- For application users, choose **User Management** > **Application User**.

Step 2 Click **Find** and select the user for whom you want to view access privileges

Step 3 From the **Related Links** drop-down list, choose the **User Privilege Report** and click **Go**.
The User Privilege window appears.

Create Custom Help Desk Role Task Flow

Some companies want their help desk personnel to have privileges to be able to perform certain administrative tasks. Follow the steps in this task flow to configure a role and access control group for help desk team members that allows them to perform tasks such as adding a phone and adding an end user.

Procedure

	Command or Action	Purpose
Step 1	Create Custom Help Desk Role, on page 20	Create a custom role for help desk team members and assign the role privileges for items such as adding new phones and adding new users.
Step 2	Create Custom Help Desk Access Control Group, on page 21	Create a new access control group for the Help Desk role.
Step 3	Assign Help Desk Role to Access Control Group, on page 21	Assign the Help Desk role to the Help Desk access control group. Any users assigned to this access control group will be assigned the privileges of the Help Desk role.
Step 4	Assign Help Desk Members to Access Control Group, on page 22	Assign help desk team members with the privileges of the custom help desk role.

Create Custom Help Desk Role

Perform this procedure to create a custom help desk role that you can assign to help desk members in your organization.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **User Management** > **User Settings** > **Role**.

Step 2 Click **Add New**.

Step 3 From the Application drop-down list, choose the application that you want to assign to this role. For example, **Cisco CallManager Administration**.

Step 4 Click **Next**.

Step 5 Enter the **Name** of the new role. For example, `Help Desk`.

Step 6 Under **Read and Update Privileges** select the privileges that you want to assign for help desk users. For example, if you want help desk members to be able to add users and phones, check the **Read** and **Update** check boxes for User web pages and Phone web pages.

Step 7 Click **Save**.

What to do next

Create Custom Help Desk Access Control Group, on page 21

Create Custom Help Desk Access Control Group

Before you begin

Create Custom Help Desk Role, on page 20

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Access Control Group**.

Step 2 Click **Add New**.

Step 3 Enter a name for the access control group. For example, **`Help_Desk`**.

Step 4 Click **Save**.

What to do next

Assign Help Desk Role to Access Control Group, on page 21

Assign Help Desk Role to Access Control Group

Perform the following steps to configure the Help Desk access control group with the privileges from the Help Desk role.

Before you begin

Create Custom Help Desk Access Control Group, on page 21

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Access Control Group**.

Step 2 Click **Find** and select the access control group that you created for Help Desk.
The **Access Control Group Configuration** window displays.

Step 3 In the **Related Links** drop-down list box, choose the **Assign Role to Access Control Group** option and click **Go**.
The **Find and List Roles** popup displays.

Step 4 Click the **Assign Role to Group** button.

Step 5 Click **Find** and select the Help Desk role.

Step 6 Click **Add Selected**.

Step 7 Click **Save**.

What to do next

Assign Help Desk Members to Access Control Group, on page 22

Assign Help Desk Members to Access Control Group

Before you begin

Assign Help Desk Role to Access Control Group, on page 21

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Access Control Group.**

Step 2 Click **Find** and select the custom Help Desk access control group that you created.

Step 3 Perform either of the following steps:

- If your help desk team members are configured as end users, click **Add End Users to Group**.
- If your help desk team members are configured as application users, click **Add App Users to Group**.

Step 4 Click **Find** and select your help desk users.

Step 5 Click **Add Selected**.

Step 6 Click **Save**.
Cisco Unified Communications Manager assigns your help desk team members with the privileges of the custom help desk role that you created.

Delete Access Control Group

Use the following procedure to delete an access control group entirely.

Before you begin

When you delete an access control group, Cisco Unified Communications Manager removes all access control group data from the database. Ensure you are aware which roles are using the access control group.

Procedure

Step 1 Choose **User Management** > **User Settings** > **Access Control Group**.

The **Find and List Access Control Groups** window appears.

Step 2 Find the access control group that you want to delete.

Step 3 Click the name of the access control group that you want to delete.

The access control group that you chose appears. The list shows the users in this access control group in alphabetical order.

Step 4 If you want to delete the access control group entirely, click **Delete**.

A dialog box appears to warn you that you cannot undo the deletion of access control groups.

Step 5 To delete the access control group, click **OK** or to cancel the action, click **Cancel**. If you click **OK**, Cisco Unified Communications Manager removes the access control group from the database.

Revoke Existing OAuth Refresh Tokens

Use an AXL API to revoke existing OAuth refresh tokens. For example, if an employee leaves your company, you can use this API to revoke that employee's current refresh token so that they cannot obtain new access tokens and will no longer be able to log in to the company account. The API is a REST-based API that is protected by AXL credentials. You can use any command-line tool to invoke the API. The following command provides an example of a cURL command that can be used to revoke a refresh token:

```
curl -k -u "admin:password" https://<UCMaddress:8443/ssosp/token/revoke?user_id=<end_user>
```

where:

- `admin:password` is the login ID and password for the Cisco Unified Communications Manager administrator account.
- `UCMaddress` is the FQDN or IP address of the Cisco Unified Communications Manger publisher node.
- `end_user` is the user ID for the user for whom you want to revoke refresh tokens.

Set up a Remote Account

Configure a remote account in the Unified Communications Manager so that Cisco support can temporarily gain access to your system for troubleshooting purposes.

Procedure

Step 1 From Cisco Unified Operating System Administration, choose **Services** > **Remote Support**.

Step 2 In the **Account Name** field, enter a name for the remote account.

Step 3 In the **Account Duration** field, enter the account duration in days.

Step 4 Click **Save**.
The system generates an encrypted pass phrase.

Step 5 Contact Cisco support to provide them with the remote support account name and pass phrase.

Standard Roles and Access Control Groups

The following table summarizes the standard roles and access control groups that come preconfigured on Cisco Unified Communications Manager. The privileges for a standard role are configured by default. In addition, the access control groups that are associated with a standard role are also configured by default.

For both standard roles and the associated access control group, you cannot edit any of the privileges, or the role assignments.

Table 1: Standard Roles, Privileges, and Access Control Groups

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard AXL API Access	Allows access to the AXL database API	Standard CCM Super Users
Standard AXL API Users	Grants login rights to execute AXL APIs.	
Standard AXL Read Only API Access	Allows you to execute AXL read only APIs (list APIs, get APIs, executeSQLQuery API) by default.	
Standard Admin Rep Tool Admin	Allows you to view and configure Cisco Unified Communications Manager CDR Analysis and Reporting (CAR).	Standard CAR Admin Users, Standard CCM Super Users
Standard Audit Log Administration	Allows you to perform the following tasks for the audit logging feature : • View and configure audit logging in the Audit Log Configuration window in Cisco Unified Serviceability • View and configure trace in Cisco Unified Serviceability and collect traces for the audit log feature in the Real-Time Monitoring Tool • View and start/stop the Cisco Audit Event service in Cisco Unified Serviceability • View and update the associated alert in the RTMT	Standard Audit Users
Standard CCM Admin Users	Grants log-in rights to Cisco Unified Communications Manager Administration.	Standard CCM Admin Users, Standard CCM Gateway Administration, Standard CCM Phone Administration, Standard CCM Read Only, Standard CCM Server Monitoring, Standard CCM Super Users, Standard CCM Server Maintenance, Standard Packet Sniffer Users
Standard CCM End Users	Grant an end user log-in rights to the Cisco Unified Communications Self Care Portal	Standard CCM End Users

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)

Standard CCM Feature Management	Allows you to perform the following tasks in Cisco Unified Communications Manager Administration:
	• View, delete, and insert the following items by using the Bulk Administration Tool:
	  • Client matter codes and forced authorization codes
	  • Call pickup groups
	• View and configure the following items in Cisco Unified Communications Manager Administration:
	  • Client matter codes and forced authorization codes
	  • Call park
	  • Call pickup
	  • Meet-Me numbers/patterns
	  • Message Waiting
	  • Cisco Unified IP Phone Services
	  • Voice mail pilots, voice mail port wizard, voice mail ports, and voice mail profiles
		Standard CCM Server Maintenance

Standard CCM Gateway Management	Allows you to perform the following tasks in Cisco Unified Communications Manager Administration: • View and configure gateway templates in the Bulk Administration Tool • View and configure gatekeepers, gateways, and trunks	Standard CCM Gateway Administration

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)

Standard CCM Phone Management	Allows you to perform the following tasks in Cisco Unified Communications Manager Administration:
	• View and export phones in the Bulk Administration Tool
	• View and insert user device profiles in the Bulk Administration Tool
	• View and configure the following items in Cisco Unified Communications Manager Administration:
	  • BLF speed dials
	  • CTI route points
	  • Default device profiles or default profiles
	  • Directory numbers and line appearances
	  • Firmware load information
	  • Phone button templates or softkey templates
	  • Phones
	  • Reorder phone button information for a particular phone by clicking the Modify Button Items button in the Phone Configuration window
		Standard CCM Phone Administration

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard CCM Route Plan Management	Allows you to perform the following tasks in Cisco Unified Communications Manager Administration: • View and configure application dial rules • View and configure calling search spaces and partitions • View and configure dial rules, including dial rule patterns • View and configure hunt lists, hunt pilots, and line groups • View and configure route filters, route groups, route hunt list, route lists, route patterns, and route plan report • View and configure time period and time schedule • View and configure translation patterns	

Standard CCM Service Management	Allows you to perform the following tasks in Cisco Unified Communications Manager Administration:
	• View and configure the following items:
	  • Annunciators, conference bridges, and transcoders
	  • audio sources and MOH servers
	  • Media resource groups and media resource group lists
	  • Media termination point
	  • Cisco Unified Communications Manager Assistant wizard
	• View and configure the Delete Managers, Delete Managers/Assistants, and Insert Managers/Assistants windows in the Bulk Administration Tool
		Standard CCM Server Maintenance

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)

Standard CCM System Management	Allows you to perform the following tasks in Cisco Unified Communications Manager Administration:
	• View and configure the following items:
	  • Automate Alternate Routing (AAR) groups
	  • Cisco Unified Communications Managers (Cisco Unified CMs) and Cisco Unified Communications Manager groups
	  • Date and time groups
	  • Device defaults
	  • Device pools
	  • Enterprise parameters
	  • Enterprise phone configuration
	  • Locations
	  • Network Time Protocol (NTP) servers
	  • Plug-ins
	  • Security profiles for phones that run Skinny Call Control Protocol (SCCP) or Session Initiation Protocol (SIP); security profiles for SIP trunks
	  • Survivable Remote Site Telephony (SRST) references
	  • Servers
	• View and configure the Job Scheduler windows in the Bulk Administration Tool
		Standard CCM Server Maintenance

Standard CCM User Privilege Management	Allows you to view and configure application users in Cisco Unified Communications Manager Administration.	

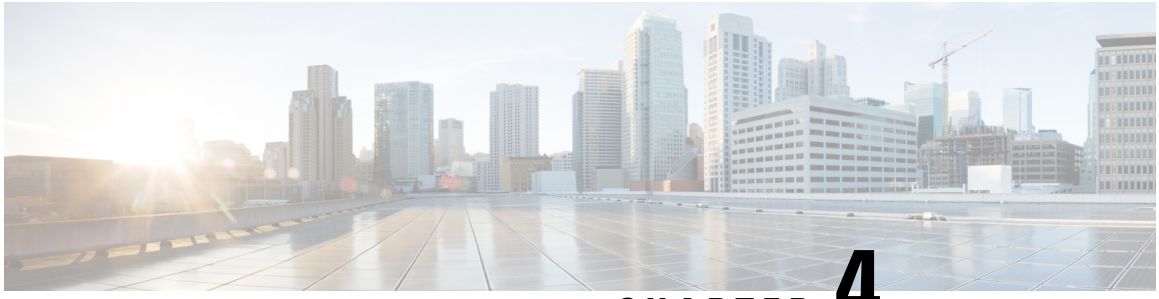
Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard CCMADMIN Administration	Allows you access to all aspects of the CCMAdmin system	
Standard CCMADMIN Administration	Allows you to view and configure all items in Cisco Unified Communications Manager Administration and the Bulk Administration Tool.	Standard CCM Super Users
Standard CCMADMIN Administration	Allows you to view and configure information in the Dialed Number Analyzer.	
Standard CCMADMIN Read Only	Allows read access to all CCMAdmin resources	
Standard CCMADMIN Read Only	Allows you to view configurations in Cisco Unified Communications Manager Administration and the Bulk Administration Tool.	Standard CCM Gateway Administration, Standard CCM Phone Administration, Standard CCM Read Only, Standard CCM Server Maintenance, Standard CCM Server Monitoring
Standard CCMADMIN Read Only	Allows you to analyze routing configurations in the Dialed Number Analyzer.	
Standard CCMUSER Administration	Allows access to the Cisco Unified Communications Self Care Portal.	Standard CCM End Users
Standard CTI Allow Call Monitoring	Allows CTI applications/devices to monitor calls	Standard CTI Allow Call Monitoring
Standard CTI Allow Call Park Monitoring	Allows CTI applications/devices to use call park. **Important** The maximum number of opened lines and park lines must not exceed 65,000. If the total exceeds 65,000, remove the Standard CTI Allow Call Park Monitoring role from the application user or reduce the number of park lines that are configured.	Standard CTI Allow Call Park Monitoring
Standard CTI Allow Call Recording	Allows CTI applications/devices to record calls	Standard CTI Allow Call Recording
Standard CTI Allow Calling Number Modification	Allows CTI applications to transform calling party numbers during a call	Standard CTI Allow Calling Number Modification

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard CTI Allow Control of All Devices	Allows control of all CTI-controllable devices	Standard CTI Allow Control of All Devices
Standard CTI Allow Control of Phones Supporting Connected Xfer and conf	Allows control of all CTI devices that supported connected transfer and conferencing	Standard CTI Allow Control of Phones supporting Connected Xfer and conf
Standard CTI Allow Control of Phones Supporting Rollover Mode	Allows control of all CTI devices that supported Rollover mode	Standard CTI Allow Control of Phones supporting Rollover Mode
Standard CTI Allow Reception of SRTP Key Material	Allows CTI applications to access and distribute SRTP key material	Standard CTI Allow Reception of SRTP Key Material
Standard CTI Enabled	Enables CTI application control	Standard CTI Enabled
Standard CTI Secure Connection	Enables a secure CTI connection to Cisco Unified Communications Manager	Standard CTI Secure Connection
Standard CUReporting	Allows application users to generate reports from various sources	
Standard CUReporting	Allows you to view, download, generate, and upload reports in Cisco Unified Reporting	Standard CCM Administration Users, Standard CCM Super Users
Standard EM Authentication Proxy Rights	Manages Cisco Extension Mobility (EM) authentication rights for applications; required for all application users that interact with Cisco Extension Mobility (for example, Cisco Unified Communications Manager Assistant and Cisco Web Dialer)	Standard CCM Super Users, Standard EM Authentication Proxy Rights
Standard Packet Sniffing	Allows you to access Cisco Unified Communications Manager Administration to enable packet sniffing (capturing).	Standard Packet Sniffer Users

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard RealtimeAndTraceCollection	Allows an you to access Cisco Unified Serviceability and the Real-Time Monitoring Tool view and use the following items: • Simple Object Access Protocol (SOAP) Serviceability AXL APIs • SOAP Call Record APIs • SOAP Diagnostic Portal (Analysis Manager) Database Service • configure trace for the audit log feature • configure Real-Time Monitoring Tool, including collecting traces	Standard RealtimeAndTraceCollection

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard SERVICEABILITY	Allows you to view and configure the following windows in Cisco Unified Serviceability or the Real-Time Monitoring Tool: • Alarm Configuration and Alarm Definitions (Cisco Unified Serviceability) • Audit Trace (marked as read/view only) • SNMP-related windows (Cisco Unified Serviceability) • Trace Configuration and Troubleshooting of Trace Configuration (Cisco Unified Serviceability) • Log Partition Monitoring • Alert Configuration (RTMT), Profile Configuration (RTMT), and Trace Collection (RTMT) Allows you to view and use the SOAP Serviceability AXL APIs, the SOAP Call Record APIs, and the SOAP Diagnostic Portal (Analysis Manager) Database Service. For the SOAP Call Record API, the RTMT Analysis Manager Call Record permission is controlled through this resource. For the SOAP Diagnostic Portal Database Service, the RTMT Analysis Manager Hosting Database access controlled thorough this resource.	Standard CCM Server Monitoring, Standard CCM Super Users
Standard SERVICEABILITY Administration	A serviceability administrator can access the Plugin window in Cisco Unified Communications Manager Administration and download plugins from this window.	
Standard SERVICEABILITY Administration	Allows you to administer all aspects of serviceability for the Dialed Number Analyzer.	

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard SERVICEABILITY Administration	Allows you to view and configure all windows in Cisco Unified Serviceability and Real-Time Monitoring Tool. (Audit Trace supports viewing only.) Allows you to view and use all SOAP Serviceability AXL APIs.	
Standard SERVICEABILITY Read Only	Allows you to view all serviceability-related data for components in the Dialed Number Analyzer.	Standard CCM Read Only
Standard SERVICEABILITY Read Only	Allows you to view configuration in Cisco Unified Serviceability and Real-Time Monitoring Tool. (excluding audit configuration window, which is represented by the Standard Audit Log Administration role) Allows an you to view all SOAP Serviceability AXL APIs, the SOAP Call Record APIs, and the SOAP Diagnostic Portal (Analysis Manager) Database Service.	
Standard System Service Management	Allows you to view, activate, start, and stop services in Cisco Unified Serviceability.	
Standard SSO Config Admin	Allows you to administer all aspects of SAML SSO configuration	
Standard Confidential Access Level Users	Allows you to access all the Confidential Access Level Pages	Standard Cisco Call Manager Administration
Standard CCMADMIN Administration	Allows you to administer all aspects of CCMAdmin system	Standard Cisco Unified CM IM and Presence Administration
Standard CCMADMIN Read Only	Allows read access to all CCMAdmin resources	Standard Cisco Unified CM IM and Presence Administration
Standard CUReporting	Allows application users to generate reports from various sources	Standard Cisco Unified CM IM and Presence Reporting



CHAPTER 4

Manage End Users

End User Overview

When administering an up and running system, you may need to make updates to the list of configured end users in your system. This includes:

- Setting up a new user
- Setting up a phone for a new end user
- Changing passwords or PINs for an end user
- Enable end users for IM and Presence Service

The **End User Configuration** window in Cisco Unified CM Administration allows you to add, search, display, and maintain information about Unified CM end users. You can also use the **Quick User/Phone Add** window to quickly configure a new end user and configure a new phone for that end user.

End User Management Tasks

Procedure

	Command or Action	Purpose
Step 1	Configure User Templates, on page 36	If you have not configured your system with user profiles or feature group templates that includes universal line and device templates, perform these tasks to set them up. You can apply these templates to any new end users in order to quickly configure new users and phones.
Step 2	Add a new end user using one of the following methods	If you have configured and if your system is synchronized with a company LDAP directory,

	Command or Action	Purpose
	• Import an End User from LDAP, on page 40 • Add an End User Manually, on page 41	you can import the new end user directly from LDAP. Else, you can add and configure the end user manually.
Step 3	Assign a phone to a new or existing end user by performing either of the following tasks: • Add New Phone for End User , on page 42 • Move an Existing Phone to a End User, on page 42	You can use the 'Add New Phone' procedure to configure a new phone for the end user using settings from a universal device template. You can also use the 'Move' procedure to assign an existing phone that has already been configured.
Step 4	Change the End User PIN, on page 43	(Optional) To change the pin for an end user in Cisco Unified Communications Manager Administration.
Step 5	Change the End User Password, on page 43	(Optional) To change the password for an end user in Cisco Unified Communications Manager Administration.
Step 6	Create a Cisco Unity Connection Voice Mailbox, on page 44	(Optional) To create individual Cisco Unity Connection voice mailboxes in Cisco Unified Communications Manager Administration.

Configure User Templates

Perform the following tasks to set up a user profile and feature group template. When you add a new end user, you can use the line and device settings to quickly configure the end user and any phones for the end user.

Procedure

	Command or Action	Purpose
Step 1	Configure Universal Line Template, on page 37	Configure universal line templates with common settings that are typically applied to a directory number.
Step 2	Configure Universal Device Template, on page 37	Configure universal device templates with common settings that are typically applied to a phone.
Step 3	Configure User Profiles, on page 38	Assign universal line and universal device templates to a user profile. If you have the self-provisioning feature configured, you can enable self-provisioning for the users who use this profile.
Step 4	Configure Feature Group Template, on page 39	Assign the user profile to a feature group template. For LDAP Synchronized Users, the

	Command or Action	Purpose
		feature group template associates the user profile settings to the end user.

Configure 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**.

What to do next

Configure Universal Device Template, on page 37

Configure 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.

Before you begin

Configure Universal Line Template, on page 37

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**.

What to do next

Configure User Profiles, on page 38

Configure User Profiles

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.

Before you begin

Configure Universal Device Template, on page 37

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **User Settings** > **User Profile**.

Step 2 Click **Add New**.

Step 3 Enter a **Name** and **Description** for the user profile.

Step 4 Assign a **Universal Device Template** to apply to users' **Desk Phones**, **Mobile and Desktop Devices**, and **Remote Destination/Device Profiles**.

