Administration Guide for Cisco Unified Communications Manager and IM and Presence Service, Release 11.5(1)

First Published: June 07, 2016

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

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

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

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2016 Cisco Systems, Inc. All rights reserved.

CONTENTS

PART I Administration Overview 1

CHAPTER 1 Administration Overview 3

- Cisco Unified CM Administration Overview 3
- Operating System Administration Overview 4
- Cisco Unified Serviceability Overview 5
- Cisco Unified Reporting Overview 6
- Disaster Recovery System Overview 7
- Bulk Administration Tool Overview 7

CHAPTER 2 Getting Started 9

- Sign In 9
- Reset the Administrator or Security Password 9
- Shut Down or Restart the System 10

PART II Manage Users 13

CHAPTER 3 Manage User Access 15

- User Access Overview 15
- Roles Overview 15
- Access Control Groups 16
- Role and Access Control Group Prerequisites 17
- Role and Access Control Group Configuration Task Flow 17
  - Create a Custom Role 18
  - Copy a Role 19
  - Create Access Control Group 20
  - Copy Access Control Group 20
  - Assign Roles for Access Control Group 21

Assign Users to Access Control Group 22
View User Privilege Report 22
Configure Overlapping Privilege Policy for Access Control Groups 23
Create Custom Help Desk Role Task Flow 23
Create Custom Help Desk Role 24
Create Custom Help Desk Access Control Group 24
Assign Help Desk Role to Access Control Group 25
Assign Help Desk Members to Access Control Group 25
Delete Access Control Group 26
Set up a Remote Account 27
Standard Roles and Access Control Groups 27

CHAPTER 4 Manage End Users 37
End User Overview 37
End User Management Tasks 37
Configure User Templates 38
Configure Universal Line Template 39
Configure Universal Device Template 39
Configure User Profiles 40
Configure Feature Group Template 41
Import an End User from LDAP 41
Add an End User Manually 42
Add New Phone for End User 43
Move an Existing Phone to a End User 43
Change the End User PIN 44
Change the End User Password 44
Create a Cisco Unity Connection Voice Mailbox 45

CHAPTER 5 Manage Application Users 47
Application Users Overview 47
Application Users Task Flow 48
Add New Application User 48
Associate Devices with Application Users 49
Add Administrator User to Cisco Unity or Cisco Unity Connection 49
Change Application User Password 50

Manage Application User Password Credential Information 50

PART III Manage Devices 53

CHAPTER 6 Manage Phones 55

Phone Management Overview 55

Phone Management Tasks 55

Add a New Phone with a Device Template 56

Move an Existing Phone 57

Find an Actively Logged-In Device 57

Find a Remotely Logged-In Device 58

Remotely Lock a Phone 58

Reset a Phone to Factory Defaults 59

Search for Locked or Reset Devices 59

View LSC Status and Generate a CAPF Report for a Phone 60

CHAPTER 7 Manage Device Firmware 63

Device Firmware Updates Overview 63

Install a Device Pack or Cisco Options Package File 63

Remove Unused Firmware from the System 64

CHAPTER 8 Manage Infrastructure Devices 67

Manage Infrastructure Overview 67

Manage Infrastructure Prerequisites 67

Manage Infrastructure Task Flow 68

View Status for Infrastructure Device 68

Deactivate Tracking for Infrastructure Device 68

Activate Tracking for Deactivated Infrastructure Devices 69

PART IV Manage the System 71

CHAPTER 9 Monitor System Status 73

View Cluster Nodes Status 73

View Hardware Status 73

View Network Status 74

View Installed Software 74
View System Status 74
View IP Preferences 75
View Last Login Details 75
Ping a Node 76
Display Service Parameters 76

CHAPTER 10 View Usage Records 79
Usage Records Overview 79
Dependency Records 79
Route Plan Reports 79
Usage Report Tasks 80
Route Plan Reports Task Flow 80
View Route Plan Records 81
Save Route Plan Reports 81
Delete Unassigned Directory Numbers 82
Update Unassigned Directory Numbers 82
Dependency Records Task Flow 83
Configure Dependency Records 83
View Dependency Records 84

CHAPTER 11 Backup the System 85
Backup Overview 85
Backup Prerequisites 85
Backup Task Flow 86
Configure Backup Devices 86
Estimate Size of Backup File 87
Configure a Scheduled Backup 88
Start a Manual Backup 89
View Current Backup Status 90
View Backup History 91
Backup Interactions and Restrictions 91
Backup Restrictions 91
SFTP Servers for Remote Backups 92

CHAPTER 12 Restore the System 95

Restore Overview 95

Master Agent 95

Local Agents 95

Restore Prerequisites 96

Restore Task Flow 96

Restore the First Node Only 97

Restore Subsequent Cluster Node 98

Restore Cluster in One Step After Publisher Rebuilds 99

Restore Entire Cluster 101

Restore Node Or Cluster to Last Known Good Configuration 102

Restart a Node 102

Check Restore Job Status 103

View Restore History 103

Data Authentication 104

Trace Files 104

Command Line Interface 104

Alarms and Messages 106

Alarms and Messages 106

Restore Interactions and Restrictions 109

Restore Restrictions 109

Troubleshooting 110

DRS Restore to Smaller Virtual Machine Fails 110

CHAPTER 13 Manage Enterprise Parameters 111

Enterprise Parameters Overview 111

View Enterprise Parameter Information 111

Update Enterprise Parameters 112

Apply Configuration to Devices 112

Restore Default Enterprise Parameters 113

PART V Manage Security 115

CHAPTER 14 Manage SAML Single Sign-On 117

SAML Single Sign-On Overview 117
Opt-In Control for Certificate-Based SSO Authentication for Cisco Jabber on iOS 117
SAML Single Sign-On Prerequisites 118
Manage SAML Single Sign-On 119
Enable SAML Single Sign-On 119
Configure SSO Login Behavior for Cisco Jabber on iOS 120
Enable SAML Single Sign-On on WebDialer After an Upgrade 121
Deactivate the Cisco WebDialer Service 121
Disable SAML Single Sign-On 121
Activate the Cisco WebDialer Service 122
Access the Recovery URL 122
Update Server Metadata After a Domain or Hostname Change 122
Manually Provision Server Metadata 123

CHAPTER 15 Manage Certificates 125
Certificates Overview 125
Third-Party Signed Certificate or Certificate Chain 126
Third-Party Certificate Authority Certificates 127
Show Certificates 128
Download Certificates 128
Install Intermediate Certificates 128
Delete a Trust Certificate 129
Regenerate a Certificate 130
Certificate Names and Descriptions 130
Upload Certificate or Certificate Chain 131
Manage Third-Party Certificate Authority Certificates 132
Generate a Certificate Signing Request 133
Download a Certificate Signing Request 133
Add Certificate Authority-Signed CAPF Root Certificate to the Trust Store 133
Restart a Service 134
Monitor Certificate Expiration 134
Configure the Online Certificate Status Protocol 135
Troubleshoot Certificate Errors 135

CHAPTER 16 Manage Bulk Certificates 137

Manage Bulk Certificates 137
Export Certificates 137
Import Certificates 138

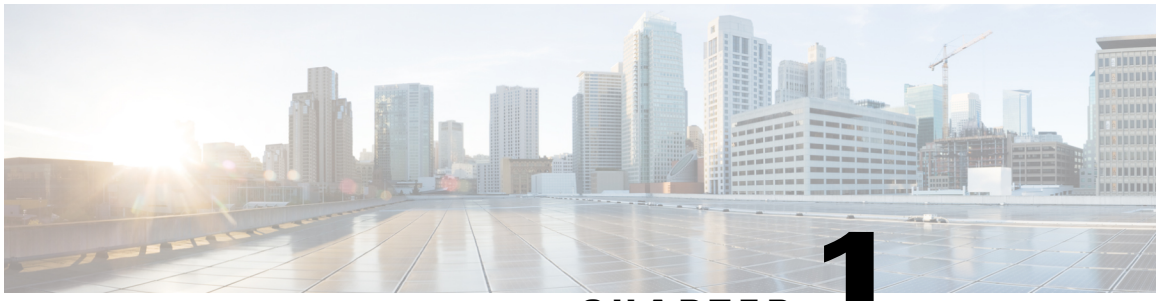
CHAPTER 17 Manage IPsec Policies 139
IPsec Policies Overview 139
Configure IPsec Policies 139
Manage IPsec Policies 140

CHAPTER 18 Manage Credential Policies 141
Credential Policy and Authentication 141
JTAPI and TAPI Support for Credential Policies 141
Configure a Credential Policy 142
Configure a Credential Policy Default 142
Monitor Authentication Activity 143
Configuring Credential Caching 144

PART I

Administration Overview

- Administration Overview, page 3
- Getting Started, page 9



CHAPTER 1

Administration Overview

- Cisco Unified CM Administration Overview, page 3
- Operating System Administration Overview, page 4
- Cisco Unified Serviceability Overview, page 5
- Cisco Unified Reporting Overview, page 6
- Disaster Recovery System Overview, page 7
- Bulk Administration Tool Overview, page 7

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.

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, which is accessed at the Cisco Unified Communications Manager and Cisco Unified Communications Manager IM and Presence Service consoles, generates consolidated reports for troubleshooting or inspecting cluster data.

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

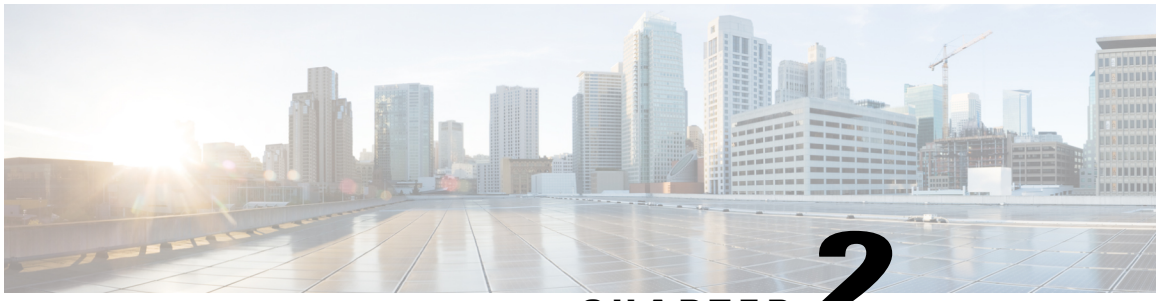
The Cisco Unified Communications Manager Bulk Administration Tool (BAT), a web-based application, lets administrators perform bulk transactions to the Cisco Unified Communications Manager database. BAT lets you add, update, or delete a large number of similar phones, users, or ports at the same time. When you use Cisco Unified 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 Unified 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, page 9
- Reset the Administrator or Security Password, page 9
- Shut Down or Restart the System, page 10

Sign In

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.

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”here 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 Cisco Unified 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.

Procedure

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

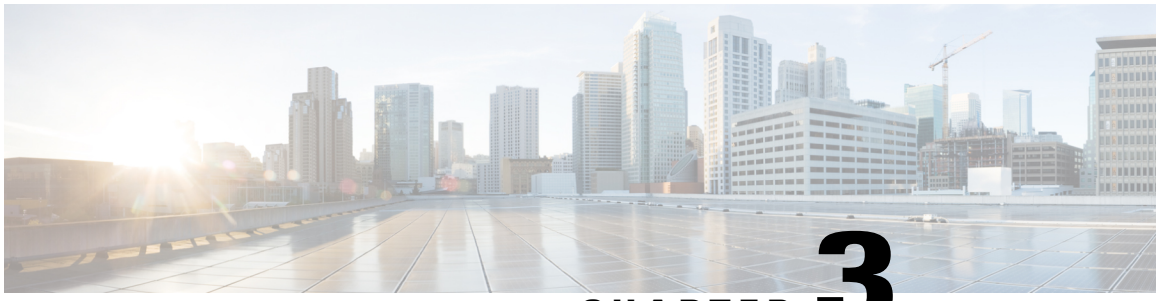
Step 2 Perform one of the following actions:

- 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

- Manage User Access, page 15
- Manage End Users, page 37
- Manage Application Users, page 47



CHAPTER 3

Manage User Access

- User Access Overview, page 15
- Roles Overview, page 15
- Access Control Groups, page 16
- Role and Access Control Group Prerequisites, page 17
- Role and Access Control Group Configuration Task Flow , page 17
- Set up a Remote Account, page 27
- Standard Roles and Access Control Groups, page 27

User Access Overview

You can manage user access to Cisco Unified Communications Manager by assigning your end users to access control groups that are associated to roles.

Roles and access control groups provide multiple levels of security to Cisco Unified Communications Manager. Each role defines a set of permissions for a specific resource within Cisco Unified Communications Manager. When you assign a role to an access control group and then assign end users to that access control group, you grant those end users all the access permissions that are defined by the role.

Upon installation Cisco Unified Communications Manager comes with predefined default roles that are assigned to predefined default access control groups. You can assign your end users to the default access control groups, or you can customize access settings by setting up new access control groups and roles.

Roles Overview

When you provision end users, you must decide on what roles you want to assign to your users. You can assign roles to an end user, application user, or to an access control group. You can assign multiple roles to a single user.

Each role contains a set of privileges that are attached to a specific resource or application. For example, the Standard CCM End Users role provides users who are assigned that role with access to the Cisco Unified Communications Self Care Portal. You can also assign roles that provide access to resources such as Cisco Unified Communications Manager Administration, Cisco CDR Analysis and Reporting, the Dialed Number

Analyzer, and the CTI interface. For most resources with graphical user interfaces, such as a specific configuration window, the privileges that are attached to the role allow the user to view or update data in that window, or in a group of related windows.

Configuring and Assigning Roles

You must decide whether you want to assign standard roles to your users, or create custom roles:

- Standard roles—Standard roles are predefined, default roles that come installed in Cisco Unified Communications Manager. You cannot edit the privileges or modify the role in any way.
- Custom roles—Custom roles are roles that you create. You can create custom roles when there are no standard roles that contain the privileges that you want to assign to your users. For example, if you want to assign a standard role, but want to modify one of the privileges, you can copy the privileges of the standard role into a custom role and then edit the privileges in that custom role.