Step 5 Assign a **Universal Line Template** to apply to the phone lines for users in this user profile.

Step 6 If you want the users in this user profile to be able to use the self-provisioning feature to provision their own phones, do the following:

a) Check the **Allow End User to Provision their own phones** check box.

b) In the **Limit Provisioning once End User has this many phones** field, enter a maximum number of phones the user is allowed to provision. The maximum is 20.

Step 7 If you want Cisco Jabber users 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 **Jabber 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 **Jabber Desktop Client Policy**, and **Jabber Mobile Client Policy** drop-down list, choose one of the following options:

- No Service—This policy disables access to all Cisco Jabber services.
- IM & Presence only—This policy enables only instant messaging and presence capabilities.
- IM & Presence, Voice and Video calls—This policy enables instant messaging, presence, voicemail, and conferencing capabilities for all users with audio or video devices. This is the default option.

Note Jabber desktop client includes Cisco Jabber for Windows users and Cisco Jabber for Mac users. Jabber mobile client includes Cisco Jabber for iPad and iPhone users and Cisco Jabber for Android users.

Step 9 Click **Save**.

What to do next

Configure Feature Group Template, on page 39

Configure 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

Add a new end user. If your system is integrated with a company LDAP directory, you can import the user directly from an LDAP directory. Otherwise, create the end user manually.

- Import an End User from LDAP, on page 40
- Add an End User Manually, on page 41

Import an End User from LDAP

Perform the following procedure to manually import a new end user from a company LDAP directory. If your LDAP synchronization configuration includes a feature group template with a user profile that includes universal line and device templates and a DN pool, the import process automatically configures the end user and primary extension.

Note You cannot add new configurations (for example, adding a feature group template) into an LDAP directory sync after the initial sync has occurred. If you want to edit an existing LDAP sync, you must either use Bulk Administration, or configure a new LDAP sync.

Before you begin

Before you begin this procedure make sure that you have already synchronized Cisco Unified Communications Manager with a company LDAP directory. The LDAP synchronization must include a feature group template with universal line and device templates.

Procedure

Step 1 In Cisco Unified CM Administration, choose **System** > **LDAP** > **LDAP Directory**.

Step 2 Click **Find** and select the LDAP directory to which the user is added.

Step 3 Click **Perform Full Sync**.
Cisco Unified Communications Manager synchronizes with the external LDAP directory. Any new end users in the LDAP directory are imported into the Cisco Unified Communications Manager database.

What to do next

If the user is enabled for self-provisioning, the end user can use the Self-Provisioning Interactive Voice Response (IVR) to provision a new phone. Otherwise, perform one of the following tasks to assign a phone to the end user:

• Add New Phone for End User , on page 42
• Move an Existing Phone to a End User, on page 42

Add an End User Manually

Perform the following procedure to add new end user and configure them with an access control group and a primary line extension.

Note Make sure that you have already set up an access control groups that has the role permissions to which you want to assign your user. For details, see the "Manage User Access" chapter.

Before you begin

Verify that you have a user profile configured that includes a universal line template. If you need to configure a new extension, Cisco Unified Communications Manager uses the settings from the universal line template to configure the primary extension.

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **Quick User/Phone Add**.

Step 2 Enter the **User ID** and **Last Name**.

Step 3 From the **Feature Group Template** drop-down list, select a feature group template.

Step 4 Click **Save**.

Step 5 From the **User Profile** drop-down list, verify that the selected user profile includes a universal line template.

Step 6 From the **Access Control Group Membership** section, click the + icon.

Step 7 From the **User is a member of** drop-down list, select an access control group.

Step 8 Under **Primary Extension**, click the + icon.

Step 9 From the **Extension** drop-down list, select a DN that displays as **(available)**.

Step 10 If all line extensions display as **(used)**, perform the following steps:

a) Click the **New...** button.
The **Add New Extension** popup displays.

b) In the **Directory Number** field, enter a new line extension.

c) From the **Line Template** drop-down list, select a universal line template.

d) Click **OK**.
Cisco Unified Communications Manager configures the directory number with the settings from the universal line template.

Step 11 (Optional) Complete any additional fields in the **Quick User/Phone Add Configuration** window.

Step 12 Click **Save**.

What to do next

Perform one of the following procedures to assign a phone to this end user:

- Add New Phone for End User , on page 42
- Move an Existing Phone to a End User, on page 42

Add New Phone for End User

Perform the following procedure to add a new phone for a new or existing end user. Make sure that the user profile for the end user includes a universal device template. Cisco Unified Communications Manager uses the universal device template settings to configure the phone.

Before you begin

Perform one of the following procedures to add an end user:

- Add an End User Manually, on page 41
- Import an End User from LDAP, on page 40

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **Quick/User Phone Add**.

Step 2 Click **Find** and select the end user for whom you want to add a new phone.

Step 3 Click the **Manage Devices**.
The Manage Devices window appears.

Step 4 Click **Add New Phone**.
The Add Phone to User popup displays.

Step 5 From the **Product Type** drop-down list, select the phone model.

Step 6 From the **Device Protocol** drop-down list select SIP or SCCP as the protocol.

Step 7 In the **Device Name** text box, enter the device MAC address.

Step 8 From the **Universal Device Template** drop-down list, select a universal device template.

Step 9 If the phone supports expansion modules, enter the number of expansion modules that you want to deploy.

Step 10 If you want to use Extension Mobility to access the phone, check the **In Extension Mobility** check box.

Step 11 Click **Add Phone**.
The Add New Phone popup closes. Cisco Unified Communications Manager adds the phone to the user and uses the universal device template to configure the phone.

Step 12 If you want to make additional edits to the phone configuration, click the corresponding Pencil icon to open the phone in the **Phone Configuration** window.

Move an Existing Phone to a End User

Perform this procedure to move an existing phone to a new or existing end user.

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **Quick/User Phone Add**.

Step 2 Click **Find** and select the user to whom you want to move an existing phone.

Step 3 Click the **Manage Devices** button.

Step 4 Click the **Find a Phone to Move To This User** button.

Step 5 Select the phone that you want to move to this user.

Step 6 Click **Move Selected**.

Change the End User PIN

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **User Management** > **End User**.
The **Find and List Users** window appears.

Step 2 To select an existing user, specify the appropriate filters in the **Find User Where** field, click **Find** to retrieve a list of users, and then select the user from the list.
The **End User Configuration** window is displayed.

Step 3 In the **PIN** field, double-click the existing PIN, which is encrypted, and enter the new PIN. You must enter at least the minimum number of characters that are specified in the assigned credential policy (1-127 characters).

Step 4 In the **Confirm PIN** field, double-click the existing, encrypted PIN and enter the new PIN again.

Step 5 Click **Save**.

Note You can login to Extension Mobility, Conference Now, Mobile Connect, and Cisco Unity Connection voicemail with the same end user PIN, if **End User Pin synchronization** checkbox is enabled in the **Application Server Configuration** window for Cisco Unity Connection. End users can use the same PIN to log in to Extension Mobility and to access their voicemail.

Change the End User Password

You cannot change an end user password when LDAP authentication is enabled.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **User Management** > **End User**.
The **Find and List Users** window appears.

Step 2 To select an existing user, specify the appropriate filters in the **Find User Where** field, click **Find** to retrieve a list of users, and then select the user from the list.
The **End User Configuration** window is displayed.

Step 3 In the **Password** field, double-click the existing password, which is encrypted, and enter the new password. You must enter at least the minimum number of characters that are specified in the assigned credential policy (1-127 characters).

Step 4 In the **Confirm Password** field, double-click the existing, encrypted password and enter the new password again.

Step 5 Click **Save**.

Create a Cisco Unity Connection Voice Mailbox

Before you begin

- You must configure Cisco Unified Communications Manager for voice messaging. For more information about configuring Cisco Unified Communications Manager to use Cisco Unity Connection, see the *System 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

- You must associate a device and a Primary Extension Number with the end user.
- You can use the import feature that is available in Cisco Unity Connection instead of performing the procedure that is described in this section. For information about how to use the import feature, see the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **User Management** > **End User**.
The **Find and List Users** window appears.

Step 2 To select an existing user, specify the appropriate filters in the **Find User Where** field, click **Find** to retrieve a list of users, and then select the user from the list.
The **End User Configuration** window is displayed.

Step 3 Verify that a primary extension number is associated with this user.

Note You must define a primary extension; otherwise, the Create Cisco Unity User link does not appear in the **Related Links** drop-down list.

Step 4 From the **Related Links** drop-down list, choose the Create Cisco Unity User link, and then click **Go**.

The Add Cisco Unity User dialog box appears.

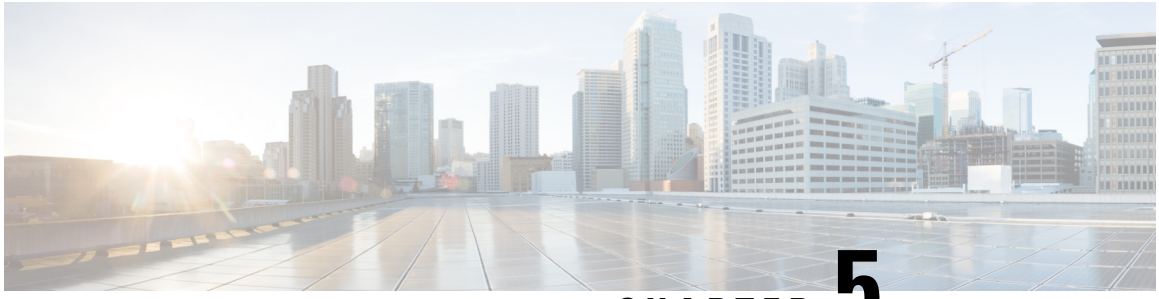
Step 5 From the **Application Server** drop-down list, choose the Cisco Unity Connection server on which you want to create a Cisco Unity Connection user, and then click **Next**.

Step 6 From the **Subscriber Template** drop-down list, choose the subscriber template that you want to use.

Step 7 Click **Save**.

The mailbox is created. The link in the **Related Links** drop-down list changes to Edit Cisco Unity User in the **End User Configuration** window. In Cisco Unity Connection Administration, you can now view the user that you created.

Note After you integrate the Cisco Unity Connection user with the Cisco Unified Communications Manager end user, you cannot edit fields in Cisco Unity Connection Administration such as Alias (User ID in Cisco Unified CM Administration), First Name, Last Name, and Extension (Primary Extension in Cisco Unified CM Administration). You can only update these fields in Cisco Unified CM Administration.



CHAPTER 5

Manage Application Users

Application Users Overview

The **Application User Configuration** window in Cisco Unified CM Administration allows the administrator to add, search, display, and maintain information about Cisco Unified Communications Manager application users.

Cisco Unified CM Administration includes the following application users by default:

- CCMAdministrator
- CCMSysUser
- CCMQRTSecureSysUser
- CCMQRTSysUser
- IPMASecureSysUser
- IPMASysUser
- WDSecureSysUser
- WDSysUser
- TabSyncSysUser
- CUCService

Note Administrator users in the Standard CCM Super Users group can access Cisco Unified Communications Manager Administration, Cisco Unified Serviceability, and Cisco Unified Reporting with a single sign-on to one of the applications.

Application Users Task Flow

Procedure

	Command or Action	Purpose
Step 1	Add New Application User, on page 48	Add a new application user.
Step 2	Associate Devices with Application Users, on page 49	Assign devices to associate with an application user.
Step 3	Add Administrator User to Cisco Unity or Cisco Unity Connection, on page 49	Add a user as an administrator user to Cisco Unity or Cisco Unity Connection. You configure the application user in Cisco Unified CM Administration; then, configure any additional settings for the user in Cisco Unity or Cisco Unity Connection Administration.
Step 4	Change Application User Password, on page 50	Change an application user password.
Step 5	Manage Application User Password Credential Information, on page 50	Change or view credential information, such as the associated authentication rules, the associated credential policy, or the time of last password change for an application user.

Add New Application User

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **Application User** .

Step 2 Click **Add New**.

Step 3 Configure the fields in the **Application User Configuration** window. See the online help for information about the fields and their configuration options.

Step 4 Click **Save**.

What to do next

Associate Devices with Application Users, on page 49

Associate Devices with Application Users

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **Application User**.
The **Find and List Users** window appears.

Step 2 To select an existing user, specify the appropriate filters in the **Find User Where** field, select **Find** to retrieve a list of users, and then select the user from the list.

Step 3 In the **Available Devices** list, choose a device that you want to associate with the application user and click the **Down arrow** below the list. The selected device moves to the **Controlled Devices** list.

Note To limit the list of available devices, click the **Find more Phones** or **Find more Route Points** button.

Step 4 If you click the **Find more Phones** button, the **Find and List Phones** window displays. Perform a search to find the phones to associate with this application user.

Repeat the preceding steps for each device that you want to assign to the application user.

Step 5 If you click the **Find more Route Points** button, the **Find and List CTI Route Points** window displays. Perform a search to find the CTI route points to associate with this application user.

Repeat the preceding steps for each device that you want to assign to the application user.

Step 6 Click **Save**.

Add Administrator User to Cisco Unity or Cisco Unity Connection

If you are integrating Cisco Unified Communications Manager with Cisco Unity Connection 7.x or later, you can use the import feature that is available in Cisco Unity Connection 7.x or later instead of performing the procedure that is described in the this section. For information on how to use the import feature, see the *User Moves, Adds, and Changes* Guide for Cisco Unity Connection 7.x or later at

http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html.

When the Cisco Unity or Cisco Unity Connection user is integrated with the Cisco Unified CM Application User, you cannot edit the fields. You can only update these fields in Cisco Unified Communications Manager Administration.

Cisco Unity and Cisco Unity Connection monitor the synchronization of data from Cisco Unified Communications Manager. You can configure the sync time in Cisco Unity Administration or Cisco Unity Connection Administration on the tools menu.

Before you begin

Ensure that you have defined an appropriate template for the user that you plan to push to Cisco Unity or Cisco Unity Connection

The **Create Cisco Unity User** link displays only if you install and configure the appropriate Cisco Unity or Cisco Unity Connection software. See the applicable *Cisco Unified Communications Manager Integration*

Guide for Cisco Unity or the applicable *Cisco Unified Communications Manager SCCP Integration Guide* for Cisco Unity Connection at

http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-installation-and-configuration-guides-list.html.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **Application User**.

Step 2 To select an existing user, specify the appropriate filters in the **Find User Where** field, select **Find** to retrieve a list of users, and then select the user from the list.

Step 3 From the **Related Links** drop-down list, choose the **Create Cisco Unity Application User** link and click **Go**.
The Add **Cisco Unity User** dialog displays.

Step 4 From the **Application Server** drop-down list, choose the Cisco Unity or Cisco Unity Connection server on which you want to create a Cisco Unity or Cisco Unity Connection user and click **Next**.

Step 5 From the **Application User Template** drop-down list, choose the template that you want to use.

Step 6 Click **Save**.
The administrator account gets created in Cisco Unity or Cisco Unity Connection. The link in Related Links changes to **Edit Cisco Unity User** in the **Application User Configuration** window. You can now view the user that you created in Cisco Unity Administration or Cisco Unity Connection Administration.

Change Application User Password

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **Application User**.
The **Find and List Users** window appears.

Step 2 To select an existing user, specify the appropriate filters in the **Find User Where** field, select **Find** to retrieve a list of users, and then select the user from the list.
The **Application User Configuration** window displays information about the chosen application user.

Step 3 In the **Password** field, double click the existing, encrypted password and enter the new password.

Step 4 In the **Confirm Password** field, double click the existing, encrypted password and enter the new password again.

Step 5 Click **Save**.

Manage Application User Password Credential Information

Perform the following procedure to manage credential information for an application user password. This allows you to perform administrative duties such as locking a password, applying a credential policy to a password, or viewing information such as the time of the last failed login attempt.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **Application User**.
The **Find and List Users** window appears.

Step 2 To select an existing user, specify the appropriate filters in the **Find User Where** field, select **Find** to retrieve a list of users, and then select the user from the list.
The **Application User Configuration** window displays information about the chosen application user.

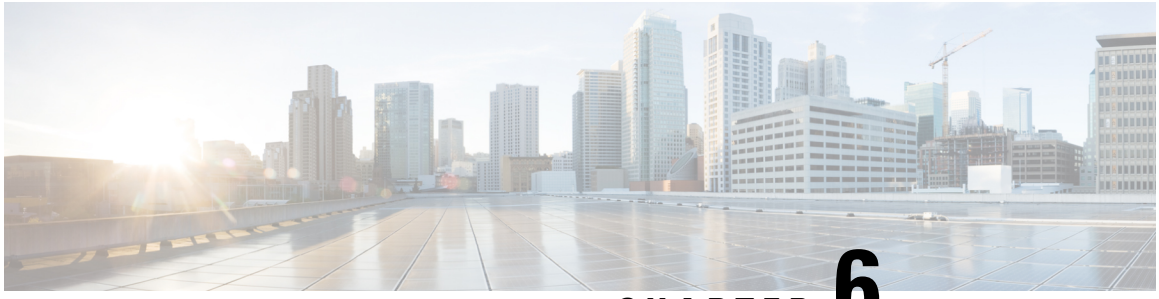
Step 3 To change or view password information, click the **Edit Credential** button next to the **Password** field.
The user **Credential Configuration** is displayed.

Step 4 Configure the fields on the **Credential Configuration** window. See the online help for more information about the fields and their configuration options.

Step 5 If you have changed any settings, click **Save**.

PART III

Manage Devices



CHAPTER 6

Manage Phones

Phone Management Overview

This chapter describes how to manage the phones in your network. The topics describe tasks such as adding new phones, moving existing phones to another user, locking phones and resetting phones.

The Cisco IP Phone Administration Guide for your phone model contains configuration information specific to the phone model.

Phone Management Tasks

Procedure

	Command or Action	Purpose
Step 1	Add a New Phone from Template with an End User, on page 56	Add a new phone for an end user and assign a universal device template.
Step 2	Move an Existing Phone, on page 57	Move a configured phone to a different end user.
Step 3	Find an Actively Logged-In Device , on page 58	Search for a specific device or list all devices for which users are actively logged in.
Step 4	Find a Remotely Logged-In Device , on page 58	Search for a specific device or list all devices for which users are logged in remotely.
Step 5	Remotely Lock a Phone, on page 59	Some phones can be locked remotely. When you remotely lock a phone, the phone cannot be used until you unlock it.
Step 6	Reset a Phone to Factory Defaults , on page 60	Reset a phone to its factory settings.

	Command or Action	Purpose
Step 7	Phone Lock/Wipe Report , on page 60	Search for devices that have been remotely locked and/or remotely reset to factory default settings.
Step 8	View LSC Status and Generate a CAPF Report for a Phone, on page 61	Search for LSC expiry status on phones, and also generate a CAPF report.

Add Phone Manually

Perform the following procedure to add a new phone manually with a user.

Procedure

Step 1 From the Cisco Unified CM Administration, choose **Device** > **Phone** > **Find and List Phones**.

Step 2 From **Find and List Phones** page, click **Add New** to manually add a phone.

Add a New Phone page is displayed.

From **Add a New Phone** page, if you click "click here to add a new phone using a Universal Device Template" hyper link, the page is redirected to the **Add a New Phone** page to add a phone from the template with or without adding a user.

Step 3 From the **Phone Type** drop-down list, select the phone model.

Step 4 Click **Next**.
The **Phone Configuration** page is displayed.

Step 5 On **Phone Configuration** page, enter the values in the required fields. See online help for more information on fields.

For additional information about the fields in the Product Specific Configuration area, see the *Cisco IP Phone Administration Guide* for your phone model.

Step 6 Click **Save** to save the phone configuration.

What to do next

Move an Existing Phone to a End User, on page 42

Add a New Phone from Template with an End User

Perform the following procedure to add a new phone for an end user.

Before you begin

The end user for whom you are adding the phone has a user profile set up that includes a universal device template. Cisco Unified Communications Manager uses the settings from the universal device template to configure the phone.

- End User Management Tasks, on page 35

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **Quick/User Phone Add**.

Step 2 Click **Find** and select the end user for whom you want to add a new phone.

Step 3 Click the **Manage Devices**.
The Manage Devices window appears.

Step 4 Click **Add New Phone**.
The Add Phone to User popup displays.

Step 5 From the **Product Type** drop-down list, select the phone model.

Step 6 From the **Device Protocol** drop-down list select SIP or SCCP as the protocol.

Step 7 In the **Device Name** text box, enter the device MAC address.

Step 8 From the **Universal Device Template** drop-down list, select a universal device template.

Step 9 If the phone supports expansion modules, enter the number of expansion modules that you want to deploy.

Step 10 If you want to use Extension Mobility to access the phone, check the **In Extension Mobility** check box.

Step 11 Click **Add Phone**.
The Add New Phone popup closes. Cisco Unified Communications Manager adds the phone to the user and uses the universal device template to configure the phone.

Step 12 If you want to make additional edits to the phone configuration, click the corresponding Pencil icon to open the phone in the **Phone Configuration** window.

Move an Existing Phone

Perform the following procedure to move a configured phone to an end user.

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **Quick/User Phone Add**.

Step 2 Click **Find** and select the user to whom you want to move an existing phone.

Step 3 Click the **Manage Devices** button.

Step 4 Click the **Find a Phone to Move To This User** button.

Step 5 Select the phone that you want to move to this user.

Step 6 Click **Move Selected**.

Find an Actively Logged-In Device

The Cisco Extension Mobility and Cisco Extension Mobility Cross Cluster features keep a record of the devices to which users are actively logged in. For the Cisco Extension Mobility feature, the actively logged-in device report tracks the local phones that are actively logged in by local users; for the Cisco Extension Mobility Cross Cluster feature, the actively logged-in device report tracks the local phones that are actively logged in by remote users.

Unified Communications Manager provides a specific search window for searching for devices to which users are logged in. Follow these steps to search for a specific device or to list all devices for which users are actively logged in.

Procedure

Step 1 Choose **Device** > **Phone**.

Step 2 Select the **Actively Logged In Device Report** from the **Related Links** drop-down list in the upper right corner and click **Go**.

Step 3 To find all actively logged-in device records in the database, ensure the dialog box is empty and proceed to step 4.

To filter or search records:

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

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

Step 4 Click **Find**.

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

Step 5 From the list of records that display, click the link for the record that you want to view.

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

The window displays the item that you choose.

Find a Remotely Logged-In Device

The Cisco Extension Mobility Cross Cluster feature keeps a record of the devices to which users are logged in remotely. The Remotely Logged In Device report tracks the phones that other clusters own but that are actively logged in by local users who are using the EMCC feature.

Unified Communications Manager provides a specific search window for searching for devices to which users are logged in remotely. Follow these steps to search for a specific device or to list all devices for which users are logged in remotely.

Procedure

Step 1 Choose **Device** > **Phone**.

Step 2 Select **Remotely Logged In Device** from the **Related Links** drop-down list in the upper right corner and click **Go**.

Step 3 To find all remotely logged-in device records in the database, ensure the dialog box is empty and proceed to step 4.

To filter or search records:

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

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

Step 4 Click **Find**.

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

Step 5 From the list of records that display, click the link for the record that you want to view.

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

The window displays the item that you choose.

Remotely Lock a Phone

Some phones can be locked remotely. When you remotely lock a phone, the phone cannot be used until you unlock it.

If a phone supports the Remote Lock feature, a **Lock** button appears in the top right hand corner.

Procedure

Step 1 Choose **Device** > **Phone**.

Step 2 From the **Find and List Phones** window, enter search criteria and click **Find** to locate a specific phone.

A list of phones that match the search criteria displays.

Step 3 Choose the phone for which you want to perform a remote lock.

Step 4 On the **Phone Configuration** window, click **Lock**.

If the phone is not registered, a popup window displays to inform you that the phone will be locked the next time it is registered. Click **Lock**.

A **Device Lock/Wipe Status** section appears, with information about the most recent request, whether it is pending, and the most recent acknowledgement.

Reset a Phone to Factory Defaults

Some phones support a remote wipe feature. When you remotely wipe a phone, the operation resets the phone to its factory settings. Everything previously stored on the phone is wiped out.

If a phone supports the remote wipe feature, a **Wipe** button appears in the top right hand corner.

Caution This operation cannot be undone. You should only perform this operation when you are sure you want to reset the phone to its factory settings.

Procedure

Step 1 Choose **Device** > **Phone**.

Step 2 In the **Find and List Phones** window, enter search criteria and click **Find** to locate a specific phone.

A list of phones that match the search criteria displays.

Step 3 Choose the phone for which you want to perform a remote wipe.

Step 4 In the **Phone Configuration** window, click **Wipe**.

If the phone is not registered, a popup window displays to inform you that the phone will be wiped the next time it is registered. Click **Wipe**.

A **Device Lock/Wipe Status** section appears, with information about the most recent request, whether it is pending, and the most recent acknowledgment.

Phone Lock/Wipe Report

Unified Communications Manager provides a specific search window for searching for devices which have been remotely locked and/or remotely wiped. Follow these steps to search for a specific device or to list all devices which have been remotely locked and/or remotely wiped.

Procedure

Step 1 Choose **Device** > **Phone**.

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

Step 2 Select the **Phone Lock/Wipe Report** from the **Related Links** drop-down list in the upper right corner of the window and click **Go**.

Step 3 To find all remotely locked or remotely wiped device records in the database, ensure that the text box is empty; go to Step 4.

To filter or search records for a specific device:

a) From the first drop-down list, select the device operation type(s) to search.
b) From the second drop-down list, select a search parameter.
c) From the third drop-down list, select a search pattern.
d) Specify the appropriate search text, if applicable.

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

Step 4 Click **Find**.

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

Step 5 From the list of records that display, click the link for the record that you want to view.

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

The window displays the item that you choose.

View LSC Status and Generate a CAPF Report for a Phone

Use this procedure to monitor Locally Significant Certificate (LSC) expiry information from within the Cisco Unified Communications Manager interface. The following search filters display the LSC information:

- LSC Expires—Displays the LSC expiry date on the phone.
- LSC Issued By—Displays the name of the issuer which can either be CAPF or third party.
- LSC Issuer Expires By—Displays the expiry date of the issuer.

Note The status of **LSC Expires** and **LSC Issuer Expires by** fields are set to “NA” when there is no LSC issued on a new device.

The status of **LSC Expires** and **LSC Issuer Expires by** fields are set to “ Unknown” when the LSC is issued to a device before the upgrade to Cisco Unified Communications Manager 11.5(1).

Procedure

Step 1 Choose **Device** > **Phone**.

Step 2 From the first **Find Phone where** drop-down list, choose one of the following criteria:

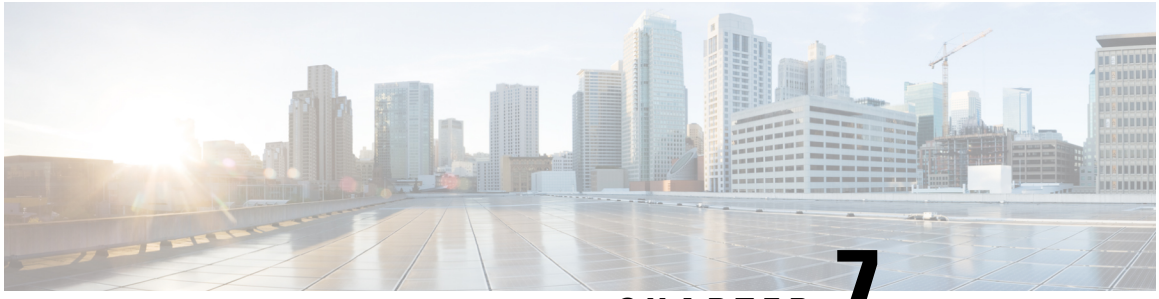
- LSC Expires
- LSC Issued By
- LSC Issuer Expires By

From the second **Find Phone where** drop-down list, choose one of the following criteria:

- is before
- is exactly
- is after
- begins with
- contains
- ends with
- is exactly
- is empty
- is not empty

Step 3 Click **Find**.
A list of discovered phones displays.

Step 4 From the **Related Links** drop-down list, choose the **CAPF Report in File** and click **Go**.
The report gets downloaded.



CHAPTER 7

Manage Device Firmware

Device Firmware Updates Overview

Device loads are the software and firmware for devices such as IP phones, telepresence systems, and others that are provisioned by and register to Cisco Unified Communications Manager. During installation or upgrade, Cisco Unified Communications Manager includes the latest loads available based on when the version of Cisco Unified Communications Manager was released. Cisco regularly releases updated firmware to introduce new features and software fixes and you may wish to update your phones to a newer load without waiting for a Cisco Unified Communications Manager upgrade that includes that load.

Before endpoints can upgrade to a new version of software, the files required by the new load must be made available for download at a location the endpoints have access to. The most common location is the Cisco UCM node with the Cisco TFTP service activated, called the “TFTP server”. Some phones also support using an alternate download location, called a “load server”.

If you want to get a list, view, or download files that already in the tftp directory on any server you can use the CLI command file list tftp to see the files in the TFTP directory, file view tftp to view a file, and file get tftp to get a copy of a file in the TFTP directory. For more information, see the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*. You may also use a web browser to download any TFTP file by going to the URL “http://<tftp_server>:6970/<filename>”.

Tip You can apply a new load to a single device before configuring it as a systemwide default. This method is useful for testing purposes. Remember, however, that all other devices of that type use the old load until you update the systemwide defaults with the new load.

Install a Device Pack or Individual Firmware

Install a device package to introduce new phone types and upgrade the firmware for multiple phone models.

- Individual firmware for existing devices can be installed or upgraded with the following options: Cisco Options Package (COP) files—The COP file contains the firmware files and the database updates so when installed on Publisher, it updates the default firmware apart from installing the firmware files.
- Firmware files only—It is supplied in a zip file, contains individual device firmware files that should be manually extracted and uploaded to the appropriate directory on the TFTP servers.

Note Refer to the README file for installation instructions that are specific to the COP or Firmware files package.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Software Upgrades** > **Install/Upgrade**.

Step 2 Fill in the applicable values in the Software Location section and click **Next**.

Step 3 In the **Available Software** drop-down list, select the device package file and click **Next**.

Step 4 Verify that the MD5 value is correct, and then click **Next**.

Step 5 In the warning box, verify that you selected the correct firmware, and then click **Install**.

Step 6 Check that you received a success message.

Note Skip to Step 8 if you are rebooting the cluster.

Step 7 Restart the **Cisco TFTP** service on all nodes where the service is running.

Step 8 Reset the affected devices to upgrade the devices to the new load.

Step 9 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Device Defaults** and manually change the name of the load file (for specific devices) to the new load.

Step 10 Click **Save**, and then reset the devices.

Step 11 Restart the **Cisco Tomcat** service on all cluster nodes.

Step 12 Do one of the following:

- If you are running 11.5(1)SU4 or lower, 12.0(1) or 12.0(1)SU1, reboot the cluster.
- If you are running an 11.5(x) release at 11.5(1)SU5 or higher, or any release higher at 12.0(1)SU2 or higher, reboot the **Cisco CallManager** service on the publisher node. However, if you are running the **Cisco CallManager** service on subscriber nodes only, you can skip this task.

Potential Issues with Firmware Installs

Here are some potential issues that you may run across after installing a device pack:

Issue	Cause/Resolution
New devices won't register	This could occur due from a device type mismatch. This can be caused by: • The device was added in the Phone Configuration window using the wrong device type. For example, Cisco DX80 was selected as the phone type instead of Cisco TelePresence DX80. Reconfigure the device with the correct device type. • The **Cisco CallManager** service doesn't know about the new device type. In this case, restart the **Cisco CallManager** service on the publisher node.
Endpoints aren't upgrading to the new firmware	**Possible reasons:** • The device pack wasn't installed on the TFTP server. As a result, the firmware isn't available for download by the phones. • The **Cisco TFTP** service wasn't restarted after the install so the service doesn't know about the new files. Make sure to install the device pack on the TFTP server.
Phone Configuration window in Cisco Unified CM Administration shows broken links where the icon image should be for a new device type	Restart the **Cisco Tomcat** service on all nodes from the CLI.

Remove Unused Firmware from the System

The **Device Load Management** window allows you to delete unused firmware (device loads) and associated files from the system to increase disk space. For example, you can delete unused loads before an upgrade to prevent upgrade failures due to insufficient disk space. Some firmware files may have dependent files that are not listed in the **Device Load Management** window. When you delete a firmware, the dependent files are also deleted. However, the dependent files are not deleted if they are associated with additional firmware.

Note You must delete unused firmware separately for each server in the cluster.

Before you begin

Caution Before you delete unused firmware, ensure that you are deleting the right loads. The deleted loads cannot be restored without performing a DRS restore of the entire cluster. We recommend that you take a backup before deleting the firmware.

Ensure that you do not delete files for devices that use multiple loads of files. For example, certain CE endpoints use multiple loads. However, only one load is referenced as **In Use** in the **Device Load Management** window.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Software Upgrades** > **Device Load Management**.

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

Step 3 Select the device load that you want to delete. You can select multiple loads if required.

Step 4 Click **Delete Selected Loads**.

Step 5 Click **OK**.

Set up Default Firmware for a Phone Model

Use this procedure to set the default firmware load for a specific phone model. When a new phone registers, Cisco Unified Communications Manager tries to send the default firmware to the phone, unless the phone configuration specifies has an overriding firmware load specified in the **Phone Configuration** window.

Note For an individual phone, the setting of the **Phone Load Name** field in the **Phone Configuration** window overrides the default firmware load for that particular phone.

Before you begin

Make sure that the firmware is loaded onto the TFTP server.

Procedure

Step 1 In Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Device Defaults**.
The **Device Defaults Configuration** window appears displaying the default firmware loads for the various phone models that Cisco Unified Communications Manager supports. The firmware appears in the **Load Information** column.

Step 2 Under **Device Type**, locate the phone models for which you want to assign the default firmware.

Step 3 In the accompanying **Load Information** field, enter the firmware load.

Step 4 (Optional) Enter the default **Device Pool** and default **Phone Template** for that phone model.

Step 5 Click **Save**.

Set the Firmware Load for a Phone

Use this procedure to assign a firmware load for a specific phone. You may want to do this if you want to use a different firmware load than the default that is specified in the **Device Defaults Configuration** window.

Note If you wish to assign a version for many phones you can use the Bulk Administration Tool to configure the **Phone Load Name** field using a CSV file or query. For details, see the *Bulk Administration Guide for Cisco Unified Communications Manager*.

Procedure

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

Step 2 Click **Find** and select an individual phone.

Step 3 In the **Phone Load Name** field, enter the name of the firmware. For this phone, the firmware load specified here overrides the default firmware load that is specified in the **Device Defaults Configuration** window.

Step 4 Complete any remaining fields in the **Phone Configuration** window. For help with the fields and their settings, see the online help.

Step 5 Click **Save**.

Step 6 Click **Apply Config** to push the changed fields to the phone.

Using a Load Server

If you want phones to download firmware updates from a server that is not the TFTP server you may configure a "load server" on the phone's **Phone Configuration** page. A load server may be another Cisco Unified Communications Manager or a third-party server. A third-party server must be capable of providing any files the phone requests through HTTP on TCP Port 6970 (preferred) or the UDP-based TFTP protocol. Some phone models such as the DX family Cisco TelePresence devices only support HTTP for firmware updates.

Note If you wish to assign a load server for many phones you can use the Bulk Administration Tool to configure the **Load Server** field using a CSV file or query. For details, see the *Bulk Administration Guide for Cisco Unified Communications Manager*.

Procedure

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

Step 2 Click **Find** and select an individual phone.

Step 3 In the **Load Server** field, enter the IP Address or hostname of the alternate server.

Step 4 Complete any remaining fields in the **Phone Configuration** window. For help with the fields and their settings, see the online help.

Step 5 Click **Save**.

Step 6 Click **Apply Config** to push the changed fields to the phone.

Find Devices with Non-default Firmware Loads

The Firmware Load Information window in Unified Communications Manager enables you to quickly locate devices that are not using the default firmware load for their device type.

Note Each device can have an individually assigned firmware load that overrides the default.

Use the following procedure to locate devices that are not using the default firmware load.

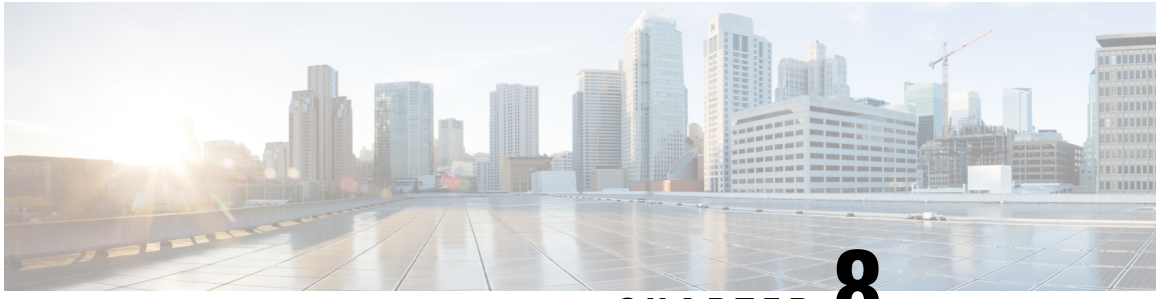
Procedure

Step 1 Choose **Device** > **Device Settings** > **Firmware Load Information**.

The page updates to display a list of device types that require firmware loads. For each device type, the Devices Not Using Default Load column links to configuration settings for any devices that use a non-default load.

Step 2 To view a list of devices of a particular device type that are using a non-default device load, click the entry for that device type in the Devices Not Using Default Load column.

The window that opens lists the devices of a particular device type that are not running the default firmware load.



CHAPTER 8

Manage Infrastructure Devices

Manage Infrastructure Overview

This chapter provides tasks to manage network infrastructure devices such as switches and wireless access points as a part of the Location Awareness feature. When Location Awareness is enabled, the Cisco Unified Communications Manager database saves status information for the switches and access points in your network, including the list of endpoints that currently associate to each switch or access point.

The endpoint to infrastructure device mapping helps Cisco Unified Communications Manager and Cisco Emergency Responder to determine the physical location of a caller. For example, if a mobile client places an emergency call while in a roaming situation, Cisco Emergency Responder uses the mapping to determine where to send emergency services.

The Infrastructure information that gets stored in the database also helps you to monitor your infrastructure usage. From the Unified Communications Manager interface, you can view network infrastructure devices such as switches and wireless access points. You can also see the list of endpoints that currently associate to a specific access point or switch. If infrastructure devices are not being used, you can deactivate infrastructure devices from tracking.

Manage Infrastructure Prerequisites

You must configure the Location Awareness feature before you can manage wireless infrastructure within the Cisco Unified Communications Manager interface. For your wired infrastructure, the feature is enabled by default.

For configuration details, see "Configure Location Awareness" chapter in the Feature Configuration Guide for Cisco Unified Communications Manager.

You must also install your network infrastructure. For details, see the hardware documentation that comes with your infrastructure devices such as wireless LAN controllers, Access Points, and Switches.

Manage Infrastructure Task Flow

Complete the following tasks to monitor and manage your network infrastructure devices.

Procedure

	Command or Action	Purpose
Step 1	View Status for Infrastructure Device, on page 70	Get the current status of a wireless access point or ethernet switch, including the list of associated endpoints.
Step 2	Deactivate Tracking for Infrastructure Device, on page 70	If you have a switch or access point that is not being used, mark the device inactive. The system will stop updating the status or the list of associated endpoints for the infrastructure device.
Step 3	Activate Tracking for Deactivated Infrastructure Devices, on page 71	Initiate tracking for an inactive infrastructure device. Cisco Unified Communications Manager begins updating the database with the status and the list of associated endpoints for the infrastructure device.

View Status for Infrastructure Device

Use this procedure to get the current status of an infrastructure device such as a wireless access point or an ethernet switch. Within the Cisco Unified Communications Manager interface, you can view the status for an access point or switch and see the current list of associated endpoints.

Procedure

Step 1 In Cisco Unified CM Administration, choose **Advanced Features** > **Device Location Tracking Services** > **Switches and Access Points**.

Step 2 Click **Find**.

Step 3 Click on the switch or access point for which you want the status.
The **Switches and Access Point Configuration** window displays the current status including the list of endpoints that currently associate to that access point or switch.

Deactivate Tracking for Infrastructure Device

Use this procedure to remove tracking for a specific infrastructure device such as a switch or access point. You may want to do this for switches or access points that are not being used.

Note If you remove tracking for an infrastructure device, the device remains in the database, but becomes inactive. Cisco Unified Communications Manager no longer updates the status for the device, including the list of endpoints that associate to the infrastructure device. You can view your inactive switches and access points from the **Related Links** drop-down in the **Switches and Access Points** window.

Procedure

Step 1 In Cisco Unified CM Administration, choose **Advanced Features** > **Device Location Tracking Services** > **Switches and Access Points**.

Step 2 Click **Find** and select the switch or access point that you want to stop tracking.

Step 3 Click **Deactivate Selected**.

Activate Tracking for Deactivated Infrastructure Devices

Use this procedure to initiate tracking for an inactive infrastructure device that has been deactivated. Once the switch or access point becomes active, Cisco Unified Communications Manager begins to dynamically track the status, including the list of endpoints that associate to the switch or access point.

Before you begin

Location Awareness must be configured. For details, see the "Location Awareness" chapter of the *System Configuration Guide for Cisco Unified Communications Manager*.

Procedure

Step 1 In Cisco Unified CM Administration, choose **Advanced Features** > **Device Location Tracking Services** > **Switches and Access Points**.

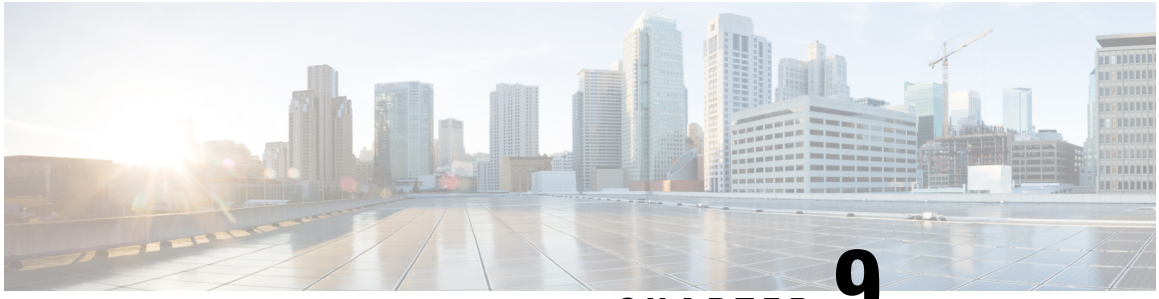
Step 2 From **Related Links**, choose **Inactive Switches and Access Points** and click **Go**.
The **Find and List Inactive Switches and Access Points** window displays infrastructure devices that are not being tracked.