Privilege Types

Each role contains a set of privileges that are attached to a specific resource. There are two types of privileges that you can assign to a resource:

- Read—Read privilege gives the user the ability to view the settings for that resource, but the user cannot make any configuration updates. For example, the privilege may allow the user to view the settings on a particular configuration window, but the configuration window for that application will not display update buttons or icons.
- Update—Update privileges give the user the ability to modify the settings for that resource. For example, the privileges may allow the user to make updates in a specific configuration window.

End User and Administrator Roles

The Standard CCM End Users role provides end users with access to the Cisco Unified Communications Self Care Portal. For additional privileges, such as CTI access, you must assign additional roles, such as the Standard CTI Enabled role.

The Standard CCM Admin Users role is the base role for all administration tasks and serves as the authentication role. This role provides users with administrative access to the Cisco Unified Communications Manager Administration user interface. Cisco Unified Communications Manager Administration defines this role as the role that is necessary to log in to Cisco Unified Communications Manager Administration.

Related Topics

Standard Roles and Access Control Groups, on page 27

Access Control Groups

You can use access control groups along with roles to quickly assign network access permissions to a group of users with similar access requirements.

An access control group is a list of end users and application users. You can assign end users or application users who share similar access needs to an access control group that contains the roles and permissions that they need.

The system includes a set of predefined standard access control groups. Each standard access control group has a set of roles assigned by default. When you assign a user to that access control group, those roles are also assigned to that end user.

You cannot edit the roles that are assigned to standard access control groups. However, you can create customized access control groups and assign the roles that you choose to your customized access control groups.

Related Topics

Standard Roles and Access Control Groups, on page 27

Role and Access Control Group Prerequisites

Before you create a new role or access control group, review the standard roles and access control groups that come pre-installed on your system to check whether an existing access control group contains the roles and permissions that you require for your users.

For details, see Standard Roles and Access Control Groups, on page 27.

Role and Access Control Group Configuration Task Flow

Perform the following tasks to configure a new role and assign it to a new access control group.

Procedure

	Command or Action	Purpose
Step 1	Create a new role using either of the following methods: • Create a Custom Role, on page 18 • Copy a Role, on page 19	Use the 'Create' procedure to create, and configure a new role from scratch. Use the 'Copy' command if the new role has similar settings as a standard role. You can copy the privilege settings from the existing standard role into the new role. You can then edit the settings in the new role.
Step 2	Create an access control group using either of the following methods: • Create Access Control Group, on page 20 • Copy Access Control Group, on page 20	Use the 'Create' procedure to create and configure a new access control group. The 'Copy' command can be used if the new access control group closely resembles one of the default group. You can copy the role assignments from the existing group into the new group and then edit them.
Step 3	Assign Roles for Access Control Group, on page 21	Update the assigned roles for an access control group by adding or deleting roles.
Step 4	Assign Users to Access Control Group, on page 22	Update the user list for an access control group by adding or deleting users from the group. All users assigned to the group will take on the privileges that are configured in the roles that are assigned to the group.

	Command or Action	Purpose
Step 5	View User Privilege Report, on page 22	Optional. If you need to review the assigned access privileges for a user, view the privilege report for that user.
Step 6	Configure Overlapping Privilege Policy for Access Control Groups, on page 23	Optional. 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.
Step 7	Create Custom Help Desk Role Task Flow, on page 23	Optional. Some companies want their help desk personnel to have privileges to be able to perform certain administrative tasks. 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.
Step 8	Delete Access Control Group, on page 26	Optional. Use this procedure if you need to delete an access control group from the system.

Create a Custom Role

Perform this procedure to create a custom role and configure the privileges for that role. You may want to create a custom role if there is no system-defined standard role that matches the privileges that you want to assign to your users.

Procedure

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

Step 2 From the **Application** drop-down list box, choose the application with which this role associates.
The **Role Configuration** window displays.

Step 3 Click **Next**.

Step 4 In the **Name** text box, enter a name for the role.
Names can comprise up to 128 characters. Valid characters include letters, numbers, dashes, dots (periods), spaces, and underscores.

Step 5 In the **Description** text box, enter a description for the role.
Descriptions can have up to 128 characters.

Step 6 For each resource in the new role, edit the privileges as follows:

- if you want the role to be able to view that resource, click the **Read** check box
- if you want the role to be able to edit that resource, click the **Update** check box
- if you want the role to be able to view and edit that resource, check both the **Read** and **Update** check boxes

- If you do not want the role to have any access to that resource, leave both check boxes unchecked.

Step 7 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 8 Click **Save**.

What to Do Next

Perform one of the following procedures to set up a new access control group:

- Create Access Control Group, on page 20
- Copy Access Control Group, on page 20

Copy a Role

Perform the following procedure to create a new role by copying the settings from a standard role into a new role. Cisco Unified Communications Manager does not allow you to edit the privileges in a standard role, but you can edit the privileges in roles that you create.

Procedure

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

Step 2 Click **Find** and select the role whose resources and privileges you want to copy.

Step 3 Click **Copy**.

Step 4 Enter the name of the new role and click **OK**.
The **Role Configuration** window displays the settings of the new role. The privileges for the new role are the same as the privileges for the role you copied.

Step 5 For any of the resources in the new role, edit the privileges as follows:

- Check the **Read** check box to allow users to view the resource.
- Check the **Update** check box to allow users to edit the resource.
- To restrict access to the resource, leave both check boxes unchecked.

Step 6 Click **Save**.

What to Do Next

In order to assign the role to users, you must create a new access control group and assign the role to that group. Perform either of the following procedures to create a new access control group:

- Create Access Control Group, on page 20

- Copy Access Control Group, on page 20

Create Access Control Group

Perform this procedure to create a new access control group.

Before You Begin

If the access control group has similar settings as an existing group, you can use the Copy command to copy the settings of the existing group to a new group that you create.

Copy Access Control Group, on page 20

Procedure

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

Step 2 Click **Add New**.

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

Step 4 Click **Save**.

What to Do Next

Assign Roles for Access Control Group, on page 21

Copy Access Control Group

Perform the following task to create a new access control group by copying the role settings from an existing access control group to a new group that can be edited.

Procedure

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

Step 2 Click **Find** and select the access control group whose settings you want to copy.

Step 3 Click **Copy**.

Step 4 Enter a name for the new access control group and click **OK**.

Step 5 Click **Save**.

What to Do Next

If you need to review and edit the roles assigned to the access control group:

Assign Roles for Access Control Group, on page 21

Assign Roles for Access Control Group

Use this procedure to assign roles for an access control group. If you copied the access control group settings from an existing group, you may also need to delete a role.

Users with full access, such as administrators, can assign roles or delete roles for access control groups. An access control group with assigned roles has access to all the resources that the role comprises.

Note When you assign roles to an access control group, you should assign the Standard Unified CM Admin Users role to the access control group. This role enables the users to log into Unified CM Administration.

Before You Begin

Perform either of the following tasks if you need to create a new access control group:

- Copy Access Control Group, on page 20
- Create Access Control Group, on page 20

Procedure

Step 1 Choose **User Management** > **User Settings** > **Access Control Group**.
The **Find and List Access Control Groups** window appears.

Step 2 Click **Find** and select the access control group for which you want to assign roles.
The Access Control Group Configuration window displays.