Step 3 Select the switch or access point for which you want to initiate tracking.

Step 4 Click **Reactivate Selected**.

PART IV

Manage the System



CHAPTER 9

Monitor System Status

View Cluster Nodes Status

Use this procedure to show information about the nodes in your cluster.

Procedure

Step 1 From Cisco Unified Operating System Administration, choose **Show** > **Cluster**.

Step 2 Review the fields in the **Cluster** window. See the online help for more information about the fields.

View Hardware Status

Use this procedure to show the hardware status and information about hardware resources in your system.

Procedure

Step 1 From the Cisco Unified Operating System Administration, select **Show** > **Hardware**.

Step 2 Review the fields in the **Hardware Status** window. See the online help for more information about the fields.

View Network Status

Use this procedure to show the network status of your system, such as ethernet and DNS information.

The network status information that is displayed depends on whether Network Fault Tolerance is enabled:

- If Network Fault Tolerance is enabled, Ethernet port 1 automatically manages network communications if Ethernet port 0 fails.
- If Network Fault Tolerance is enabled, network status information is displayed for the network ports Ethernet 0, Ethernet 1, and Bond 0.
- If Network Fault Tolerance is not enabled, status information is displayed for only Ethernet 0.

Procedure

Step 1 From Cisco Unified Operating System Administration, choose **Show** > **Network**.

Step 2 Review the fields in the **Network Configuration** window. See the online help for more information about the fields.

View Installed Software

Use this procedure to show information about software versions and installed software packages.

Procedure

Step 1 From Cisco Unified Operating System Administration, choose **Show** > **Software**.

Step 2 Review the fields in the **Software Packages** window. See the online help for more information about the fields.

View System Status

Use this procedure to show the overall system status, such as information about locales, up time, CPU use, and memory use.

Procedure

Step 1 From Cisco Unified Operating System Administration, choose **Show** > **System**.

Step 2 Review the fields in the **System Status** window. See the online help for more information about the fields.

View IP Preferences

Use this procedure to show a list of registered ports are available to the system.

Procedure

Step 1 From Cisco Unified Operating System Administration, choose **Show** > **IP Preferences**.

Step 2 (Optional) To filter or search records, perform one of the following tasks:

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

Step 3 Click **Find**.

Step 4 Review the fields that appear in the **System Status** window. See the online help for more information about the fields.

View Last Login Details

When end users (with either local and LDAP credentials) and administrators log in to web applications for Cisco Unified Communications Manager or IM and Presence Service, the main application window displays the last successful and unsuccessful login details.

Users logging in using SAML SSO feature can only view the last successful system login information. The user can refer to the Identity Provider (IdP) application to track the unsuccessful SAML SSO login information.

The following web applications display the login attempt information:

- Cisco Unified Communications Manager:
  - Cisco Unified CM Administration
  - Cisco Unified Reporting
  - Cisco Unified Serviceability
- IM and Presence Service
  - Cisco Unified CM IM and Presence Administration
  - Cisco Unified IM and Presence Reporting
  - Cisco Unified IM and Presence Serviceability

Only administrators can login and view the last login details for the following web applications in Cisco Unified Communications Manager:

- Disaster Recovery System
- Cisco Unified OS Administration

Ping a Node

Use the Ping Utility to ping another node in the network. These results can help you verify or troubleshoot device connectivity.

Procedure

Step 1 From Cisco Unified Operating System Administration, choose **Services** > **Ping**.

Step 2 Configure the fields on the **Ping Configuration** window. See the online help for more information about the fields and their configuration options.

Step 3 Choose **Ping**.

The ping results are displayed.

Display Service Parameters

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

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

Procedure

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

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

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

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

Step 4 In the Service Parameter Configuration window that displays, choose Parameters for All Servers in The Related Links Drop-down List Box; then, click Go.

The Parameters for All Servers window displays. For the current service, the list shows all parameters in alphabetical order. For each parameter, the suggested value displays next to the parameter name. Under each parameter name, a list of servers that contain this parameter displays. Next to each server name, the current value for this parameter on this server displays.

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

Step 5 If you need to display out-of-sync service parameters, choose Out of Sync Parameters for All Servers in the Related Links drop-down list box, then click Go.

The Out of Sync Parameters for All Servers window displays. For the current service, service parameters that have different values on different servers display in alphabetical order. For each parameter, the suggested value displays next to the parameter name. Under each parameter name, a list of servers that contain this parameter displays. Next to each server name, the current value for this parameter on this server displays.

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

Step 6 If you need to display service parameters that have been modified from the suggested value, choose Modified Parameters for All Servers in the Related Links drop-down list box; then, click Go.

The Modified Parameters for All Servers window displays. For the current service, service parameters that have values that differ from the suggested values display in alphabetical order. For each parameter, the suggested value displays next to the parameter name. Under each parameter name, a list of servers that have different values from the suggested values displays. Next to each server name, the current value for this parameter on this server displays.

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

CHAPTER 10

View Usage Records

Usage Records Overview

Cisco Unified Communications Manager provides records that allow you to see how configured items are used in your system. Configured items include devices, as well as system-level settings such as device pools, date and time groups, and route plans.

Dependency Records

Use dependency records for the following purposes:

- Find information about system-level settings, such as servers, device pools, and date and time groups.
- Determine the records in the database that use other records. For example, you can determine which devices, such as CTI route points or phones, use a particular calling search space.
- Show dependencies between records before you delete any records. For example, before you delete a partition, use dependency records to see which calling search spaces (CSSs) and devices are associated with it. You can then reconfigure the settings to remove the dependency.

Route Plan Reports

The route plan report allows you to view either a partial or full list of numbers, routes, and patterns that are configured in the system. When you generate a report, you can access the configuration window for each item by clicking the entry in the Pattern/Directory Number, Partition, or Route Detail columns of the report.

In addition, the route plan report allows you to save report data into a.CSV file that you can import into other applications. The.CSV file contains more detailed information than the web pages, including directory numbers for phones, route patterns, pattern usage, device name, and device description.

Cisco Unified Communications Manager uses the route plan to route both internal calls and external public switched telephone network (PSTN) calls. Because you might have several records in your network, Cisco Unified Communications Manager Administration lets you locate specific route plan records on the basis of specific criteria.

Usage Report Tasks

Procedure

	Command or Action	Purpose
Step 1	To view route plan records and use them to manage unassigned directory numbers, see the following procedures: • View Route Plan Records, on page 82 • Save Route Plan Reports, on page 83 • Delete Unassigned Directory Numbers, on page 83 • Update Unassigned Directory Numbers, on page 84	Use these procedures to locate specific route plan records, save the records in a .CSV file, and manage unassigned directory numbers.
Step 2	To use dependency records, see the following procedures: • View Dependency Records, on page 85	Use these procedures to find information about system-level settings and show dependencies between records in the database.

Route Plan Reports Task Flow

Procedure

	Command or Action	Purpose
Step 1	View Route Plan Records, on page 82.	View route plan records and generate customized route plan reports.
Step 2	Save Route Plan Reports, on page 83.	View route plan reports in a.csv file format.
Step 3	Delete Unassigned Directory Numbers, on page 83.	Delete an unassigned directory number from the route plan report.
Step 4	Update Unassigned Directory Numbers, on page 84.	Update the settings of an unassigned directory number from the route plan report.

View Route Plan Records

This section describes how to view route plan records. Because you might have several records in your network, Cisco Unified Communications Manager Administration lets you locate specific route plan records on the basis of specific criteria. Use the following procedure to generate customized route plan reports.

Procedure

Step 1 Choose **Call Routing** > **Route Plan Report**.

Step 2 To find all records in the database, ensure the dialog box is empty and proceed to step 3.

To filter or search records

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

Step 3 Click **Find**.

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

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

The window displays the item that you choose.

Save Route Plan Reports

This section contains information on how to view route plan reports in a.csv file.

Procedure

Step 1 Choose **Call Routing** > **Route Plan Report**.

Step 2 Choose **View In File** from the **Related Links** drop-down list on the **Route Plan Report** window and click **Go**.

From the dialog box that appears, you can either save the file or import it into another application.

Step 3 Click **Save**.

Another window displays that allows you to save this file to a location of your choice.

Note You may also save the file as a different file name, but the file name must include a.CSV extension.

Step 4 Choose the location in which to save the file and click **Save**. This action should save the file to the location that you designated.

Step 5 Locate the.CSV file that you just saved and double-click its icon to view it.

Delete Unassigned Directory Numbers

This section describes how to delete an unassigned directory number from the route plan report. Directory numbers get configured and removed in the Directory Number Configuration window of Cisco Unified Communications Manager Administration. When a directory number gets removed from a device or a phone gets deleted, the directory number still exists in the Cisco Unified Communications Manager database. To delete the directory number from the database, use the Route Plan Report window.

Procedure

Step 1 Choose Call **Call Routing** > **Route Plan Report**.

Step 2 In the Route Plan Report window, use the three drop-down lists to specify a route plan report that lists all unassigned DNs.

Step 3 Three ways exist to delete directory numbers:

a) Click the directory number that you want to delete. When the Directory Number Configuration window displays, click Delete.

b) Check the check box next to the directory number that you want to delete. Click Delete Selected.

c) To delete all found unassigned directory numbers, click Delete All Found Items.

A warning message verifies that you want to delete the directory number.

Step 4 To delete the directory number, click OK. To cancel the delete request, click Cancel.

Update Unassigned Directory Numbers

This section describes how to update the settings of an unassigned directory number from the route plan report. Directory numbers get configured and removed in the Directory Number Configuration window of Cisco Unified Communications Manager Administration. When a directory number gets removed from a device, the directory number still exists in the Cisco Unified Communications Manager database. To update the settings of the directory number, use the Route Plan Report window.

Procedure

Step 1 Choose **Call Routing** > **Route Plan Report**.

Step 2 In the **Route Plan Report** window, use the three drop-down lists to specify a route plan report that lists all unassigned DNs.

Step 3 Click the directory number that you want to update.

Note You can update all the settings of the directory number except the directory number and partition.

Step 4 Make the required updates such as calling search space or forwarding options.

Step 5 Click **Save**.

The Directory Number Configuration window redisplays, and the directory number field is blank.

Dependency Records Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure Dependency Records, on page 85.	Use this procedure to enable or disable dependency records. This procedure runs at below-normal priority and may take time to complete due to dial plan size and complexity, CPU speed, and CPU requirements of other applications.
Step 2	View Dependency Records, on page 85.	After you enable dependency records, you can access them from the configuration windows on the interface.

Configure Dependency Records

Use dependency records to view relationships between records in the Cisco Unified Communications Manager database. For example, before you delete a partition, use dependency records to see which calling search spaces (CSSs) and devices are associated with it.

Caution Dependency records cause high CPU usage. This procedure runs at below-normal priority and may take time to complete due to dial plan size and complexity, CPU speed, and CPU requirements of other applications.

If you have dependency records enabled and your system is experiencing CPU usage issues, you can disable dependency records.

Procedure

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

Step 2 Scroll to the **CCMAdmin Parameters** section and from the **Enable Dependency Records** drop-down list, choose one of the following options:

- **True**—Enable dependency records.
- **False**—Disable dependency records.

Based on the option you choose, a dialog box appears with a message about the consequences of enabling or disabling the dependency records. Read the message before you click **OK** in this dialog box.

Step 3 Click **OK**.

Step 4 Click **Save**.
The `Update Successful` message appears confirming the change.

View Dependency Records

After you enable dependency records, you can access them from the configuration windows on the interface.

Before you begin

Configure Dependency Records, on page 85

Procedure

Step 1 From Cisco Unified CM Administration, navigate to the configuration window for the records that you want to view.

Example:

To view dependency records for a device pool, select **System** > **Device Pool**.

Note You cannot view dependency records from the **Device Defaults** and **Enterprise Parameters Configuration** windows.

Step 2 Click **Find**.

Step 3 Click one of the records.
The configuration window appears.

Step 4 From the **Related Links** list box, choose **Dependency Records** box, and click **Go**.

Note If you have not enabled the dependency records, the **Dependency Records Summary** window displays a message, not the information about the record.

The **Dependency Records Summary** window appears showing the records that are used by other records in the database.

Step 5 Select one of the following dependency record buttons in this window:

- **Refresh**—Update the window with current information.
- **Close**—Close the window without returning to the configuration window in which you clicked the Dependency Records link.
- **Close and Go Back**—Close the window and returns to the configuration window in which you clicked the Dependency Records link.

CHAPTER 11

Manage Enterprise Parameters

Enterprise Parameters Overview

Enterprise parameters provide default settings that apply to all devices and services across the entire cluster. For example, your system uses the enterprise parameters to set the initial values of its device defaults.

You cannot add or delete enterprise parameters, but you can update existing enterprise parameters. The configuration window lists enterprise parameters under categories; for example, CCMAdmin parameters, CCMUser parameters, and CDR parameters.

You can view detailed descriptions for enterprise parameters on the **Enterprise Parameters Configuration** window.

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

View Enterprise Parameter Information

Access information about enterprise parameters through embedded content in the **Enterprise Parameter Configuration** window.

Procedure

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

Step 2 Perform one of the following tasks:

- To view the description of a particular enterprise parameter, click the parameter name.
- To view the descriptions of all the enterprise parameters, click **?**.

Update Enterprise Parameters

Use this procedure to open the **Enterprise Parameter Configuration** window and configure system-level settings.

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

Procedure

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

Step 2 Choose the desired values for the enterprise parameters that you want to change.

Step 3 Click **Save**.

What to do next

Apply Configuration to Devices, on page 88

Apply Configuration to Devices

Use this procedure to update all affected devices in the cluster with the settings you configured.

Before you begin

Update Enterprise Parameters, on page 88

Procedure

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

Step 2 Verify your changes, and then click **Save**.

Step 3 Choose one of the following options:

- Click **Apply Config** if you want your system to determine which devices to reboot. In some cases, a device may not need a reboot. Calls in progress may be dropped but connected calls will be preserved unless the device pool includes SIP trunks.
- Click **Reset** if you want to reboot all devices in your cluster. We recommend that you perform this step during off-peak hours.

Step 4 After you read the confirmation dialog, click **OK**.

Restore Default Enterprise Parameters

Use this procedure if you want to reset the enterprise parameters to the default settings. Some enterprise parameters contain suggested values, as shown in the column on the configuration window; this procedure uses these values as the default settings.

Procedure

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

Step 2 Click **Set to Default**.

Step 3 After you read the confirmation prompt, click **OK**.

CHAPTER 12

Manage the Server

Manage the Server Overview

This chapter describes how to manage the properties of the Cisco Unified Communications Manager node, view the Presence Server status and configure a host name for the Unified Communications Manager server.

Server Deletion

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

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

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

Before you delete a server, consider the following information:

- Cisco Unified Communications Manager Administration does not allow you to delete the first node in the cluster, but you can delete any subsequent node.

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

Note When a subscriber node is removed from a cluster, its certificates still exist in publisher and other nodes. Admin has to manually remove:

- the certificate of the subscriber node removed from the trust-store of the individual cluster members.
- the certificates of each of the other cluster members from the trust-store of the removed subscriber node.

Delete Unified Communications Manager Node from Cluster

Use this procedure to delete a Cisco Unified Communications Manager node from the cluster.

Procedure

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

Step 2 Click **Find** and select the node you want to delete.

Step 3 Click **Delete**.

Step 4 Click **OK** when a warning dialog box indicates that this action cannot be undone.

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

Delete IM and Presence Node From Cluster

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

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

Procedure

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

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

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

Note You cannot delete the publisher node directly from a presence redundancy group. To delete a publisher node, first unassign users from the publisher node and delete the presence redundancy group completely.

However, you can add the deleted IM and Presence node back into the cluster. For more information on how to add the deleted nodes, see Add Deleted Server Back in to Cluster, on page 94. In this scenario, the **DefaultCUPSubcluster** is created automatically when the deleted publisher node is added back to the server in the **System** > **Server** screen in the Cisco Unified CM Administration console.

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

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

Step 6 Restart the **Cisco XCP Router** on all nodes.

Add Deleted Server Back in to Cluster

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

Procedure

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

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

Tip Make sure that the version that you install matches the version that runs on the publisher node. If the version that is running on the publisher does not match your installation file, choose the Upgrade During Install option during the installation process. For details, see the *Installation Guide for Cisco Unified Communications Manager and the IM and Presence Service*.

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

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

Add Node to Cluster Before Install

Use Cisco Unified Communications Manager Administration to add a new node to a cluster before installing the node. The server type you select when adding the node must match the server type you install.

You must configure a new node on the first node using Cisco Unified Communications Manager Administration before you install the new node. To install a node on a cluster, see the *Cisco Unified Communications Manager Installation Guide*.

For Cisco Unified Communications Manager Video/Voice servers, the first server you add during an initial installation of the Cisco Unified Communications Manager software is designated the publisher node. All subsequent server installations or additions are designated as subscriber nodes. The first Cisco Unified Communications Manager IM and Presence node you add to the cluster is designated the IM and Presence Service database publisher node.

Note You cannot use Cisco Unified Communications Manager Administration to change the server type after the server has been added. You must delete the existing server instance, and then add the new server again and choose the correct server type setting.

Procedure

Step 1 Select **System** > **Server**.

The **Find and List Servers** window displays.

Step 2 Click **Add New**.

The **Server Configuration - Add a Server** window displays.

Step 3 From the **Server Type** drop-down list box, choose the server type that you want to add, and then click **Next**.

- CUCM Video/Voice
- CUCM IM and Presence

Step 4 In the **Server Configuration** window, enter the appropriate server settings.

For server configuration field descriptions, see Server Settings.

Step 5 Click **Save**.

View Presence Server Status

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

Procedure

Step 1 Select **System** > **Server**.

The **Find and List Servers** window appears.

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

Matching records appear.

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

The **Server Configuration** window appears.

Step 4 Click on the Presence Server Status link in the IM and Presence Server Information section of the **Server Configuration** window.

The **Node Details** window for the server appears.

Configure Ports

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

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

Procedure

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

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

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

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

Step 5 Click **Save**.

Step 6 Click **Apply Config**.

Step 7 Click **OK**.

Port Settings

Field	Description
Ethernet Phone Port	The system uses this TCP port to communicate with the Cisco Unified IP Phones (SCCP only) on the network. • Accept the default port value of 2000 unless this port is already in use on your system. Choosing 2000 identifies this port as non-secure. • Ensure all port entries are unique. • Valid port numbers range from 1024 to 49151.
MGCP Listen Port	The system uses this TCP port to detect messages from its associated MGCP gateway. • Accept the default port of 2427 unless this port is already in use on your system. • Ensure all port entries are unique. • Valid port numbers range from 1024 to 49151.

Field	Description
MGCP Keep-alive Port	The system uses this TCP port to exchange keepalive messages with its associated MGCP gateway. • Accept the default port of 2428 unless this port is already in use on your system. • Ensure all port entries are unique. • Valid port numbers range from 1024 to 49151.
SIP Phone Port	This field specifies the port number that Unified Communications Manager uses to listen for SIP line registrations over TCP and UDP.
SIP Phone Secure Port	This field specifies the port number that the system uses to listen for SIP line registrations over TLS.

Hostname Configuration

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

Table 2: Host Name Configuration in Cisco Unified Communications Manager

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

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

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

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

  After you install the Unified Communications Manager publisher node, the host name for the publisher automatically displays in this field. Before you install a Unified Communications Manager subscriber node, enter either the IP address or the host name for the subscriber node in this field on the Unified Communications Manager publisher node.

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

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

- During the installation of the Unified Communications Manager publisher node, you enter the host name, which is mandatory, and IP address of the publisher node to configure network information; that is, if you want to use static networking.

  During the installation of a Unified Communications Manager subscriber node, you enter the hostname and IP address of the Unified Communications Manager publisher node, so that Unified Communications Manager can verify network connectivity and publisher-subscriber validation. Additionally, you must enter the host name and the IP address for the subscriber node. When the Unified Communications Manager installation prompts you for the host name of the subscriber server, enter the value that displays in the Server Configuration window in Cisco Unified Communications Manager Administration; that is, if you configured a host name for the subscriber server in the Host Name/IP Address field.

kerneldump Utility

The kerneldump utility allows you to collect crash dump logs locally on the affected machine without requiring a secondary server.

In a Unified Communications Manager cluster, you only need to ensure the kerneldump utility is enabled on the server before you can collect the crash dump information.

Note Cisco recommends that you verify the kerneldump utility is enabled after you install Unified Communications Manager to allow for more efficient troubleshooting. If you have not already done so, enable the kerneldump utility before you upgrade the Unified Communications Manager from supported appliance releases.

Important Enabling or disabling the kerneldump utility will require a reboot of the node. Do not execute the enable command unless you are within a window where a reboot would be acceptable.

The *command line interface* (CLI) for the *Cisco Unified Communications Operating System* can be used to enable, disable, or check the status of the kerneldump utility.