Step 3 From the **Related Links** drop-down list, choose **Assign Role to Access Control Group**, and click **Go**.
The **Role Assignment** pane displays.

Step 4 If you want to add new roles to the access control group, do the following:

a) Click **Assign Role to Group**.
b) Click **Find** to search the list of roles.
c) Choose the roles that you want to add to this access control group.
d) Click **Add Selected**.
The new role appears in the Role list box.

Step 5 If you want to delete an assigned role from the access control group, do the following:

a) In the **Role** list box, highlight the role that you want to delete.
b) Click **Delete Role Assignment**.

Step 6 Click **Save**.
The role assignments are added to the access control group in the database.

What to Do Next

Assign Users to Access Control Group, on page 22

Assign Users to Access Control Group

Perform this task to update the list of end users or application users in an access control group by assigning new users or deleting existing users.

Before You Begin

Assign Roles for Access Control Group, on page 21

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 Click **Find** to display the list of users.

Step 4 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 5 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 6 Click **Save**.

What to Do Next

Optional. If you need to view the user privilege report for a specific end user or application user, see the following:

- View User Privilege Report, on page 22

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.

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**.

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 24	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 24	Create a new access control group for the Help Desk role.
Step 3	Assign Help Desk Role to Access Control Group, on page 25	Assign the Help Desk role to the Help Desk access control group. Any users assigned to this access control

	Command or Action	Purpose
		group will be assigned the privileges of the Help Desk role.
Step 4	Assign Help Desk Members to Access Control Group, on page 25	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 24

Create Custom Help Desk Access Control Group

Before You Begin

Create Custom Help Desk Role, on page 24

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 25

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 24

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 25

Assign Help Desk Members to Access Control Group

Before You Begin

Assign Help Desk Role to Access Control Group, on page 25

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.

Set up a Remote Account

Configure a remote account so that Cisco support can temporarily gain access to your system for troubleshooting purposes.

Procedure

Step 1 From Cisco Unified Operating 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**.
Fields appear that show information about the remote support account. See the online help for more information about the fields.

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

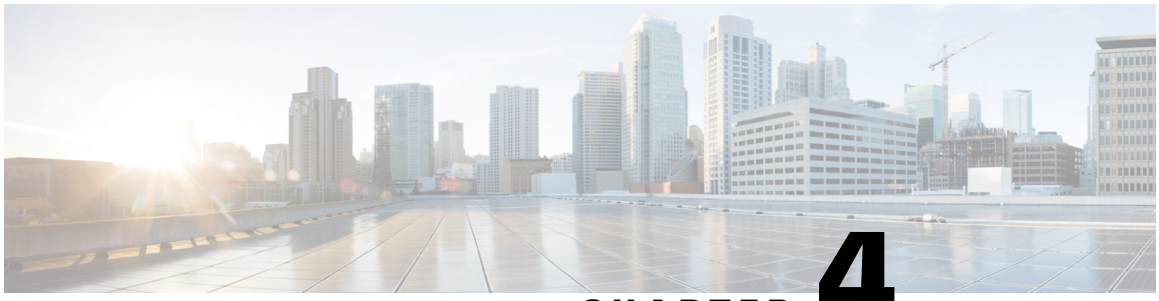
Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard CCM System Management	Allows you to perform the following tasks in Cisco Unified Communications Manager Administration: • View and configure the following items: ◦ Automate Alternate Routing (AAR) groups ◦ Cisco Unified Communications Managers (Cisco Unified CMs) and Cisco Unified Communications Manager groups ◦ Date and time groups ◦ Device defaults ◦ Device pools ◦ Enterprise parameters ◦ Enterprise phone configuration ◦ Locations ◦ Network Time Protocol (NTP) servers ◦ Plug-ins ◦ Security profiles for phones that run Skinny Call Control Protocol (SCCP) or Session Initiation Protocol (SIP); security profiles for SIP trunks ◦ Survivable Remote Site Telephony (SRST) references ◦ Servers • View and configure the Job Scheduler windows in the Bulk Administration Tool	Standard CCM Server Maintenance
Standard CCM User Privilege Management	Allows you to view and configure application users in Cisco Unified Communications Manager Administration.	
Standard CCMADMIN Administration	Allows you access to all aspects of the CCMAdmin system	
Standard CCMADMIN Administration	Allows you to view and configure all items in Cisco Unified Communications Manager Administration and the Bulk Administration Tool.	Standard CCM Super Users
Standard 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 Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
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	Standard CTI Allow Call Park Monitoring
Standard CTI Allow Call Recording	Allows CTI applications/devices to record calls	Standard CTI Allow Call Recording
Standard CTI Allow Calling Number Modification	Allows CTI applications to transform calling party numbers during a call	Standard CTI Allow Calling Number Modification
Standard CTI Allow Control of All Devices	Allows control of all CTI-controllable devices	Standard CTI Allow Control of All Devices
Standard CTI Allow Control of Phones Supporting Connected Xfer and conf	Allows control of all CTI devices that supported connected transfer and conferencing	Standard CTI Allow Control of Phones supporting Connected Xfer and conf
Standard 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 Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard CUReporting	Allows you to view, download, generate, and upload reports in Cisco Unified Reporting	Standard CCM Administration Users, Standard CCM Super Users
Standard EM Authentication Proxy Rights	Manages Cisco Extension Mobility (EM) authentication rights for applications; required for all application users that interact with Cisco Extension Mobility (for example, Cisco Unified Communications Manager Assistant and Cisco Web Dialer)	Standard CCM Super Users, Standard EM Authentication Proxy Rights
Standard Packet Sniffing	Allows you to access Cisco Unified Communications Manager Administration to enable packet sniffing (capturing).	Standard Packet Sniffer Users
Standard RealtimeAndTraceCollection	Allows an you to access Cisco Unified Serviceability and the Real-Time Monitoring Tool view and use the following items: • Simple Object Access Protocol (SOAP) Serviceability AXL APIs • SOAP Call Record APIs • SOAP Diagnostic Portal (Analysis Manager) Database Service • configure trace for the audit log feature • configure Real-Time Monitoring Tool, including collecting traces	Standard RealtimeAndTraceCollection

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

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



CHAPTER 4

Manage End Users

- End User Overview, page 37
- End User Management Tasks, page 37

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 38	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.

	Command or Action	Purpose
Step 2	Add a new end user using one of the following methods • Import an End User from LDAP, on page 41 • Add an End User Manually, on page 42	If your system is synchronized with a company LDAP directory, you can import the new end user directly from LDAP. If you have configured 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 43 • Move an Existing Phone to a End User, on page 43	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 44	(Optional) To change the pin for an end user in Cisco Unified Communications Manager Administration.
Step 5	Change the End User Password, on page 44	(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 45	(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 39	Configure universal line templates with common settings that are typically applied to a directory number.
Step 2	Configure Universal Device Template, on page 39	Configure universal device templates with common settings that are typically applied to a phone.
Step 3	Configure User Profiles, on page 40	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.

	Command or Action	Purpose
Step 4	Configure Feature Group Template, on page 41	Assign the user profile to a feature group template. For LDAP Synchronized Users, the feature group template associates the user profile settings to the end user.

Configure Universal Line Template

Configure a universal line template with common settings that are typically applied to a directory number. You can create one or more universal line templates to create a collection of settings that reflect the most common directory number configurations in your organization and, through the user profile, you can apply those settings to new directory numbers that you provision for an end user.

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 Click **Save**.

What to Do Next

Configure Universal Device Template, on page 39

Configure Universal Device Template

Configure a universal device template. A universal device template contains a set of common settings that are typically applied to a phone, remote destination profile, or an extension mobility profile. You can create one or more universal device templates that reflect the most common device configurations in your organization and through a user profile, you can apply those settings to any new devices that you provision for an end user.

Before You Begin

Configure Universal Line Template, on page 39

Procedure

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

Step 2 Click **Add New**.

Step 3 Complete the fields in the **Universal Device Template Configuration** window. For field descriptions, see the online help.

Step 4 Click **Save**.

What to Do Next

Configure User Profiles, on page 40

Configure User Profiles

Configure a user profile that includes the universal line templates and universal device templates that you want to assign to end users who use that profile. You can also enable self-provisioning for end users who use this service profile.

Before You Begin

Configure Universal Device Template, on page 39

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **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 end user will be allowed to provision. The maximum is 20.

Step 7 Click **Save**.

What to Do Next

Configure Feature Group Template, on page 41

Configure Feature Group Template

A feature group template contains a set of common line, device, and feature settings. When you apply the feature group template to a new user, those line, device, and feature settings are applied to the user phones and phone lines. Feature group templates aid in your system deployment by helping you to very quickly configure phones, lines, and features for your provisioned users.

Procedure

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

Step 2 Click **Add New**.

Step 3 Complete the fields in the **Feature Group Template Configuration** window. Refer to the online help for field descriptions.

Step 4 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 41
- Add an End User Manually, on page 42

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, as well as a DN pool, the import process automatically configures the end user and primary extension.

Before You Begin

This procedure assumes 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 43
- Move an Existing Phone to a End User, on page 43

Add an End User Manually

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

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's **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 directory number 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 box, 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 43
- Move an Existing Phone to a End User, on page 43

Add New Phone for End User

Perform the following procedure to add a new phone for a new or existing end user. This procedure assumes 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 a end user:

- Add an End User Manually, on page 42
- Import an End User from LDAP, on page 41

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** button.
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 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.

What to Do Next

Move an Existing Phone to a End User, on page 43

Move an Existing Phone to a End User

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

Before You Begin

Add New Phone for End User , on page 43

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.

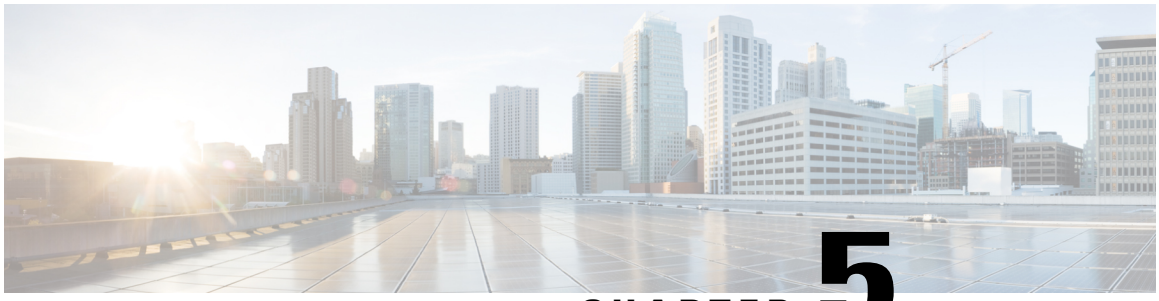
Step 5 From the **Application Server** drop-down list, choose the Cisco Unity Connection server on which you want to create a Cisco Unity Connection user, and then click **Next**.

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, page 47
- Application Users Task Flow, page 48

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.

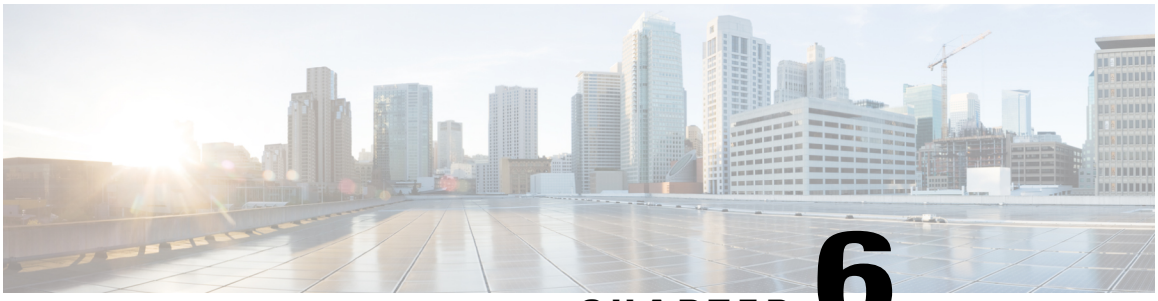
Step 4 Configure the fields on the **Credential Configuration** window. See the online help for more information about the fields and their configuration options.

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

PART III

Manage Devices

- Manage Phones, page 55
- Manage Device Firmware, page 63
- Manage Infrastructure Devices, page 67



CHAPTER 6

Manage Phones

- Phone Management Overview, page 55
- Phone Management Tasks, page 55

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.

Phone Management Tasks

Procedure

	Command or Action	Purpose
Step 1	Add a New Phone with a Device Template, 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 57	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 58	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 59	Reset a phone to its factory settings.

	Command or Action	Purpose
Step 7	Search for Locked or Reset Devices, on page 59	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 60	Search for LSC expiry status on phones, and also generate a CAPF report.

Add a New Phone with a Device Template

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 37

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** button.
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 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.

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

Procedure

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

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

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

Step 4 Click **Find**.
All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

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

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

The window displays the item that you choose.

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.

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

Procedure

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

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 box, select a search parameter.

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

c) Specify the appropriate search text, if applicable.

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

Step 4 Click Find.

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

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

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

The window displays the item that you choose.

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.

Search for Locked or Reset Devices

You can search for devices that have been remotely locked and/or remotely reset to factory default settings. 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 box, select the device operation type(s) to search.
b) From the second drop-down list box, select a search parameter.
c) From the third drop-down list box, select a search pattern.
d) Specify the appropriate search text, if applicable.

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

Step 4 Click **Find**.
All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

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

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

The window displays the item that you choose.