Use the following procedure to enable the kernel dump utility:

Working with Files That Are Collected by the Utility

To view the crash information from the kerneldump utility, use the *Cisco Unified Real-Time Monitoring Tool* or the *Command Line Interface* (CLI). To collect the kerneldump logs by using the *Cisco Unified Real-Time Monitoring Tool*, choose the Collect Files option from Trace & Log Central. From the Select System Services/Applications tab, choose the Kerneldump logs check box. For more information on collecting files using *Cisco Unified Real-Time Monitoring Tool*, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

To use the CLI to collect the kerneldump logs, use the "file" CLI commands on the files in the crash directory. These are found under the "activelog" partition. The log filenames begin with the IP address of the kerneldump client and end with the date that the file is created. For more information on the file commands, refer to the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

Enable the Kerneldump Utility

Use this procedure to enable the kerneldump utility. In the event of a kernel crash, the utility provides a mechanism for collecting and dumping the crash. You can configure the utility to dump logs to the local server or to an external server.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Complete either of the following:

- To dump kernel crashes on the local server, run the `utils os kernelcrash enable` CLI command.
- To dump kernel crashes to an external server, run the `utils os kerneldump ssh enable <ip_address>` CLI command with the IP address of the external server.

Step 3 Reboot the server.

Example

Note If you need to disable the kerneldump utility, you can run the `utils os kernelcrash disable` CLI command to disable the local server for core dumps and the `utils os kerneldump ssh disable <ip_address>` CLI command to disable the utility on the external server.

What to do next

Configure an email alert in the Real-Time Monitoring Tool to be advised of core dumps. For details, see Enable Email Alert for Core Dump, on page 100

Refer to the *Troubleshooting Guide for Cisco Unified Communications Manager* for more information on the kerneldump utility and troubleshooting.

Enable Email Alert for Core Dump

Use this procedure to configure the Real-Time Monitoring Tool to email the administrator whenever a core dump occurs.

Procedure

Step 1 Select **System** > **Tools** > **Alert** > **Alert Central**.

Step 2 Right-click **CoreDumpFileFound** alert and select **Set Alert Properties**.

Step 3 Follow the wizard prompts to set your preferred criteria:

a) In the **Alert Properties: Email Notification** popup, make sure that **Enable Email** is checked and click **Configure** to set the default alert action, which will be to email an administrator.

b) Follow the prompts and **Add** a Receipient email address. When this alert is triggered, the default action will be to email this address.

c) Click **Save**.

Step 4 Set the default Email server:

a) Select **System** > **Tools** > **Alert** > **Config Email Server**.

b) Enter the e-mail server settings.

c) Click **OK**.

PART V

Manage Security

CHAPTER 13

Manage SAML Single Sign-On

SAML Single Sign-On Overview

Use SAML Single Sign-On (SSO) to access a defined set of Cisco applications 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 (such as Cisco Unified Communications Manager) to authenticate a user. With SAML, security authentication information is exchanged between an identity provider (IdP) and a service provider. The feature provides secure mechanisms to use common credentials and relevant information across various 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 user information of the IdP to provide access to the various services or applications.

The client authenticates against the IdP, and the IdP grants an Assertion to the client. The client presents the assertion to the service provider. Because a CoT established, the service provider trusts the assertion and grants access to the client.

Opt-In Control for Certificate-Based SSO Authentication for Cisco Jabber on iOS

This release of Cisco Unified Communications Manager introduces the opt-in configuration option to control Cisco Jabber on iOS SSO login behavior with an Identity provider (IdP). Use this option to allow Cisco Jabber to perform certificate-based authentication with the IdP in a controlled mobile device management (MDM) deployment.

You can configure the opt-in control through the **SSO Login Behavior for iOS** enterprise parameter in Cisco Unified Communications Manager.

Note Before you change the default value of this parameter, see the Cisco Jabber feature support and documentation at http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/tsd-products-support-series-home.html to ensure Cisco Jabber on iOS support for SSO login behavior and certificate-based authentication.

To enable this feature, see the Configure SSO Login Behavior for Cisco Jabber on iOS, on page 105 procedure.

SAML Single Sign-On Prerequisites

- DNS configured for the Cisco Unified Communications Manager cluster
- An identity provider (IdP) server
- An LDAP server that is trusted by the IdP server and supported by your system

The following IdPs using SAML 2.0 are tested for the SAML SSO feature:

- OpenAM 10.0.1
- Microsoft® Active Directory® Federation Services 2.0 (AD FS 2.0)
- PingFederate® 6.10.0.4
- F5 BIP-IP 11.6.0

The third-party applications must meet the following configuration requirements:

- The mandatory attribute "uid" must be configured on the IdP. This attribute must match the attribute that is used for the LDAP-synchronized user ID in Cisco Unified Communications Manager.
- The clocks of all the entities participating in SAML SSO must be synchronized. For information about synchronizing clocks, see "NTP Settings" in the *System 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.

Manage SAML Single Sign-On

Enable SAML Single Sign-On

Note You cannot enable SAML SSO until the verify sync agent test succeeds.

Before you begin

- Ensure that user data is synchronized to the Unified Communications Manager database. For more information, see the *System 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.

- Verify that the Cisco Unified CM IM and Presence Service Cisco Sync Agent service successfully completed data synchronization. Check the status of this test by choosing **Cisco Unified CM IM and Presence Administration** > **Diagnostics** > **System Troubleshooter**. The "Verify Sync Agent has sync'ed over relevant data (e.g. devices, users, licensing information)" test indicates a test passed outcome if data synchronization successfully completed.
- Ensure that at least one LDAP synchronized user is added to the Standard CCM Super Users group to enable access to Cisco Unified CM Administration. For more information, see the *System 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.
- 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.

Procedure

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

Step 2 Click **Enable SAML SSO**.

Step 3 After you see warning message to notify you that all server connections will be restarted, click **Continue**.

Step 4 Click **Browse** to locate and upload the IdP metadata file.

Step 5 Click **Import IdP Metadata**.

Step 6 Click **Next**.

Step 7 Click **Download Trust Metadata Fileset** to download server metadata to your system.

Step 8 Upload the server metadata on the IdP server.

Step 9 Click **Next** to continue.

Step 10 Choose an LDAP synchronized user with administrator rights from the list of valid administrator IDs.

Step 11 Click **Run Test**.

Step 12 Enter a valid username and password.

Step 13 Close the browser window after you see the success message.

Step 14 Click **Finish** and allow 1 to 2 minutes for the web applications to restart.

Configure SSO Login Behavior for Cisco Jabber on iOS

Procedure

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

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

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

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

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

Step 3 Click **Save**.

Enable SAML Single Sign-On on WebDialer After an Upgrade

Follow these tasks to reactivate SAML Single Sign-On on Cisco WebDialer after an upgrade. If Cisco WebDialer is activated before SAML Single Sign-On is enabled, SAML Single Sign-On is not enabled on Cisco WebDialer by default.

Procedure

	Command or Action	Purpose
Step 1	Deactivate the Cisco WebDialer Service, on page 106	Deactivate the Cisco WebDialer web service if it is already activated.
Step 2	Disable SAML Single Sign-On, on page 107	Disable SAML Single Sign-On if it is already enabled.
Step 3	Activate the Cisco WebDialer Service, on page 107	
Step 4	Enable SAML Single Sign-On, on page 104	

Deactivate the Cisco WebDialer Service

Deactivate the Cisco WebDialer web service if it is already activated.

Procedure

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

Step 2 From the **Servers** drop-down list, choose the Cisco Unified Communications Manager server that is listed.

Step 3 From **CTI Services**, uncheck the **Cisco WebDialer Web Service** check box.

Step 4 Click **Save**.

What to do next

Disable SAML Single Sign-On, on page 107

Disable SAML Single Sign-On

Disable SAML Single Sign-On if it is already enabled.

Before you begin

Deactivate the Cisco WebDialer Service, on page 106

Procedure

From the CLI, run the command **utils sso disable**.

What to do next

Activate the Cisco WebDialer Service, on page 107

Activate the Cisco WebDialer Service

Before you begin

Disable SAML Single Sign-On, on page 107

Procedure

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

Step 2 From the **Servers** drop-down list, choose the Unified Communications Manager server that is listed.

Step 3 From **CTI Services**, check the **Cisco WebDialer Web Service** check box.

Step 4 Click **Save**.

Step 5 From Cisco Unified Serviceability, choose **Tools** > **Control Center - Feature Services** to confirm that the CTI Manager service is active and is in start mode.

For WebDialer to function properly, the CTI Manager service must be active and in start mode.

What to do next

Enable SAML Single Sign-On, on page 104

Access the Recovery URL

Use the recovery URL to bypass SAML Single Sign-On and log in to the Cisco Unified Communications Manager Administration and Cisco Unified CM IM and Presence Service interfaces for troubleshooting. For

example, enable the recovery URL before you change the domain or hostname of a server. Logging in to the recovery URL facilitates an update of the server metadata.

Before you begin

- Only application users with administrative privileges can access the recovery URL.
- If SAML SSO is enabled, the recovery URL is enabled by default. You can enable and disable the recovery URL from the CLI. For more information about the CLI commands to enable and disable the recovery URL, see *Command Line Interface Guide for Cisco Unified Communications Solutions*.

Procedure

In your browser, enter `https://hostname:8443/ssosp/local/login`.

Update Server Metadata After a Domain or Hostname Change

After a domain or hostname change, SAML Single Sign-On is not functional until you perform this procedure.

Note If you are unable to log in to the **SAML Single Sign-On** window even after performing this procedure, clear the browser cache and try logging in again.

Before you begin

If the recovery URL is disabled, it does not appear for you to bypass the Single Sign-On link. To enable the recovery URL, log in to the CLI and execute the following command: **utils sso recovery-url enable**.

Procedure

Step 1 In the address bar of your web browser, enter the following URL:

```
https://<Unified CM-server-name>
```

where `<Unified CM-server-name>` is the hostname or IP address of the server.

Step 2 Click **Recovery URL to bypass Single Sign-On (SSO)**.

Step 3 Enter the credentials of an application user with an administrator role and click **Login**.

Step 4 From Cisco Unified CM Administration, choose **System** > **SAML Single Sign-On**.

Step 5 Click **Export Metadata** to download the server metadata.

Step 6 Upload the server metadata file to the IdP.

Step 7 Click **Run Test**.

Step 8 Enter a valid User ID and password.

Step 9 After you see the success message, close the browser window.

Manually Provision Server Metadata

To provision a single connection in your Identity Provider for multiple UC applications, you must manually provision the server metadata while configuring the Circle of Trust between the Identity Provider and the Service Provider. For more information about configuring the Circle of Trust, see the IdP product documentation.

The general URL syntax is as follows:

```
https://<SP FQDN>:8443/ssosp/saml/SSO/alias/<SP FQDN>
```

Procedure

To provision the server metadata manually, use the Assertion Customer Service (ACS) URL.

Example:

Sample ACS URL:

```
<md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://cucm.ucsso.cisco.com:8443/ssosp/saml/SSO/alias/cucm.ucsso.cisco.com"
index="0"/>
```

CHAPTER 14

Manage Certificates

Certificates Overview

Your system uses self-signed- and third-party-signed certificates. Certificates are used between devices in your system to securely authenticate devices, encrypt data, and hash the data to ensure its integrity from source to destination. Certificates allow for secure transfer of bandwidth, communication, and operations.

The most important part of certificates is that you know and define how your data is encrypted and shared with entities such as the intended website, phone, or FTP server.

When your system trusts a certificate, this means that there is a preinstalled certificate on your system which states it is fully confident that it shares information with the correct destination. Otherwise, it terminates the communication between these points.

In order to trust a certificate, trust must already be established with a third-party certificate authority (CA).

Your devices must know that they can trust both the CA and intermediate certificates first, before they can trust the server certificate presented by the exchange of messages called the secure sockets layer (SSL) handshake.

Note EC-based certificates for Tomcat are supported. This new certificate is called tomcat-ECDSA. For further information, see the Enhanced TLS Encryption on IM and Presence Service section of the *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.

EC Ciphers on the Tomcat interface are disabled by default. You can enable them using the **HTTPS Ciphers** enterprise parameter on Cisco Unified Communications Manager or on IM and Presence Service. If you change this parameter the Cisco Tomcat service must be restarted on all nodes.

For further information on EC-based certificates see, ECDSA Support for Common Criteria for Certified Solutions in the Release Notes for Cisco Unified Communications Manager and IM and Presence Service.

Third-Party Signed Certificate or Certificate Chain

Upload the certificate authority root certificate of the certificate authority that signed an application certificate. If a subordinate certificate authority signs an application certificate, you must upload the certificate authority root certificate of the subordinate certificate authority. You can also upload the PKCS#7 format certificate chain of all certificate authority certificates.

You can upload certificate authority root certificates and application certificates by using the same **Upload Certificate** dialog box. When you upload a certificate authority root certificate or certificate chain that contains only certificate authority certificates, choose the certificate name with the format certificate type-trust. When you upload an application certificate or certificate chain that contains an application certificate and certificate authority certificates, choose the certificate name that includes only the certificate type.

For example, choose **tomcat-trust** when you upload a Tomcat certificate authority certificate or certificate authority certificate chain; choose **tomcat** or **tomcat-ECDSA** when you upload a Tomcat application certificate or certificate chain that contains an application certificate and certificate authority certificates.

When you upload a CAPF certificate authority root certificate, it is copied to the CallManager-trust store, so you do not need to upload the certificate authority root certificate for CallManager separately.

Note Successful upload of third-party certificate authority signed certificate deletes a recently generated CSR that was used to obtain a signed certificate and overwrites the existing certificate, including a third-party signed certificate if one was uploaded.

Note The system automatically replicates tomcat-trust, CallManager-trust and Phone-SAST-trust certificates to each node in the cluster.

Note You can upload a directory trust certificate to tomcat-trust, which is required for the DirSync service to work in secure mode.

Third-Party Certificate Authority Certificates

To use an application certificate that a third-party certificate authority issues, you must obtain both the signed application certificate and the certificate authority root certificate from the certificate authority or PKCS#7 certificate chain (distinguished encoding rules [DER]), which contains both the application certificate and certificate authority certificates. Retrieve information about obtaining these certificates from your certificate authority. The process varies among certificate authorities. The signature algorithm must use RSA encryption.

Cisco Unified Communications Operating System generates CSRs in privacy enhanced mail (PEM) encoding format. The system accepts certificates in DER and PEM encoding formats and PKCS#7 Certificate chain in PEM format. For all certificate types except certificate authority proxy function (CAPF), you must obtain and upload a certificate authority root certificate and an application certificate on each node.

For CAPF, obtain and upload a certificate authority root certificate and an application certificate only on the first node. CAPF and Unified Communications Manager CSRs include extensions that you must include in your request for an application certificate from the certificate authority. If your certificate authority does not support the ExtensionRequest mechanism, you must enable the X.509 extensions, as follows:

- The CAPF CSR uses the following extensions:

```
X509v3 Extended Key Usage:
TLS Web Server Authentication
X509v3 Key Usage:
Digital Signature, Certificate Sign
```

- The CSRs for Tomcat and Tomcat-ECDSA, use the following extensions:

Note Tomcat or Tomcat-ECDSA does not require the key agreement or IPsec end system key usage.

```
X509v3 Extended Key Usage:
 TLS Web Server Authentication, TLS Web Client Authentication, IPSec End System

 X509v3 Key Usage:
 Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
```

- The CSRs for IPsec use the following extensions:

```
 X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication, IPSec End System
X509v3 Key Usage:
Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
```

- The CSRs for Unified Communications Manager use the following extensions:

```
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Key Usage:
Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
```

- The CSRs for the IM and Presence Service cup and cup-xmpp certificates use the following extensions:

```
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication, IPSec End System
X509v3 Key Usage:
Digital Signature, Key Encipherment, Data Encipherment, Key Agreement,
```

Note You can generate a CSR for your certificates and have them signed by a third party certificate authority with a SHA256 signature. You can then upload this signed certificate back to Unified Communications Manager, allowing Tomcat and other certificates to support SHA256.

Certificate Signing Request Key Usage Extensions

The following tables display key usage extensions for Certificate Signing Requests (CSRs) for both Unified Communications Manager and the IM and Presence Service CA certificates.

Table 3: Cisco Unified Communications Manager CSR Key Usage Extensions

	Multi server	Extended Key Usage			Key Usage				
		Server Authentication (1.3.6.1.5.5.7.3.1)	Client Authentication (1.3.6.1.5.5.7.3.2)	IP security end system (1.3.6.1.5.5.7.3.5)	Digital Signature	Key Encipherment	Data Encipherment	Key Cert Sign	Key Agreement
CallManager CallManager-ECDSA	Y	Y	Y		Y	Y	Y		
CAPF (publisher only)	N	Y			Y	Y		Y	
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		
TVS	Y	Y	Y		Y	Y	Y		

Table 4: IM and Presence Service CSR Key Usage Extensions

	Multi server	Extended Key Usage			Key Usage				
		Server Authentication (1.3.6.1.5.5.7.3.1)	Client Authentication (1.3.6.1.5.5.7.3.2)	IP security end system (1.3.6.1.5.5.7.3.5)	Digital Signature	Key Encipherment	Data Encipherment	Key Cert Sign	Key Agreement
cup cup-ECDSA	N	Y	Y	Y	Y	Y	Y		Y
cup-xmpp cup-xmpp-ECDSA	Y	Y	Y	Y	Y	Y	Y		Y
cup-xmpp-s2s cup-xmpp-s2s-ECDSA	Y	Y	Y	Y	Y	Y	Y		Y
ipsec	N	Y	Y	Y	Y	Y	Y		

	Multi server	Extended Key Usage			Key Usage				
		Server Authentication (1.3.6.1.5.5.7.3.1)	Client Authentication (1.3.6.1.5.5.7.3.2)	IP security end system (1.3.6.1.5.5.7.3.5)	Digital Signature	Key Encipherment	Data Encipherment	Key Cert Sign	Key Agreement
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		

Show Certificates

Use the filter option on the Certificate List page, to sort and view the list of certificates, based on their common name, expiry date, key type, and usage. The filter option thus allows you to sort, view, and manage your data effectively.

From Unified Communications Manager Release 14, you can choose the usage option to sort and view the list of identity or trust certificates.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.
The Certificate List page appears.

Step 2 From the **Find Certificate List where** drop-down list, choose the required filter option, enter the search item in the **Find** field, and click the **Find** button.

For example, to view only identity certificates, choose **Usage** from the **Find Certificate List where** drop-down list, enter Identity in the **Find** field, and click the **Find** button.

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**.

Install Intermediate Certificates

To install an intermediate certificate, you must install a root certificate first and then upload the signed certificate. This step is required only if the certificate authority provides a signed certificate with multiple certificates in the certificate chain.

Procedure

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

Step 2 Click **Upload Certificate / Certificate Chain**.

Step 3 Choose the appropriate trust store from the **Certificate Purpose** drop-down list to install the root certificate.

Step 4 Enter the description for the certificate purpose selected.

Step 5 Choose the file to upload by performing one of the following steps:

- In the **Upload File** text box, enter the path to the file.
- Click **Browse** and navigate to the file; then click **Open**.

Step 6 Click **Upload**.

Step 7 Access the Cisco Unified Intelligence Center URL using the FQDN after you install the customer certificate. If you access the Cisco Unified Intelligence Center using an IP address, you will see the message “Click here to continue”, even after you successfully install the custom certificate.

Note
- TFTP service should be deactivated and later activated when a Tomcat certificate is uploaded. Else, the TFTP continues to offer the old cached self-signed tomcat certificate.

Delete a Trust Certificate

A trusted certificate is the only type of certificate that you can delete. You cannot delete a self-signed certificate that is generated by your system.

Caution Deleting a certificate can affect your system operations. It can also break a certificate chain if the certificate is part of an existing chain. Verify this relationship from the username and subject name of the relevant certificates in the **Certificate List** window. You cannot undo this action.

Procedure

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

Step 2 Use the **Find** controls to filter the certificate list.

Step 3 Choose the filename of the certificate.

Step 4 Click **Delete**.

Step 5 Click **OK**.

Note
- If you delete the , “tomcat-trust”, “CallManager-trust”, or “Phone-SAST-trust” certificate type, the certificate is deleted across all servers in the cluster.

Regenerate a Certificate

We recommend you to regenerate certificates before they expire. You will receive warnings in RTMT (Syslog Viewer) and an email notification when the certificates are about to expire.

However, you can also regenerate an expired certificate. Perform this task after business hours, because you must restart phones and reboot services. You can regenerate only a certificate that is listed as type “cert” in Cisco Unified OS Administration

Caution Regenerating a certificate can affect your system operations. Regenerating a certificate overwrites the existing certificate, including a third-party signed certificate if one was uploaded.

Procedure

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

Enter search parameters to find a certificate and view its configuration details. The system displays the records that match all the criteria in the **Certificate List** window.

Click **Regenerate** button in certificate details page, a self-signed certificate with the same key length is regenerated.

Click **Generate Self-Signed Certificate** to regenerate a self-signed certificate with a new key length of 3072 or 4096.

Step 2 Configure the fields on the **Generate New Self-Signed Certificate** window. See online help for more information about the fields and their configuration options.

Step 3 Click **Generate**.