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:

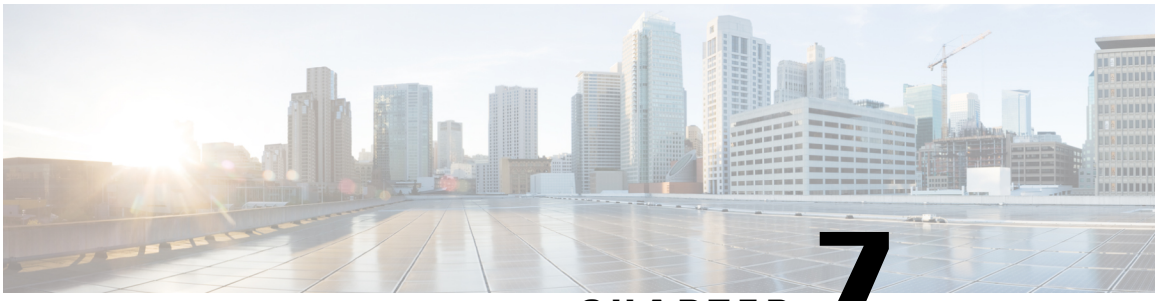
- LSC Expires
- LSC Issued By
- LSC Issuer Expires By

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, page 63
- Install a Device Pack or Cisco Options Package File, page 63
- Remove Unused Firmware from the System, page 64

Device Firmware Updates Overview

Device firmware loads are files that contain updated firmware for devices. The four types of firmware loads are phone loads, gateway loads, media termination point (MTP) loads, and conference bridge loads. During installation or upgrade, Cisco Unified Communications Manager provides the latest loads; however, you can also receive a load between releases that contains patches or other information that is important to the devices, such as phones or gateways.

The `/usr/local/cm/tftp` subdirectory stores these load files with a `.bin`, `.zip`, or `.sbin` extension. During installation or upgrade, this location stores the latest loads. To use new loads that you received between releases, you must copy the loads to this location so that the system can access them.

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

Install a Device Pack or Cisco Options Package File

Install a device package to provide capability for new features and phone models. Otherwise, individual device firmware is installed with individual device load Cisco Options Package (COP) files, or you can upload the individual device load files to the TFTP directory. Apply a device package to all of your Cisco Unified Communications Manager servers, beginning with the publisher server and the TFTP server. The system can upload and process only software that Cisco approves. You cannot install or use third-party or Windows-based software applications that you used with a previous version of Cisco Unified Communications Manager.

Before You Begin

Note When you apply a device package to enable new device support, a clusterwide reboot is no longer required for those devices to register successfully but the TFTP application and Tomcat services on Publisher node need to be restarted.

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 Stop and restart the TFTP server.

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.

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 retrieved. We recommend that you take a backup before deleting the firmware.

Procedure

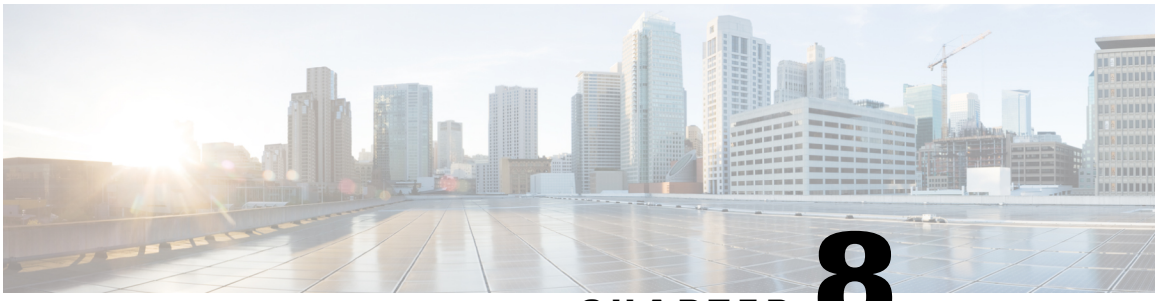
Step 1 From Cisco Unified OS Administration, choose **Software Upgrades** > **Device Load Management**.

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**.



CHAPTER 8

Manage Infrastructure Devices

- Manage Infrastructure Overview, page 67
- Manage Infrastructure Prerequisites, page 67
- Manage Infrastructure Task Flow, page 68

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 Cisco 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 the following chapter:

"Location Awareness", System 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 68	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 68	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 69	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.

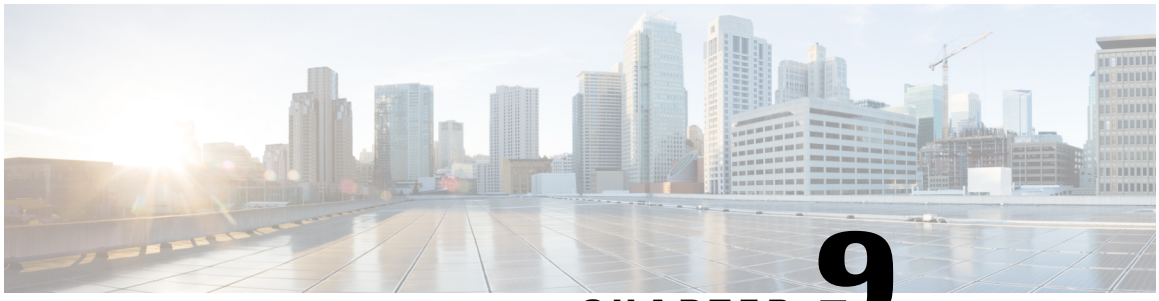
Step 3 Select the switch or access point for which you want to initiate tracking.

Step 4 Click **Reactivate Selected**.

PART IV

Manage the System

- Monitor System Status, page 73
- View Usage Records, page 79
- Backup the System, page 85
- Restore the System, page 95
- Manage Enterprise Parameters, page 111



CHAPTER 9

Monitor System Status

- View Cluster Nodes Status, page 73
- View Hardware Status, page 73
- View Network Status, page 74
- View Installed Software, page 74
- View System Status, page 74
- View IP Preferences, page 75
- View Last Login Details, page 75
- Ping a Node, page 76
- Display Service Parameters , page 76

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.

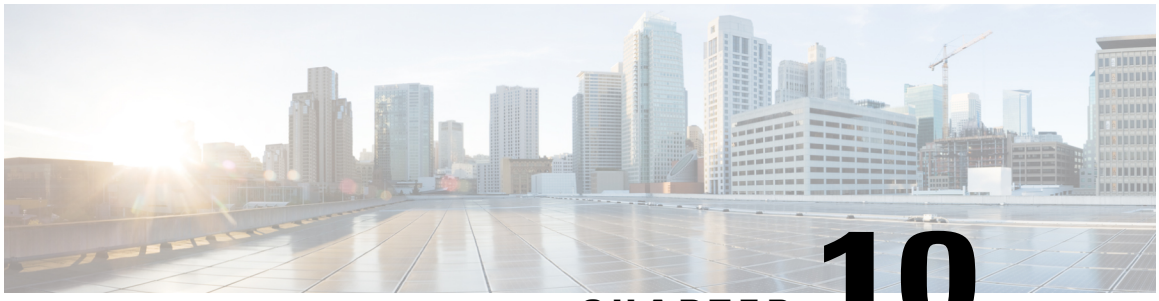
For a given parameter, click on the server name or on the current parameter value to link to the corresponding service parameter window to change the value. Click Previous and Next to navigate between Parameters for All Servers windows.

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, page 79
- Usage Report Tasks, page 80

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 81 • Save Route Plan Reports, on page 81 • Delete Unassigned Directory Numbers, on page 82 • Update Unassigned Directory Numbers, on page 82	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 84	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 81.	View route plan records and generate customized route plan reports.
Step 2	Save Route Plan Reports, on page 81.	View route plan reports in a .csv file format.
Step 3	Delete Unassigned Directory Numbers, on page 82.	Delete an unassigned directory number from the route plan report.
Step 4	Update Unassigned Directory Numbers, on page 82.	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 83.	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 84.	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 83

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.