Step 4 Restart all services that are affected by the regenerated certificate.

Step 5 Update the CTL file (if configured) after you regenerate the CAPF, ITLRecovery Certificates or CallManager Certificates.

Note After you regenerate certificates, you must perform a system backup so that the latest backup contains the regenerated certificates. If your backup does not contain the regenerated certificates and you perform a system restoration task, you must manually unlock each phone in your system so that the phone can register.

Certificate Names and Descriptions

The following table describes the system security certificates that you can regenerate and the related services that must be restarted. For information about regenerating the TFTP certificate, see the *Cisco Unified Communications Manager Security Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Table 5: Certificate Names and Descriptions

Name	Description	Related Services
tomcat tomcat-ECDSA	This certificate is used by WebServices and Cisco CallManager services when SIP Oauth mode is enabled.	Cisco Tomcat Services, Cisco CallManager Service.
CallManager CallManager-ECDSA	This is used for SIP, SIP trunk, SCCP, TFTP etc.	CallManager - NA CallManager-ECDSA - Cisco CallManager Service
CAPF	Used by the CAPF service running on the Unified Communications Manager Publisher. This certificate is used to issue LSC to the endpoints (except online and offline CAPF mode)	N/A
TVS	This is used by Trust verification service, which acts as a secondary trust verification mechanism for the phones in case the server certificate changes.	N/A

Note A new enterprise parameter Phone Interaction on Certificate Update under section Security Parameter is introduced to reset phones either manually or automatically as applicable when one of the TVS, CAPF, or TFTP certificates are updated. This parameter is by default set to reset the phones automatically.

Regenerate Keys for OAuth Refresh Logins

Use this procedure to regenerate both the encryption key and the signing key using the Command Line Interface. Complete this task only if the encryption key or signing key that Cisco Jabber uses for OAuth authentication with Unified Communications Manager has been compromised. The signing key is asymmetric and RSA-based whereas the encryption key is a symmetric key.

After you complete this task, the current access and refresh tokens that use these keys become invalid.

We recommend that you complete this task during off-hours to minimize the impact to end users.

The encryption key can be regenerated only via the CLI below, but you can also use the Cisco Unified OS Administration GUI of the publisher to regenerate the signing key. Choose **Security** > **Certificate Management**, select the **AUTHZ** certificate, and click **Regenerate**.

Procedure

Step 1 From the Unified Communications Manager publisher node, log in to the **Command Line** Interface .

Step 2 If you want to regenerate the encryption key:

a) Run the `set key regen authz encryption` command.

b) Enter `yes`.

Step 3 If you want to regenerate the signing key:

a) Run the `set key regen authz signing` command.

b) Enter `yes`.
The Unified Communications Manager publisher node regenerates keys and replicates the new keys to all Unified Communications Manager cluster nodes, including any local IM and Presence Service nodes.

You must regenerate and sync your new keys on all of your UC clusters:

- IM and Presence central cluster—If you have an IM and Presence centralized deployment, your IM and Presence nodes are running on a separate cluster from your telephony. In this case, repeat this procedure on the Unified Communications Manager publisher node of the IM and Presence Service central cluster.
- Cisco Expressway or Cisco Unity Connection—Regenerate the keys on those clusters as well. See your Cisco Expressway and Cisco Unity Connection documentation for details.

Note Restart the Cisco CallManager Service on all nodes in the cluster after the keys are reassigned.

Upload Certificate or Certificate Chain

Upload any new certificates or certificate chains that you want your system to trust.

Procedure

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

Step 2 Click **Upload Certificate/Certificate Chain**.

Step 3 Choose the certificate name from the **Certificate Purpose** drop-down list.

Step 4 Choose the file to upload by performing one of the following steps:

- In the **Upload File** text box, enter the path to the file.
- Click **Browse**, navigate to the file, and then click **Open**.

Step 5 To upload the file to the server, click **Upload File**.

Note Restart the affected service after uploading the certificate. When the server comes back up you can access the CCMAdmin or CCMUser GUI to verify your newly added certificates in use.

Manage Third-Party Certificate Authority Certificates

This task flow provides an overview of the third-party certificate process, with references to each step in the sequence. Your system supports certificates that a third-party certificate authority issues with a PKCS # 10 certificate signing request (CSR).

Procedure

	Command or Action	Purpose
Step 1	Generate a Certificate Signing Request, on page 121	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.
Step 2	Download a Certificate Signing Request, on page 121	Download the CSR after you generate it and have it ready to submit to your certificate authority.
Step 3	See your certificate authority documentation.	Obtain application certificates from your certificate authority.
Step 4	See your certificate authority documentation.	Obtain a root certificate from your certificate authority.
Step 5	Add Certificate Authority-Signed CAPF Root Certificate to the Trust Store , on page 121	Add the root certificate to the trust store. Perform this step when using a certificate authority-signed CAPF certificate.
Step 6	Upload Certificate or Certificate Chain, on page 119	Upload the certificate authority root certificate to the node.
Step 7	If you updated the certificate for CAPF or Cisco Unified Communications Manager, generate a new CTL file.	See the *Cisco Unified Communications Manager Security Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html. Rerun the CTL client (if configured) after you upload the third-party signed CAPF or CallManager certificate.
Step 8	Restart a Service, on page 122	Restart the services that are affected by the new certificate. For all certificate types, restart the

	Command or Action	Purpose
		corresponding service (for example, restart the Cisco Tomcat service if you updated the Tomcat or Tomcat-ECDSA certificate).

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**.

Add Certificate Authority-Signed CAPF Root Certificate to the Trust Store

Add the root certificate to the Unified Communications Manager trust store when using a Certificate Authority-Signed CAPF Certificate.

Procedure

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

Step 2 Click **Upload Certificate/Certificate Chain**.

Step 3 In the **Upload Certificate/Certificate Chain** popup window, choose **CallManager-trust** from the **Certificate Purpose** drop-down list and browse to the certificate authority-signed CAPF root certificate.

Step 4 Click **Upload** after the certificate appears in the **Upload File** field.

Restart a Service

Use this procedure if your system requires that you restart any feature or network services on a particular node in your cluster.

Procedure

Step 1 Depending on the service type that you want to restart, perform one of the following tasks:

- Choose **Tools** > **Control Center - Feature Services**.
- Choose **Tools** > **Control Center - Network Services**.

Step 2 Choose your system node from the **Server** drop-down list, and then click **Go**.

Step 3 Click the radio button next to the service that you want to restart, and then click **Restart**.

Step 4 After you see the message that indicates that the restart will take some time, click **OK**.

CertificateRevocationthroughOnlineCertificateStatusProtocol

Unified Communications Manager provisions the OCSP for monitoring certificate revocation. System checks for the certificate status to confirm validity at scheduled intervals and every time there is, a certificate uploaded.

The Online Certificate Status Protocol (OCSP) helps administrators manage their system's certificate requirements. When OCSP is configured, it provides a simple, secure, and automated method to check certificate validity and revoke expired certificates in real-time.

For FIPS deployments with Common Criteria mode enabled, OCSP also helps your system comply with Common Criteria requirements.

Validation Checks

Unified Communications Manager checks the certificate status and confirms validity.

The certificates are validated as follows:

- Unified Communications Manager uses the Delegated Trust Model (DTM) and checks the Root CA or Intermediate CA for the OCSP signing attribute. The Root CA or the Intermediate CA must sign the OCSP Certificate to check the status. If the delegated trust model fails, Unified Communications Manager

falls back to the Trust Responder Model (TRP) and uses a designated OCSP response signing certificate from an OCSP server to validate certificates.

Note OCSP Responder must be running to check the revocation status of the certificates.

- Enable OCSP option in the **Certificate Revocation** window to provide the most secure means of checking certificate revocation in real-time. Choose from options to use the OCSP URI from a certificate or from the configured OCSP URI. For more information on manual OCSP configuration, see Configure Certificate Revocation via OCSP.

Note In case of leaf certificates, TLS clients like syslog, FileBeat, SIP, ILS, LBM, and so on send OCSP requests to the OCSP responder and receives the certificate revocation response in real-time from the OCSP responder.

One of the following status is returned for the certificate once the validations are performed and the Common Criteria mode is ON.

- **Good** --The **good** state indicates a positive response to the status inquiry. At a minimum, this positive response indicates that the certificate is not revoked, but does not necessarily mean that the certificate was ever issued or that the time at which the response was produced is within the certificate's validity interval. Response extensions may be used to convey additional information on assertions made by the responder regarding the status of the certificate such as positive statement about issuance, validity, etc.
- **Revoked** --The **revoked** state indicates that the certificate has been revoked (either permanantly or temporarily (on hold)).
- **Unknown** -- The **unknown** state indicates that the OCSP responder doesn't know about the certificate being requested.

Note In Common Criteria mode, the connection fails in both **Revoked** as well as **Unknown** case whereas the connection would succeed in **Unknown** response case when Common Criteria is not enabled.

Certificate Monitoring Task Flow

Complete these tasks to configure the system to monitor certificate status and expiration automatically.

- Email you when certificates are approaching expiration.
- Revoke expired certificates.

Procedure

	Command or Action	Purpose
Step 1	Configure Certificate Monitor Notifications, on page 124	Configure automatic certificate monitoring. The system periodically checks certificate statuses and emails you when a certificate is approaching expiration.
Step 2	Configure Certificate Revocation via OCSP, on page 125	Configure the OCSP so that the system revokes expired certificates automatically.

Configure Certificate Monitor Notifications

Configure automated certificate monitoring for Unified Communications Manager or the IM and Presence Service. The system periodically checks the status of certificates and emails you when a certificate is approaching expiration.

Note The **Cisco Certificate Expiry Monitor** network service must be running. This service is enabled by default, but you can confirm the service is running in Cisco Unified Serviceability by choosing **Tools** > **Control Center - Network Services** and verifying that the **Cisco Certificate Expiry Monitor Service** status is **Running**.

Procedure

Step 1 Log in to Cisco Unified OS Administration (for Unified Communications Manager certificate monitoring) or Cisco Unified IM and Presence Administration (for IM and Presence Service certificate monitoring).

Step 2 Choose **Security** > **Certificate Monitor**.

Step 3 In the **Notification Start Time** field, enter a numeric value. This value represents the number of days before certificate expiration where the system starts to notify you of the upcoming expiration.

Step 4 In the **Notification Frequency** fields, enter the frequency of notifications.

Step 5 Optional. Check the **Enable E-mail notification** check box to have the system send email alerts of upcoming certificate expirations..

Step 6 Check the **Enable LSC Monitoring** check box to include LSC certificates in the certificate status checks.

Step 7 In the **E-mail IDs** field, enter the email addresses where you want the system to send notifications. You can enter multiple email addresses separated by a semicolon.

Step 8 Click **Save**.

Note The certificate monitor service runs once every 24 hours by default. When you restart the certificate monitor service, it starts the service and then calculates the next schedule to run only after 24 hours. The interval does not change even when the certificate is close to the expiry date of seven days. It runs every 1 hour when the certificate either has expired or is going to expire in one day.

What to do next

Configure the Online Certificate Status Protocol (OCSP) so that the system revokes expired certificates automatically. For details, seeConfigure Certificate Revocation via OCSP, on page 125

Configure Certificate Revocation via OCSP

Enable the Online Certificate Status Protocol (OCSP) to check certificate status regularly and to revoke expired certificates automatically.

Before you begin

Make sure that your system has the certificates that are required for OCSP checks. You can use Root or Intermediate CA certificates that are configured with the OCSP response attribute or you can use a designated OCSP signing certificate that has been uploaded to the tomcat-trust.

Procedure

Step 1 Log in to Cisco Unified OS Administration (for Unified Communications Manager certificate revocation) or Cisco Unified IM and Presence Administration (for IM and Presence Service certificate revocation).

Step 2 Choose **Security** > **Certificate Revocation**.

Step 3 Check the **Enable OCSP** check box, and perform one of the following tasks:

- If you want to specify an OCSP responder for OCSP checks, select the **Use configured OCSP URI** button and enter the URI of the responder in the **OCSP Configured URI** field.
- If the certificate is configured with an OCSP responder URI, select the **Use OCSP URI from Certificate** button.

Step 4 Check the **Enable Revocation Check** check box.

Step 5 Complete the **Check Every** field with the interval period for revocation checks.

Step 6 Click **Save**.

Step 7 Optional. If you have CTI, IPsec or LDAP links, you must also complete these steps in addition to the above steps to enable OCSP revocation support for those long-lived connections:

a) From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

b) Under **Certificate Revocation and Expiry**, set the **Certificate Validity Check** parameter to **True**.

c) Configure a value for the **Validity Check Frequency** parameter.

Note The interval value of the **Enable Revocation Check** parameter in the **Certificate Revocation** window takes precedence over the value of the **Validity Check Frequency** enterprise parameter.

d) Click **Save**.

Troubleshoot Certificate Errors

Before you begin

If you encounter an error when you attempt to access Unified Communications Manager services from an IM and Presence Service node or IM and Presence Service functionality from a Unified Communications Manager node, the source of the issue is the tomcat-trust certificate. The error message `Connection to the Server cannot be established (unable to connect to Remote Node)` appears on the following Serviceability interface windows:

- **Service Activation**
- **Control Center - Feature Services**
- **Control Center - Network Services**

Use this procedure to help you resolve the certificate error. Start with the first step and proceed, if necessary. Sometime, you may only have to complete the first step to resolve the error; in other cases, you have to complete all the steps.

Procedure

Step 1 From Cisco Unified OS Administration, verify that the required tomcat-trust certificates are present: **Security** > **Certificate Management**.

If the required certificates are not present, wait 30 minutes before checking again.

Step 2 Choose a certificate to view its information. Verify that the content matches with the corresponding certificate on the remote node.

Step 3 From the CLI, restart the Cisco Intercluster Sync Agent service: **utils service restart Cisco Intercluster Sync Agent**.

Step 4 After the Cisco Intercluster Sync Agent service restarts, restart the Cisco Tomcat service: **utils service restart Cisco Tomcat**.

Step 5 Wait 30 minutes. If the previous steps do not address the certificate error and a tomcat-trust certificate is present, delete the certificate. After you delete the certificate, you must manually exchange it by downloading the Tomcat and Tomcat-ECDSA certificate for each node and uploading it to its peers as a tomcat-trust certificate.

Step 6 After the certificate exchange is complete, restart Cisco Tomcat on each affected server: **utils service restart Cisco Tomcat**.

CHAPTER 15

Manage Bulk Certificates

Manage Bulk Certificates

Use bulk certificate management if you want to share a set of certificates between clusters. This step is required for system functions that require established trust between clusters, such as extension mobility cross cluster.

Procedure

	Command or Action	Purpose
Step 1	Export Certificates, on page 127	This procedure creates a PKCS12 file that contains certificates for all nodes in the cluster.
Step 2	Import Certificates, on page 128	Import the certificates back into the home and remote (visiting) clusters.

Export Certificates

This procedure creates a PKCS12 file that contains certificates for all nodes in the cluster.

Procedure

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

Step 2 Configure the settings for a TFTP server that both the home and remote clusters can reach. See the online help for information about the fields and their configuration options.

Step 3 Click **Save**.

Step 4 Click **Export**.

Step 5 In the **Bulk Certificate Export** window, choose **All** for the **Certificate Type** field.

Step 6 Click **Export**.

Step 7 Click **Close**.

Note When the bulk certificate export is performed, the certificates are then uploaded to the remote cluster as follows:

- CAPF certificate gets uploaded as a CallManager-trust
- Tomcat certificate gets uploaded as a Tomcat-trust
- CallManager certificate gets uploaded as a CallManager-trust
- CallManager certificate gets uploaded as a Phone-SAST-trust
- ITLRecovery certificate gets uploaded as a PhoneSast-trust and CallManager-trust

The above steps are performed when certificates are self-signed and there is no common trust in another cluster. If there is a common trust or the same signer then the export of ALL certificates is not needed.

Import Certificates

Import the certificates back into the home and remote (visiting) clusters.

Note Import of certificate using bulk certificate management causes phones to reset.

Before you begin

Before the Import button appears, you must complete the following activities:

- Export the certificates from at least two clusters to the SFTP server.
- Consolidate the exported certificates.

Procedure

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

Step 2 From the **Certificate Type** drop-down list, choose **All**.

Step 3 Choose **Import**.

Note When the bulk certificate import is performed, the certificates are then uploaded to the remote cluster as follows:

- CAPF certificate gets uploaded as a CallManager-trust
- Tomcat certificate gets uploaded as a Tomcat-trust
- CallManager certificate gets uploaded as a CallManager-trust
- CallManager certificate gets uploaded as a Phone-SAST-trust
- ITLRecovery certificate gets uploaded as a PhoneSast-trust and CallManager-trust

Note The following types of certificates determines phones that are restarted:

- Callmanager - ALL phones only IF TFTP service is activated on the node the certificate belongs.
- TVS - SOME phones based on Callmanager group membership.
- CAPF - ALL phones only IF CAPF is activated.

CHAPTER 16

Manage IPSec Policies

IPsec Policies Overview

IPsec is a framework that ensures private, secure communications over IP networks through the use of cryptographic security services. IPsec policies are used to configure IPsec security services. The policies provide varying levels of protection for most traffic types in your network. You can configure IPsec policies to meet the security requirements of a computer, organizational unit (OU), domain, site, or global enterprise.

Configure IPsec Policies

Note

- Because any changes that you make to an IPsec policy during a system upgrade will be lost, do not modify or create IPsec policies during an upgrade.
- IPsec requires bidirectional provisioning, or one peer for each host (or gateway).
- When you provision the IPSec policy on two Unified Communications Manager nodes with one IPsec policy protocol set to “ANY” and the other IPsec policy protocol set to “UDP” or “TCP”, the validation can result in a false negative if run from the node that uses the “ANY” protocol.
- IPsec, especially with encryption, affects the performance of your system.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **IPSec Configuration**.

Step 2 Click **Add New**.

Step 3 Configure the fields on the **IPSEC Policy Configuration** window. See the online help for more information about the fields and their configuration options.

Step 4 Click **Save**.

Step 5 (Optional) To validate IPsec, choose **Services** > **Ping**, check the **Validate IPsec** check box, and then click **Ping**.

Manage IPsec Policies

Because any changes that you make to an IPsec policy during a system upgrade are lost, do not modify or create IPsec policies during an upgrade.

Caution Any changes that you make to the existing IPsec certificate because of hostname, domain, or IP address changes require you to delete the IPsec policies and recreate them, if certificate names are changed. If certificate names are unchanged, then after importing the remote node's regenerated certificate, the IPsec policies must be disabled and enabled.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **IPSEC Configuration**.

Step 2 To display, enable, or disable a policy, follow these steps:

a) Click the policy name.

b) To enable or disable the policy, check or uncheck the **Enable Policy** check box.

c) Click **Save**.

Step 3 To delete one or more policies, follow these steps:

a) Check the check box next to each policy that you want to delete.

You can click **Select All** to select all policies or **Clear All** to clear all the check boxes.

b) Click **Delete Selected**.

CHAPTER 17

Manage Credential Policies

Credential Policy and Authentication

The authentication function authenticates users, updates credential information, tracks and logs user events and errors, records credential change histories, and encrypts or decrypts user credentials for data storage.

The system always authenticates application user passwords and end user PINs against the Unified Communications Manager database. The system can authenticate end user passwords against the corporate directory or the database.

If your system is synchronized with the corporate directory, either the authentication function in Unified Communications Manager or lightweight directory access protocol (LDAP) can authenticate the password:

- With LDAP authentication enabled, user passwords and credential policies do not apply. These defaults are applied to users that are created with directory synchronization (DirSync service).
- When LDAP authentication is disabled, the system authenticates user credentials against the database. With this option, you can assign credential policies, manage authentication events, and administer passwords. End users can change passwords and PINs through the phone user interfaces.

Credential policies do not apply to operating system users or CLI users. These administrators use standard password verification procedures that the operating system supports.

After users are configured in the database, the system stores a history of user credentials in the database to prevent users from entering previous information when users are prompted to change their credentials.

JTAPI and TAPI Support for Credential Policies

Because the Cisco Unified Communications Manager Java telephony applications programming interface (JTAPI) and telephony applications programming interface (TAPI) support the credential policies that are assigned to application users, developers must create applications that respond to the password expiration, PIN expiration, and lockout return codes for credential policy enforcement.

Applications use an API to authenticate with the database or corporate directory, regardless of the authentication model that an application uses.

For more information about JTAPI and TAPI for developers, see the developer guides at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-programming-reference-guides-list.html.

Configure a Credential Policy

Credential policies apply to application users and end users. You assign a password policy to end users and application users and a PIN policy to end users. The Credential Policy Default Configuration lists the policy assignments for these groups. When you add a new user to the database, the system assigns the default policy. You can change the assigned policy and manage user authentication events.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Credential Policy**.

Step 2 Perform one of the following steps:

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

Step 3 Complete the fields in the **Credential Policy Configuration** window. See the online help for more information about the fields and their configuration settings.

Step 4 Click **Save**.

Configure a Credential Policy Default

At installation, Cisco Unified Communications Manager assigns a static default credential policy to user groups. It does not provide default credentials. Your system provides options to assign new default policies and to configure new default credentials and credential requirements for users.

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Credential Policy Default**.

Step 2 From the **Credential Policy** drop-down list box, choose the credential policy for this group.