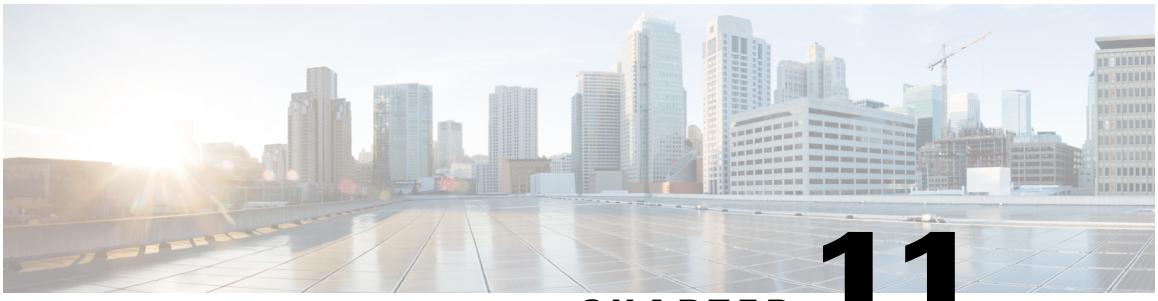
Step 4 From the **Related Links** list box, choose **Dependency Records** box, and click **Go**.

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

Backup the System

- Backup Overview, page 85
- Backup Prerequisites, page 85
- Backup Task Flow, page 86
- Backup Interactions and Restrictions, page 91

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 all cluster nodes are running the same version of Cisco Unified Communications Manager or Cisco IM and Presence Service. If different nodes are running different versions, the certificates will not match and your backup or restore could fail.

- 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 92

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 86	Specify the devices on which to back up data.
Step 2	Estimate Size of Backup File, on page 87	Estimate size of backup file created on the SFTP device.
Step 3	Choose one of the following options: • Configure a Scheduled Backup, on page 88 • Start a Manual Backup, on page 89	Create a backup schedule to back up data on a schedule. Optionally, run a manual backup.
Step 4	View Current Backup Status, on page 90	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 91	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 87

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 88
- Start a Manual Backup, on page 89

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 86

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 87
- (Optional) View Current Backup Status, on page 90

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 86
- Estimate Size of Backup File, on page 87

- 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 90

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 91

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 2: 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. You can use any SFTP server product, but we recommend products that are certified with Cisco Technology Partners. For information on which vendors have certified their products with your version of Cisco Unified Communications Manager, see the *Solutions Catalog* on the Cisco Developer Network at https://marketplace.cisco.com.

Use the information in the following table to determine which SFTP server solution to use in your system.

Table 3: SFTP Server Information

SFTP Server	Information
SFTP Server on Cisco Prime Collaboration Deployment	This server is provided and tested by Cisco, and 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 Admin Guide* before you upgrade its version (SFTP) or Unified Communications Manager to ensure that the versions are compatible.

SFTP Server	Information
SFTP Server from a Technology Partner	These servers are third party provided, third party tested, and jointly supported by TAC and the Cisco vendor. 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 from another Third Party	These servers are third party provided, have limited Cisco testing, 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. For a fully tested and supported SFTP solution, use Cisco Prime Collaboration Deployment or a Technology Partner.

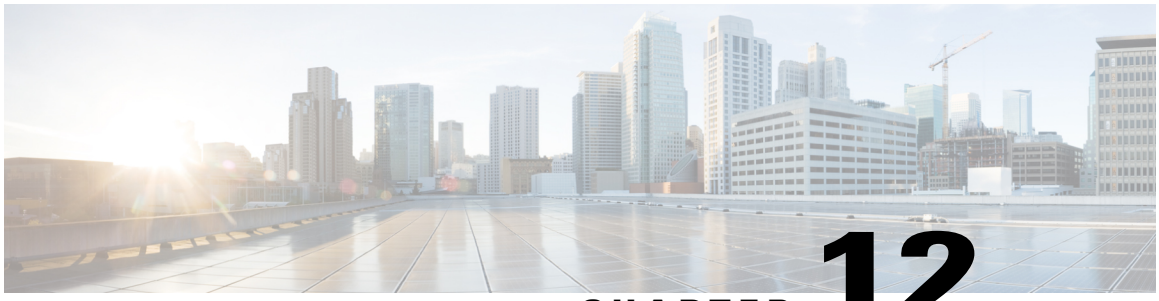
Cisco uses the following servers for internal testing. You may use one of the servers, but you must contact the vendor for support:

- Open SSH
- Titan

Cisco does not support using the SFTP product freeFTPd. This is because of the 1 GB file size limit on this SFTP product.

For details on how to set up third-party SFTP products, contact the third-party vendor for support. For issues with third-party products that have not been certified through the Cisco Technology Developer Program process, contact the third-party vendor for support. For information on using GlobalSCAPE with the supported Cisco Unified Communications Manager versions, contact GlobalSCAPE.

Note We recommend that you retest the DRS with your SFTP server after you upgrade your Unified Communications Manager, upgrade your SFTP server, or you switch to a different SFTP server. Perform this step to ensure that these components operate correctly together. As a best practice, perform a backup and restore on a standby or backup server.



CHAPTER 12

Restore the System

- Restore Overview, page 95
- Restore Prerequisites, page 96
- Restore Task Flow, page 96
- Data Authentication, page 104
- Alarms and Messages, page 106
- Restore Interactions and Restrictions, page 109
- Troubleshooting, page 110

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 all cluster nodes are running the same version of Cisco Unified Communications Manager (for Cisco Unified Communications Manager restores) or IM and Presence Service (for IM and Presence restores) and that the version matches the backup file version.
- 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 97	(Optional) Use this procedure only to restore the first publisher node in the cluster.
Step 2	Restore Subsequent Cluster Node, on page 98	(Optional) Use this procedure to restore the subscriber nodes in a cluster.
Step 3	Restore Cluster in One Step After Publisher Rebuilds, on page 99	(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 101	(Optional) Use this procedure to restore all nodes in the cluster, including the publisher node. If a major hard drive failure or upgrade 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 102	(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 102	Use this procedure to restart a node.

	Command or Action	Purpose
Step 7	Check Restore Job Status, on page 103	(Optional) Use this procedure to check the restore job status.
Step 8	View Restore History, on page 103	(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 Select the node to restore.

Step 9 Click **Restore** to restore the data.

Step 10 Click **Next**.

Step 11 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 12 (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 13 Click **Restore**.

Step 14 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 15 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 103
- To restart a node, see Restart a Node, on page 102

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 103
- To restart a node, see Restart a Node, on page 102

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. See the Related topics for more information about these procedures.

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 97 and Restore Subsequent Cluster Node, on page 98.

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 103
- To restart a node, see Restart a Node, on page 102

Related Topics

Restore the First Node Only, on page 97
Restore Subsequent Cluster Node, on page 98

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 103
- To restart a node, see Restart a Node, on page 102

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.

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 103.

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 4: 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

Command	Description
utils disaster_recovery jschLogs	Enables or disables JSch library logging
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.

Command	Description
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 5: 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.

Alarm Name	Description	Explanation
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.
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.