Step 3 Enter the password in both the **Change Credential** and **Confirm Credential** configuration windows.

Step 4 Check the **User Cannot Change** check box if you do not want your users to be able to change this credential.

Step 5 Check the **User Must Change at Next Login** check box if you want to use this credential as a temporary credential that an end user must change the next time that they login.

Note Please note that, if you check this box, your users are unable to change PIN using Personal Directory service.

Step 6 If you do not want the credential to expire, check the **Does Not Expire** check box.

Step 7 Click **Save**.

Monitor Authentication Activity

The system shows the most current authentication results, such as last hack attempt time, and counts for failed logon attempts.

The system generates log file entries for the following credential policy events:

- Authentication success
- Authentication failure (bad password or unknown)
- Authentication failure because of
  - Administrative lock
  - Hack lock (failed logon lockouts)
  - Expired soft lock (expired credential)
  - Inactive lock (credential not used for some time)
  - User must change (credential set to user must change)
  - LDAP inactive (switching to LDAP authentication and LDAP not active)
- Successful user credential updates
- Failed user credential updates

Note If you use LDAP authentication for end user passwords, LDAP tracks only authentication successes and failures.

All event messages contain the string “ims-auth” and the user ID that is attempting authentication.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **End Users**.

Step 2 Enter search criteria, click **Find**, and then choose a user from the resulting list.

Step 3 Click **Edit Credential** to view the user's authentication activity.

What to do next

You can view log files with the Cisco Unified Real-Time Monitoring Tool (Unified RTMT). You can also collect captured events into reports. For detailed steps about how to use Unified RTMT, see the *Cisco Unified*

Real-Time Monitoring Tool Administration Guide at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Configuring Credential Caching

Enable credential caching to increase system efficiency. Your system does not have to perform a database lookup or invoke a stored procedure for every single login request. An associated credential policy is not enforced until the caching duration expires.

This setting applies to all Java applications that invoke user authentication.

Procedure

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

Step 2 Perform the following tasks as needed:

- Set the **Enable Caching** enterprise parameter to **True**. With this parameter enabled, Cisco Unified Communications Manager uses cached credentials for up to 2 minutes.
- Set the **Enable Caching** enterprise parameter to **False** to disable caching, so that the system does not use cached credentials for authentication. The system ignores this setting for LDAP authentication. Credential caching requires a minimal amount of additional memory per user.

Step 3 Click **Save**.

PART VI

Disaster Recovery

CHAPTER 18

Back Up the System

Backup Overview

Cisco recommends performing regular backups. You can use the Disaster Recovery System (DRS) to do a full data backup for all servers in a cluster. You can set up automatic backups or invoke a backup at any time.

The Disaster Recovery System performs a cluster-level backup, which means that it collects backups for all servers in a Cisco Unified Communications Manager cluster to a central location and archives the backup data to physical storage device. Backup files are encrypted and can be opened only by the system software.

DRS restores its own settings (backup device settings and schedule settings) as part of the platform backup/restore. DRS backs up and restores the drfDevice.xml and drfSchedule.xml files. When the server is restored with these files, you do not need to reconfigure DRS backup device and schedule.

When you perform a system data restoration, you can choose which nodes in the cluster you want to restore.

The Disaster Recovery System includes the following capabilities:

- A user interface for performing backup and restore tasks.
- A distributed system architecture for performing backup functions.
- Scheduled backups or manual (user-invoked) backups.
- It archives backups to a remote sftp server.

Backup Prerequisites

- Make sure that you meet the version requirements:
  - All Cisco Unified Communications Manager cluster nodes must be running the same version of the Cisco Unified Communications Manager application.

- All IM and Presence Service cluster nodes must be running the same version of the IM and Presence Service application.
- The software version saved in the backup file must match the version that is running on the cluster nodes.

The entire version string must match. For example, if the IM and Presence database publisher node is at version 11.5.1.10000-1, then all IM and Presence subscriber nodes must be 11.5.1.10000-1, and the backup file must also be must be 11.5.1.10000-1. If you try to restore the system from a backup file that does not match the current version, the restore will fail. Ensure that you backup the system whenever you upgrade the software version so that the version saved in the backup file matches the version that is running on the cluster nodes.

- Be aware the DRS encryption depends on the cluster security password. When running the backup, DRS generates a random password for encryption and then encrypts the random password with the cluster security password. If the cluster security password ever gets changed between the backup and this restore, you will need to know what the password was at the time of the backup in order to use that backup file to restore your system or take a backup immediately after the security password change/reset.
- If you want to back up to a remote device, make sure that you have an SFTP server set up. For more information on the available SFTP servers, see SFTP Servers for Remote Backups , on page 146

Backup Task Flow

Complete these tasks to configure and run a backup. Do not perform any OS Administration tasks while a backup is running. This is because Disaster Recovery System blocks all OS Administration requests by locking platform API. However, Disaster Recovery System does not block most CLI commands, because only the CLI-based upgrade commands use the Platform API locking package.

Procedure

	Command or Action	Purpose
Step 1	Configure Backup Devices, on page 141	Specify the devices on which to back up data.
Step 2	Estimate Size of Backup File, on page 142	Estimate size of backup file created on the SFTP device.
Step 3	Choose one of the following options: • Configure a Scheduled Backup, on page 142 • Start a Manual Backup, on page 143	Create a backup schedule to back up data on a schedule. Optionally, run a manual backup.
Step 4	View Current Backup Status, on page 144	Optional. Check the Status of the Backup. While a backup is running, you can check the status of the current backup job.
Step 5	View Backup History, on page 145	Optional. View Backup History

Configure Backup Devices

You can configure up to 10 backup devices. Perform the following steps to configure the location where you want to store backup files.

Before you begin

- Ensure you have write access to the directory path in the SFTP server to store the backup file.
- Ensure that the username, password, server name, and directory path are valid as the DRS Master Agent validates the configuration of the backup device.

Note Schedule backups during periods when you expect less network traffic.

Procedure

Step 1 From Disaster Recovery System, select **Backup** > **Backup Device**.

Step 2 In the **Backup Device List** window, do either of the following:

- To configure a new device, click **Add New**.
- To edit an existing backup device, enter the search criteria, click Find, and **Edit Selected**.
- To delete a backup device, select it in the **Backup Device** list and click **Delete Selected**.

You cannot delete a backup device that is configured as the backup device in a backup schedule.

Step 3 Enter a backup name in the **Backup Device Name** field.

The backup device name contains only alphanumeric characters, spaces (), dashes (-) and underscores (_). Do not use any other characters.

Step 4 In the **Select Destination** area, under **Network Directory** perform the following:

- In the **Host name/IP Address** field, enter the hostname or IP address for the network server.
- In the **Path name** field, enter the directory path where you want to store the backup file.
- In the **User name** field, enter a valid username.
- In the **Password** field, enter a valid password.
- From the **Number of backups to store on Network Directory** drop-down list, choose the required number of backups.

Step 5 Click **Save**.

What to do next

Estimate Size of Backup File, on page 142

Estimate Size of Backup File

Cisco Unified Communications Manager will estimate the size of the backup tar, only if a backup history exists for one or more selected features.

The calculated size is not an exact value but an estimated size of the backup tar. Size is calculated based on the actual backup size of a previous successful backup and may vary if the configuration changed since the last backup.

You can use this procedure only when the previous backups exist and not when you back up the system for the first time.

Follow this procedure to estimate the size of the backup tar that is saved to a SFTP device.

Procedure

Step 1 From the Disaster Recovery System, select **Backup** > **Manual Backup**.

Step 2 In the **Select Features** area, select the features to back up.

Step 3 Click **Estimate Size** to view the estimated size of backup for the selected features.

What to do next

Perform one of the following procedures to backup your system:

- Configure a Scheduled Backup, on page 142
- Start a Manual Backup, on page 143

Configure a Scheduled Backup

You can create up to 10 backup schedules. Each backup schedule has its own set of properties, including a schedule for automatic backups, the set of features to back up, and a storage location.

Be aware that your backup .tar files are encrypted by a randomly generated password. This password is then encrypted by using the cluster security password and gets saved along with the backup .tar files. You must remember this security password or take a backup immediately after the security password change or reset.

Caution Schedule backups during off-peak hours to avoid call processing interruptions and impact to service.

Before you begin

Configure Backup Devices, on page 141

Procedure

Step 1 From the Disaster Recovery System, choose **Backup Scheduler**.

Step 2 In the **Schedule List** window, do one of the following steps to add a new schedule or edit an existing schedule.

- To create a new schedule, click **Add New**.
- To configure an existing schedule, click the name in the Schedule List column.

Step 3 In the **scheduler** window, enter a schedule name in the **Schedule Name** field.

Note You cannot change the name of the default schedule.

Step 4 Select the backup device in the **Select Backup Device** area.

Step 5 Select the features to back up in the **Select Features** area. You must choose at least one feature.

Step 6 Choose the date and time when you want the backup to begin in the **Start Backup at** area.

Step 7 Choose the frequency at which you want the backup to occur in the **Frequency** area. The frequency can be set to Once Daily, Weekly, and Monthly. If you choose **Weekly**, you can also choose the days of the week when the backup will occur.

Tip To set the backup frequency to **Weekly**, occurring Tuesday through Saturday, click **Set Default**.

Step 8 To update these settings, click **Save**.

Step 9 Choose one of the following options:

- To enable the selected schedules, click **Enable Selected Schedules**.
- To disable the selected schedules, click **Disable Selected Schedules**.
- To delete the selected schedules, click **Delete Selected**.

Step 10 To enable the schedule, click **Enable Schedule**.

The next backup occurs automatically at the time that you set.

Note Ensure that all servers in the cluster are running the same version of Cisco Unified Communications Manager or Cisco IM and Presence Service and are reachable through the network. Servers that are not reachable at the time of the scheduled backup will not get backed up.

What to do next

Perform the following procedures:

- Estimate Size of Backup File, on page 142
- (Optional) View Current Backup Status, on page 144

Start a Manual Backup

Before you begin

- Ensure that you use a network device as the storage location for the backup files. Virtualized deployments of Unified Communications Manager do not support the use of tape drives to store backup files.
- Ensure that all cluster nodes have the same installed version of Cisco Unified Communications Manager or IM and Presence Service.

- The backup process can fail due to non availability of space on a remote server or due to interruptions in the network connectivity. You need to start a fresh backup after addressing the issues that caused the backup to fail.
- Ensure that there are no network interruptions.
- Configure Backup Devices, on page 141
- Estimate Size of Backup File, on page 142
- Make sure that you have a record of the cluster security password. If the cluster security password changes after you complete this backup, you will need to know the password or you will not be able to use the backup file to restore your system.

Note While a backup is running, you cannot perform any tasks in Cisco Unified OS Administration or Cisco Unified IM and Presence OS Administration because Disaster Recovery System locks the platform API to block all requests. However, Disaster Recovery System does not block most CLI commands because only the CLI-based upgrade commands use the Platform API locking package.

Procedure

Step 1 From the Disaster Recovery System, select **Backup** > **Manual Backup**.

Step 2 In the **Manual Backup** window, select a backup device from the **Backup Device Name** area.

Step 3 Choose a feature from the **Select Features** area.

Step 4 Click **Start Backup.**

What to do next

(Optional) View Current Backup Status, on page 144

View Current Backup Status

Perform the following steps to check the status of the current backup job.

Caution Be aware that if the backup to the remote server is not completed within 20 hours, the backup session times out and you must begin a fresh backup.

Procedure

Step 1 From the Disaster Recovery System, select **Backup** > **Current Status**.

Step 2 To view the backup log file, click the log filename link.

Step 3 To cancel the current backup, click **Cancel Backup**.

Note The backup cancels after the current component completes its backup operation.

What to do next

View Backup History, on page 145

View Backup History

Perform the following steps to view the backup history.

Procedure

Step 1 From the Disaster Recovery System, select **Backup** > **History**.

Step 2 From the **Backup History** window, you can view the backups that you have performed, including filename, backup device, completion date, result, version, features that are backed up, and failed features.

Note The **Backup History** window displays only the last 20 backup jobs.

Backup Interactions and Restrictions

Backup Restrictions

The following restrictions apply to backups:

Table 6: Backup Restrictions

Restriction	Description
Cluster Security Password	We recommend that you run a backup whenever you change the cluster security password. Backup encryption uses the cluster security password to encrypt data on the backup file. If you edit the cluster security password after a backup file is created, you will not be able to use that backup file to restore data unless you remember the old password.

Restriction	Description
Certificate Management	The Disaster Recovery System (DRS) uses an SSL-based communication between the Master Agent and the Local Agent for authentication and encryption of data between the Cisco Unified Communications Manager cluster nodes. DRS makes use of the IPsec certificates for its Public/Private Key encryption. Be aware that if you delete the IPSEC truststore(hostname.pem) file from the Certificate Management pages, then DRS will not work as expected. If you delete the IPSEC-trust file manually, you must ensure that you upload the IPSEC certificate to the IPSEC-trust. For more details, see the "Certificate management" section in the *Security Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

SFTP Servers for Remote Backups

To back up data to a remote device on the network, you must have an SFTP server that is configured. For internal testing, Cisco uses the SFTP Server on Cisco Prime Collaboration Deployment (PCD) which is provided by Cisco, and which is supported by Cisco TAC. Refer to the following table for a summary of the SFTP server options:

Use the information in the following table to determine which SFTP server solution to use in your system.

Table 7: SFTP Server Information

SFTP Server	Information
SFTP Server on Cisco Prime Collaboration Deployment	This server is the only SFTP server that is provided and tested by Cisco, and fully supported by Cisco TAC. Version compatibility depends on your version of Unified Communications Manager and Cisco Prime Collaboration Deployment. See the *Cisco Prime Collaboration Deployment Administration Guide* before you upgrade its version (SFTP) or Unified Communications Manager to ensure that the versions are compatible.
SFTP Server from a Technology Partner	These servers are third party provided and third party tested. Version compatibility depends on the third party test. See the Technology Partner page if you upgrade their SFTP product and/or upgrade Unified Communications Manager for which versions are compatible: https://marketplace.cisco.com

SFTP Server	Information
SFTP Server from another Third Party	These servers are third party provided and are not officially supported by Cisco TAC. Version compatibility is on a best effort basis to establish compatible SFTP versions and Unified Communications Manager versions. **Note** These products have not been tested by Cisco and we cannot guarantee functionality. Cisco TAC does not support these products. For a fully tested and supported SFTP solution, use Cisco Prime Collaboration Deployment or a Technology Partner.

Cipher Support

For Unified Communications Manager 11.5, Unified Communications Manager advertises the following CBC and CTR ciphers for SFTP connections:

- aes128-cbc
- 3des-cbc
- aes128-ctr
- aes192-ctr
- aes256-ctr

Note Make sure that the backup SFTP Server supports one of these ciphers to communicate with Unified Communications Manager.

From Unified Communications Manager 12.0 release onwards, CBC ciphers are not supported. Unified Communications Manager supports and advertises only the following CTR ciphers:

- aes256-ctr
- aes128-ctr
- aes192-ctr

Note Make sure that the backup SFTP Server supports one of these CTR ciphers to communicate with Unified Communications Manager.

CHAPTER 19

Restore the System

Restore Overview

The Disaster Recovery System (DRS) provides a wizard to walk you through the process of restoring your system.

The backup files are encrypted and only the DRS system can open them to restore the data. The Disaster Recovery System includes the following capabilities:

- A user interface for performing restore tasks.
- A distributed system architecture for performing restore functions.

Master Agent

The system automatically starts the Master Agent service on each node of the cluster, but the Master Agent is functional only on the publisher node. The Master Agents on the subscriber nodes do not perform any functions.

Local Agents

The server has a Local Agent to perform backup and restore functions.

Each node in a Cisco Unified Communications Manager cluster, including the node that contains the Master Agent, must have its own Local Agent to perform backup and restore functions.

Note By default, a Local Agent automatically gets started on each node of the cluster, including IM and Presence nodes.

Restore Prerequisites

- Make sure that you meet the version requirements:
  - All Cisco Unified Communications Manager cluster nodes must be running the same version of the Cisco Unified Communications Manager application.
  - All IM and Presence Service cluster nodes must be running the same version of the IM and Presence Service application.
  - The version saved in the backup file must match the version that is running on the cluster nodes.

  The entire version string must match. For example, if the IM and Presence database publisher node is at version 11.5.1.10000-1, then all IM and Presence subscriber nodes must be 11.5.1.10000-1, and the backup file must also be must be 11.5.1.10000-1. If you try to restore the system from a backup file that does not match the current version, the restore will fail.
- Make sure that the IP address, hostname, DNS configuration and deployment type for the server matches the IP address, hostname, DNS configuration and deployment type that are stored on the backup file.
- If you have changed the cluster security password since the backup was run, make sure that you have a record of the old password, or the restore will fail.

Restore Task Flow

During the restore process, do not perform any tasks with Cisco Unified Communications Manager OS Administration or Cisco Unified IM and Presence OS Administration.

Procedure

	Command or Action	Purpose
Step 1	Restore the First Node Only, on page 151	(Optional) Use this procedure only to restore the first publisher node in the cluster.
Step 2	Restore Subsequent Cluster Node, on page 153	(Optional) Use this procedure to restore the subscriber nodes in a cluster.
Step 3	Restore Cluster in One Step After Publisher Rebuilds, on page 154	(Optional) Follow this procedure to restore the entire cluster in one step if the publisher has already been rebuilt.
Step 4	Restore Entire Cluster, on page 155	(Optional) Use this procedure to restore all nodes in the cluster, including the publisher node. If a major hard drive failure or upgrade

	Command or Action	Purpose
		occurs, or in the event of a hard drive migration, you may need to rebuild all nodes in the cluster.
Step 5	Restore Node Or Cluster to Last Known Good Configuration, on page 157	(Optional) Use this procedure only if you are restoring a node to a last known good configuration. Do not use this after a hard drive failure or other hardware failure.
Step 6	Restart a Node, on page 157	Use this procedure to restart a node.
Step 7	Check Restore Job Status, on page 158	(Optional) Use this procedure to check the restore job status.
Step 8	View Restore History, on page 158	(Optional) Use this procedure to view the restore history.

Restore the First Node Only

If you are restoring the first node after a rebuild, you must configure the backup device.

This procedure is applicable to the Cisco Unified Communications Manager First Node, also known as the publisher node. The other Cisco Unified Communications Manager nodes and all the IM and Presence Service nodes are considered as secondary nodes or subscribers.

Before you begin

If there is an IM and Presence Service node in the cluster, ensure that it is running and accessible when you restore the first node. This is required so that a valid backup file can be found during the procedure.

Procedure

Step 1 From the Disaster Recovery System, choose **Restore** > **Restore Wizard**.

Step 2 In the **Restore Wizard Step 1** window, **Select Backup Device** area, select the appropriate backup device to restore.

Step 3 Click **Next**.

Step 4 In the **Restore Wizard Step 2** window, select the backup file you want to restore.

Note The backup filename indicates the date and time that the system created the backup file.

Step 5 Click **Next**.

Step 6 In the **Restore Wizard Step 3** window, click **Next**.

Step 7 Choose the features that you want to restore.

Note The features that you have selected for backup will be displayed.

Step 8 Click **Next**. The Restore Wizard Step 4 window displays.

Step 9 Select the Perform file integrity check using the SHA1 Message Digest checkbox if you want to run a file integrity check.

Note The file integrity check is optional and is only needed in the case of SFTP backups.

Be aware that the file integrity check process consumes a significant amount of CPU and network bandwidth, which slows down the restore process.

Step 10 Select the node to restore.

Step 11 Click **Restore** to restore the data.

Step 12 Click **Next**.

Step 13 When you are prompted to select the nodes to restore, choose only the first node (the publisher).

Caution Do not select the subsequent (subscriber) nodes in this condition as this will result in failure of the restore attempt.

Step 14 (Optional) From the **Select Server Name** drop-down list, select the subscriber node from which you want to restore the publisher database. Ensure that the subscriber node that you chose is in-service and connected to the cluster.
The Disaster Recovery System restores all non database information from the backup file and pulls the latest database from the chosen subscriber node.

Note This option appears only if the backup file that you selected includes the CCMDB database component. Initially, only the publisher node is fully restored, but when you perform Step 14 and restart the subsequent cluster nodes, the Disaster Recovery System performs database replication and fully synchronizes all cluster node databases. This ensures that all cluster nodes are using current data.

Step 15 Click **Restore**.

Step 16 Your data is restored on the publisher node. Depending on the size of your database and the components that you choose to restore, the system can require a few hours to restore.

Note Restoring the first node restores the whole Cisco Unified Communications Manager database to the cluster. This may take up to several hours based on number of nodes and size of database that is being restored. Depending on the size of your database and the components that you choose to restore, the system can require a few hours to restore.

Step 17 When the **Percentage Complete** field on the **Restore Status** window, shows 100%, restart the server. Restart of all the nodes in the cluster is required in case of restoring only to the first node. Ensure that you restart the first node before you restart the subsequent nodes. For information about how to restart the server, see the What to Do Next section.

Note If you are restoring a Cisco Unified Communications Manager node only, the Cisco Unified Communications Manager and IM and Presence Service cluster must be restarted.

If you are restoring an IM and Presence Service Publisher node only, the IM and Presence Service cluster must be restarted.

What to do next

- (Optional) To view the status of the restore, see Check Restore Job Status, on page 158
- To restart a node, see Restart a Node, on page 157

Restore Subsequent Cluster Node

This procedure is applicable to the Cisco Unified Communications Manager subscriber (subsequent) nodes only. The first Cisco Unified Communications Manager node installed is the publisher node. All other Cisco Unified Communications Manager nodes, and all IM and Presence Service nodes are subscriber nodes.

Follow this procedure to restore one or more Cisco Unified Communications Manager subscriber nodes in the cluster.

Before you begin

Before you perform a restore operation, ensure that the hostname, IP address, DNS configuration, and deployment type of the restore matches the hostname, IP address, DNS configuration, and deployment type of the backup file that you want to restore. Disaster Recovery System does not restore across different hostnames, IP addresses, DNS configurations and deployment types.

Ensure that the software version that is installed on the server matches the version of the backup file that you want to restore. Disaster Recovery System supports only matching software versions for restore operations. If you are restoring the subsequent nodes after a rebuild, you must configure the backup device.

Procedure

Step 1 From the Disaster Recovery System, select **Restore** > **Restore Wizard**.

Step 2 In the **Restore Wizard Step 1** window, **Select Backup Device** area, choose the backup device from which to restore.

Step 3 Click **Next**.

Step 4 In the **Restore Wizard Step 2** window, select the backup file that you want to restore.

Step 5 Click **Next**.

Step 6 In the **Restore Wizard Step 3** window, select the features that you want to restore.

Note Only the features that were backed up to the file that you chose display.

Step 7 Click **Next**. The Restore Wizard Step 4 window displays.

Step 8 In the **Restore Wizard Step 4** window, when you are prompted to choose the nodes to restore, select only the subsequent nodes.

Step 9 Click **Restore**.

Step 10 Your data is restored on the subsequent nodes. For more information about how to view the status of the restore, see the What to Do Next section.

Note During the restore process, do not perform any tasks with Cisco Unified Communications Manager Administration or User Options.

Step 11 When the **Percentage Complete** field on the **Restore Status** window shows 100%, restart the secondary servers you just restored. Restart of all the nodes in the cluster is required in case of restoring only to the first node. Ensure that you restart the first node before you restart the subsequent nodes. For information about how to restart the server, see the What to Do Next section.

Note If the IM and Presence Service first node is restored. Ensure to restart the IM and Presence Service first node before you restart the IM and Presence Service subsequent nodes.

What to do next

- (Optional) To view the status of the restore, see Check Restore Job Status, on page 158
- To restart a node, see Restart a Node, on page 157

Restore Cluster in One Step After Publisher Rebuilds

Depending on the size of your database and the components that you choose to restore, the system can require a few hours to restore. Follow this procedure to restore the entire cluster in one step if the publisher has already been rebuilt or freshly installed.

Procedure

Step 1 From the Disaster Recovery System, select **Restore** > **Restore Wizard**.

Step 2 In the **Restore Wizard Step 1** window **Select Backup Device** area, choose the backup device from which to restore.

Step 3 Click **Next**.

Step 4 In the **Restore Wizard Step 2** window, select the backup file that you want to restore.

The backup filename indicates the date and time that the system created the backup file.

Choose only the backup file of the cluster from which you want to restore the entire cluster.

Step 5 Click **Next**.

Step 6 In the **Restore Wizard Step 3** window, select the features that you want to restore.

The screen displays only those features that were saved to the backup file.

Step 7 Click **Next**.

Step 8 In the **Restore Wizard Step 4** window, click **One-Step Restore**.

This option appears on **Restore Wizard Step 4** window only if the backup file selected for restore is the backup file of the cluster and the features chosen for restore includes the feature(s) that is registered with both publisher and subscriber nodes. For more information, see Restore the First Node Only, on page 151 and Restore Subsequent Cluster Node, on page 153.

Note If a status message indicates that *Publisher has failed to become cluster aware. Cannot start one-step restore*, you need to restore the publisher node and then the subscriber node. See the Related topics for more information.

This option allows the publisher to become cluster aware and will take five minutes to do so. Once you click on this option, a status message displays as “Please wait for 5 minutes until Publisher becomes cluster aware and do not start any backup or restore activity in this time period”.

After the delay, if the publisher becomes cluster aware, a status message displays as “Publisher has become cluster aware. Please select the servers and click on Restore to start the restore of entire cluster”.

After the delay, if the publisher has not become cluster aware, a status message displays as "Publisher has failed to become cluster aware. Cannot start one-step restore. Please go ahead and do a normal two-step restore." To restore the whole cluster in two-step (publisher and then subscriber), perform the steps mentioned in Restore the First Node Only, on page 151 and Restore Subsequent Cluster Node, on page 153.

Step 9 When you are prompted to choose the nodes to restore, choose all the nodes in the cluster.

The Disaster Recovery System restores the Cisco Unified Communications Manager database (CCMDB) on subsequent nodes automatically when you restore a first node. This may take up to several hours based on number of nodes and size of that database that is being restored.

Step 10 Click **Restore**.
Your data is restored on all the nodes of the cluster.

Step 11 When the **Percentage Complete** field on the **Restore Status window** shows 100%, restart the server. Restart of all the nodes in the cluster is required in case of restoring only to the first node. Ensure that you restart the first node before you restart the subsequent nodes. For information about how to restart the server, see the What to Do Next section.

What to do next

- (Optional) To view the status of the restore, see Check Restore Job Status, on page 158
- To restart a node, see Restart a Node, on page 157

Related Topics

Restore the First Node Only, on page 151
Restore Subsequent Cluster Node, on page 153

Restore Entire Cluster

If a major hard drive failure or upgrade occurs, or in the event of a hard drive migration, you have to rebuild all nodes in the cluster. Follow these steps to restore an entire cluster.

If you are doing most other types of hardware upgrades, such as replacing a network card or adding memory, you do not need to perform this procedure.

Procedure

Step 1 From Disaster Recovery System, select **Restore** > **Restore Wizard**.

Step 2 In the **Select Backup Device** area, select the appropriate backup device to restore.

Step 3 Click **Next**.

Step 4 In the **Restore Wizard Step 2** window, select the backup file you want to restore.

Note The backup filename indicates the date and time that the system created the backup file.

Step 5 Click **Next**.

Step 6 In the **Restore Wizard Step 3** window, click **Next**.

Step 7 In the **Restore Wizard Step 4** window, select all the nodes when prompted to choose restore nodes.

Step 8 Click **Restore** to restore the data.

The Disaster Recovery System restores the Cisco Unified Communications Manager database (CCMDB) on subsequent nodes automatically when you restore a first node. This may take up to several hours based on number of nodes and size of that database.

Data is restored on the all the nodes.

Note During the restore process, do not perform any tasks with Cisco Unified Communications Manager Administration or User Options.

Depending on the size of your database and the components that you choose to restore, the system can require a few hours to restore.

Step 9 Restart the server once the restoration process is completed. See the What to Do Next section for more information about how to restart the server.

Note Make sure that you restart the first node before you restart the subsequent nodes.

After the first node has restarted and is running the restored version of Cisco Unified Communications Manager, restart the subsequent nodes.

Step 10 Replication will be setup automatically after cluster reboot. Check the Replication Status value on all nodes by using the “utils dbreplication runtimestate” CLI command as described in the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*. The value on each node should equal 2.

Note Database replication on the subsequent nodes may take enough time to complete after the subsequent node restarts, depending on the size of the cluster.

Tip If replication does not set up properly, use the "utils dbreplication rebuild" CLI command as described in the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

What to do next

- (Optional) To view the status of the restore, see Check Restore Job Status, on page 158
- To restart a node, see Restart a Node, on page 157

Restore Node Or Cluster to Last Known Good Configuration

Follow this procedure to restore node or cluster to last known good configuration.

Before you begin

- Ensure that the restore file contains the hostname, IP address, DNS configuration, and deployment type that is configured in the backup file.
- Ensure that the Cisco Unified Communications Manager version installed on the server matches the version of the backup file that you want to restore.
- Ensure this procedure is used only to restore node to a last known good configuration.

Procedure

Step 1 From the Disaster Recovery System, choose **Restore** > **Restore Wizard**.

Step 2 In the **Select Backup Device** area, select the appropriate backup device to restore.

Step 3 Click **Next**.

Step 4 In the **Restore Wizard Step 2** window, select the backup file you want to restore.

Note The backup filename indicates the date and time that the system created the backup file.

Step 5 Click **Next**.

Step 6 In the **Restore Wizard Step 3** window, click **Next**.

Step 7 Select the appropriate node, when prompted to choose restore nodes.
Data is restored on the chosen nodes.

Step 8 Restart all nodes in the cluster. Restart the first Cisco Unified Communications Manager node before restarting the subsequent Cisco Unified Communications Manager nodes. If the cluster also has Cisco IM and Presence nodes, restart the first Cisco IM and Presence node before restarting the subsequent IM and Presence nodes. See the What to Do Next section for more information.

Restart a Node

You must restart a node after you restore data.

If you are restoring a publisher node (first node), you must restart the publisher node first. Restart subscriber nodes only after the publisher node has restarted and is successfully running the restored version of the software.

Note Do not restart IM and Presence subscriber nodes if the CUCM publisher node is offline. In such cases, the node services will fail to start because the subscriber node is unable to connect to the CUCM publisher.

Caution This procedure causes the system to restart and become temporarily out of service.

Perform this procedure on every node in the cluster that you need to restart.

Procedure

Step 1 From Cisco Unified OS Administration, select **Settings** > **Version**.

Step 2 To restart the node, click **Restart**.

Step 3 Replication will be setup automatically after cluster reboot. Check the Replication Status value on all nodes by using the **utils dbreplication runtimestate** CLI command. The value on each node should be equal 2. See the Related Topics section below to find information about CLI commands.

If replication does not set up properly, use the **utils dbreplication reset** CLI command as described in the *Command Line Reference Guide for Cisco Unified Communications Solutions*. See the Related Topics section below to find information about CLI commands.

Note Database replication on the subsequent nodes may take several hours to complete after the subsequent nodes restart, depending on the size of the cluster.

What to do next

(Optional) To view the status of the restore, see Check Restore Job Status, on page 158.

Related Topics

Cisco Unified Communications Manager (CallManager) Command References

Check Restore Job Status

Follow this procedure to check the restore job status.

Procedure

Step 1 From the Disaster Recovery System, select **Restore** > **Current Status**.

Step 2 In the **Restore Status** window, click the log filename link to view the restore status.

View Restore History

Perform the following steps to view the restore history.

Procedure

Step 1 From Disaster Recovery System, choose **Restore** > **History**.

Step 2 From the **Restore History** window, you can view the restores that you have performed, including filename, backup device, completion date, result, version, features that were restored, and failed features.

The **Restore History** window displays only the last 20 restore jobs.

Data Authentication

Trace Files

The following trace file locations are used during troubleshooting or while collecting the logs.

Trace files for the Master Agent, the GUI, each Local Agent, and the JSch library get written to the following locations:

- For the Master Agent, find the trace file at platform/drf/trace/drfMA0*
- For each Local Agent, find the trace file at platform/drf/trace/drfLA0*
- For the GUI, find the trace file at platform/drf/trace/drfConfLib0*
- For the JSch, find the trace file at platform/drf/trace/drfJSch*

For more information, see the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-command-reference-list.html.

Command Line Interface

The Disaster Recovery System also provides command line access to a subset of backup and restore functions, as shown in the following table. For more information on these commands and on using the command line interface, see the *Command Line Interface Reference Guide* for Cisco Unified Communications Solutions at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-command-reference-list.html.

Table 8: Disaster Recovery System Command Line Interface

Command	Description
utils disaster_recovery estimate_tar_size	Displays estimated size of backup tar from SFTP/Local device and requires one parameter for feature list
utils disaster_recovery backup	Starts a manual backup by using the features that are configured in the Disaster Recovery System interface
utils disaster_recovery jschLogs	Enables or disables JSch library logging

Command	Description
utils disaster_recovery restore	Starts a restore and requires parameters for backup location, filename, features, and nodes to restore
utils disaster_recovery status	Displays the status of ongoing backup or restore job
utils disaster_recovery show_backupfiles	Displays existing backup files
utils disaster_recovery cancel_backup	Cancels an ongoing backup job
utils disaster_recovery show_registration	Displays the currently configured registration
utils disaster_recovery device add	Adds the network device
utils disaster_recovery device delete	Deletes the device
utils disaster_recovery device list	Lists all the devices
utils disaster_recovery schedule add	Adds a schedule
utils disaster_recovery schedule delete	Deletes a schedule
utils disaster_recovery schedule disable	Disables a schedule
utils disaster_recovery schedule enable	Enables a schedule
utils disaster_recovery schedule list	Lists all the schedules
utils disaster_recovery backup	Starts a manual backup by using the features that are configured in the Disaster Recovery System interface.
utils disaster_recovery restore	Starts a restore and requires parameters for backup location, filename, features, and nodes to restore.
utils disaster_recovery status	Displays the status of ongoing backup or restore job.
utils disaster_recovery show_backupfiles	Displays existing backup files.
utils disaster_recovery cancel_backup	Cancels an ongoing backup job.
utils disaster_recovery show_registration	Displays the currently configured registration.

Alarms and Messages

Alarms and Messages

The Disaster Recovery System issues alarms for various errors that could occur during a backup or restore procedure. The following table provides a list of Cisco Disaster Recovery System alarms.

Table 9: Disaster Recovery System Alarms and Messages

Alarm Name	Description	Explanation
DRFBackupDeviceError	DRF backup process has problems accessing device.	DRS backup process encountered errors while it was accessing device.
DRFBackupFailure	Cisco DRF Backup process failed.	DRS backup process encountered errors.
DRFBackupInProgress	New backup cannot start while another backup is still running	DRS cannot start new backup while another backup is still running.
DRFInternalProcessFailure	DRF internal process encountered an error.	DRS internal process encountered an error.
DRFLA2MAFailure	DRF Local Agent cannot connect to Master Agent.	DRS Local Agent cannot connect to Master Agent.
DRFLocalAgentStartFailure	DRF Local Agent does not start.	DRS Local Agent might be down.
DRFMA2LAFailure	DRF Master Agent does not connect to Local Agent.	DRS Master Agent cannot connect to Local Agent.
DRFMABackupComponentFailure	DRF cannot back up at least one component.	DRS requested a component to back up its data; however, an error occurred during the backup process, and the component did not get backed up.
DRFMABackupNodeDisconnect	The node that is being backed up disconnected from the Master Agent prior to being fully backed up.	While the DRS Master Agent was running a backup operation on a Cisco Unified Communications Manager node, the node disconnected before the backup operation completed.
DRFMARestoreComponentFailure	DRF cannot restore at least one component.	DRS requested a component to restore its data; however, an error occurred during the restore process, and the component did not get restored.
DRFMARestoreNodeDisconnect	The node that is being restored disconnected from the Master Agent prior to being fully restored.	While the DRS Master Agent was running a restore operation on a Cisco Unified Communications Manager node, the node disconnected before the restore operation completed.
DRFMasterAgentStartFailure	DRF Master Agent did not start.	DRS Master Agent might be down.

Alarm Name	Description	Explanation
DRFNoRegisteredComponent	No registered components are available, so backup failed.	DRS backup failed because no registered components are available.
DRFNoRegisteredFeature	No feature got selected for backup.	No feature got selected for backup.
DRFRestoreDeviceError	DRF restore process has problems accessing device.	DRS restore process cannot read from device.
DRFRestoreFailure	DRF restore process failed.	DRS restore process encountered errors.
DRFSftpFailure	DRF SFTP operation has errors.	Errors exist in DRS SFTP operation.
DRFSecurityViolation	DRF system detected a malicious pattern that could result in a security violation.	The DRF Network Message contains a malicious pattern that could result in a security violation like code injection or directory traversal. DRF Network Message has been blocked.
DRFTruststoreMissing	The IPsec truststore is missing on the node.	The IPsec truststore is missing on the node. DRF Local Agent cannot connect to Master Agent.
DRFUnknownClient	DRF Master Agent on the Pub received a Client connection request from an unknown server outside the cluster. The request has been rejected.	The DRF Master Agent on the Pub received a Client connection request from an unknown server outside the cluster. The request has been rejected.
DRFBackupCompleted	DRF backup completed successfully.	DRF backup completed successfully.
DRFRestoreCompleted	DRF restore completed successfully.	DRF restore completed successfully.
DRFNoBackupTaken	DRF did not find a valid backup of the current system.	DRF did not find a valid backup of the current system after an Upgrade/Migration or Fresh Install.
DRFComponentRegistered	DRF successfully registered the requested component.	DRF successfully registered the requested component.
DRFRegistrationFailure	DRF Registration operation failed.	DRF Registration operation failed for a component due to some internal error.
DRFComponentDeRegistered	DRF successfully deregistered the requested component.	DRF successfully deregistered the requested component.

Alarm Name	Description	Explanation
DRFDeRegistrationFailure	DRF deregistration request for a component failed.	DRF deregistration request for a component failed.
DRFFailure	DRF Backup or Restore process has failed.	DRF Backup or Restore process encountered errors.
DRFRestoreInternalError	DRF Restore operation has encountered an error. Restore cancelled internally.	DRF Restore operation has encountered an error. Restore cancelled internally.
DRFLogDirAccessFailure	DRF could not access the log directory.	DRF could not access the log directory.
DRFDeRegisteredServer	DRF automatically de-registered all the components for the server.	The server may have been disconnected from the Unified Communications Manager cluster.
DRFSchedulerDisabled	DRF Scheduler is disabled because no configured features are available for backup.	DRF Scheduler is disabled because no configured features are available for backup
DRFSchedulerUpdated	DRF Scheduled backup configuration is updated automatically due to feature de-registration.	DRF Scheduled backup configuration is updated automatically due to feature de-registration

License Reservation

License Reservation

Follow the below steps, after performing the restore operation on the Specific License Reservation enabled Unified Communications Manager.

Table 10: Disaster Recovery System for License Reservation

State after Restore	Product on CSSM	Solution
UNREGISTERED	Yes	Contact Cisco to remove the product from CSSM and do register from the product.
	No	Nothing required

State after Restore	Product on CSSM	Solution
RESERVATION IN PROGRESS	Yes	Do either of the below procedures: Procedure-1: **1.** Get the authorization code for the product from CSSM. **2.** Run the below CLI by giving the authorization code **license smart reservation return-authorization "<authorization-code>"**. Procedure-2: **1.** Contact Cisco to remove the product from CSSM.
	No	Execute the CLI from the product **license smart reservation cancel**.
REGISTERED	Yes	**1.** Execute the below CLI **license smart reservation return** from the product. A reservation return code will be printed on the console. **2.** Enter the reservation return code on CSSM to remove the product.
	No	Execute the CLI from the product **license smart reservation return**.

Restore Interactions and Restrictions

Restore Restrictions

The following restrictions apply to using Disaster Recovery System to restore Cisco Unified Communications Manager or IM and Presence Service

Table 11: Restore Restrictions

Restriction	Description
Export Restricted	You can restore the DRS backup from a restricted version only to a restricted version and the backup from an unrestricted version can be restored only to an unrestricted version. Note that if you upgrade to the U.S. export unrestricted version of Cisco Unified Communications Manager, you will not be able to later upgrade to or be able to perform a fresh install of the U.S. export restricted version of this software
Platform Migrations	You cannot use the Disaster Recovery System to migrate data between platforms (for example, from Windows to Linux or from Linux to Windows). A restore must run on the same product version as the backup. For information on data migration from a Windows-based platform to a Linux-based platform, see the *Data Migration Assistant User Guide*.
HW Replacement and Migrations	When you perform a DRS restore to migrate data to a new server, you must assign the new server the identical IP address and hostname that the old server used. Additionally, if DNS was configured when the backup was taken, then the same DNS configuration must be present prior to performing a restore. For more information about replacing a server, refer to the *Replacing a Single Server or Cluster for Cisco Unified Communications Manager guide*. In addition, you must run the Certificate Trust List (CTL) client after a hardware replacement. You must run the CTL client if you do not restore the subsequent node (subscriber) servers. In other cases, DRS backs up the certificates that you need. For more information, see the “Installing the CTL Client” and “Configuring the CTL Client ” procedures in the *Cisco Unified Communications Manager Security Guide*.
Extension Mobility Cross Cluster	Extension Mobility Cross Cluster users who are logged in to a remote cluster at backup shall remain logged in after restore.

Note DRS backup/restore is a high CPU-oriented process. Smart Licence Manager is one of the components that are backed-up and restored. During this process Smart License Manger service is restarted. You can expect high resource utilization so recommended to schedule the process during maintenance period.

After successfully restoring the Cisco Unified Communications server components, register the Cisco Unified Communications Manager with Cisco Smart Software Manager or Cisco Smart Software Manager satellite. If the product is already registered before taking the backup, then reregister the product for updating the license information.

For more information on how to register the product with Cisco Smart Software Manager or Cisco Smart Software Manager satellite, see the *System Configuration Guide for Cisco Unified Communications Manager* for your release.

Troubleshooting

DRS Restore to Smaller Virtual Machine Fails

Problem

A database restore may fail if you restore an IM and Presence Service node to a VM with smaller disks.

Cause

This failure occurs when you migrate from a larger disk size to a smaller disk size.

Solution

Deploy a VM for the restore from an OVA template that has 2 virtual disks.