Alarm Name	Description	Explanation
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.
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

Alarm Name	Description	Explanation
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

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 6: 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*.

Restriction	Description
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.

Troubleshooting

DRS Restore to Smaller Virtual Machine Fails

Problem

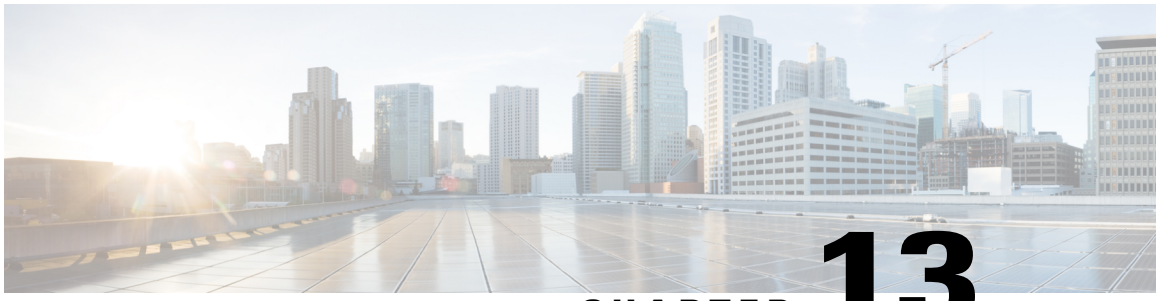
A database restore may fail if you restore an IM and Presence Service node to a VM with smaller disks.

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.



CHAPTER 13

Manage Enterprise Parameters

- Enterprise Parameters Overview, page 111

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 112

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 112

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**.

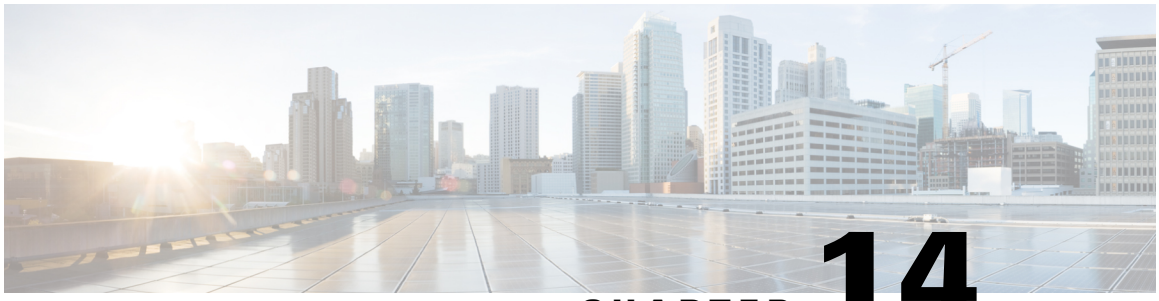
Step 2 Click **Set to Default**.

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

PART V

Manage Security

- Manage SAML Single Sign-On, page 117
- Manage Certificates, page 125
- Manage Bulk Certificates, page 137
- Manage IPsec Policies, page 139
- Manage Credential Policies, page 141



CHAPTER 14

Manage SAML Single Sign-On

- SAML Single Sign-On Overview, page 117
- Opt-In Control for Certificate-Based SSO Authentication for Cisco Jabber on iOS, page 117
- SAML Single Sign-On Prerequisites, page 118
- Manage SAML Single Sign-On, page 119

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 120 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.

  Note Cisco Unified Communications Manager currently supports only the sAMAccountName option as the LDAP attribute for user ID settings.

  For information about configuring mandatory attribute mapping, see the IdP product documentation.

- 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 121	Deactivate the Cisco WebDialer web service if it is already activated.
Step 2	Disable SAML Single Sign-On, on page 121	Disable SAML Single Sign-On if it is already enabled.
Step 3	Activate the Cisco WebDialer Service, on page 122	
Step 4	Enable SAML Single Sign-On, on page 119	

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 121

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 121

Procedure

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

What to Do Next

Activate the Cisco WebDialer Service, on page 122

Activate the Cisco WebDialer Service

Before You Begin

Disable SAML Single Sign-On, on page 121

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**, 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 119

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.

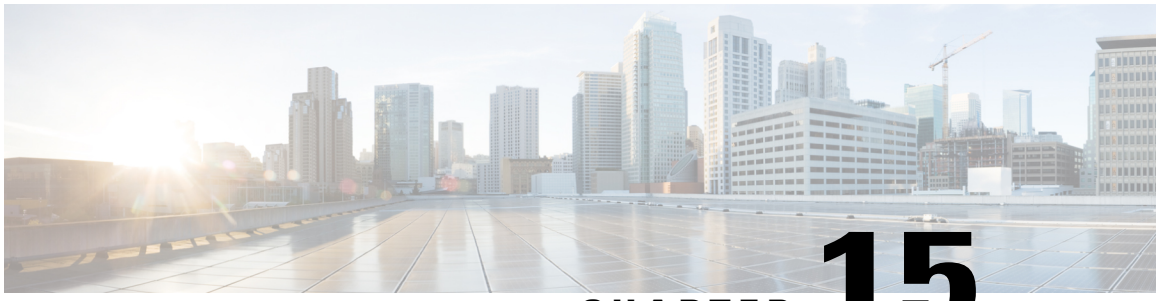
The general URL syntax is as follows:

`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 15

Manage Certificates

- Certificates Overview, page 125
- Show Certificates, page 128
- Download Certificates, page 128
- Install Intermediate Certificates, page 128
- Delete a Trust Certificate, page 129
- Regenerate a Certificate, page 130
- Upload Certificate or Certificate Chain, page 131
- Manage Third-Party Certificate Authority Certificates, page 132
- Monitor Certificate Expiration, page 134
- Configure the Online Certificate Status Protocol, page 135
- Troubleshoot Certificate Errors, page 135

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 Cisco 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, IPSec End System
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 Cisco Unified Communications Manager 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 Cisco Unified Communications Manager, allowing Tomcat and other certificates to support SHA256.

Show Certificates

View details about the certificates and trust stores that belong to your system.

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 To view details of a certificate or trust store, click the .PEM or .DER filename of the certificate.

Step 4 To return to the **Certificate List** window, click **Back To Find/List** in the **Related Links** list, and then click **Go**.

Download Certificates

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 file name of the certificate or certificate trust list (CTL).

Step 4 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 provided a signed certificate with multiple certificates in the certificate chain.

Tip The root certificate name is the `.pem` filename that was generated when the root certificate was uploaded.

Procedure

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

Step 2 Click **Upload Certificate**.

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

Step 4 Click **Browse**, navigate to the file, and then click **Open**.

Step 5 Click **Upload File**.

Step 6 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Step 7 Click **Upload Certificate**.

Step 8 In the **Upload Certificate** pop-up window, choose **IntelligenceCenter-srvr** from the **Certificate name** drop down list and enter the root certificate name.

Step 9 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 10 Click **Upload File**.

Step 11 After you install the customer certificate, access the Cisco Unified Intelligence Center URL using the FQDN. 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 When a Tomcat certificate is uploaded, the TFTP service should be deactivated and later activated. Else, the TFTP will continue 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. Deleting a certificate can break a certificate chain if the certificate is part of an existing chain. You can 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 the certificate that you delete is of the type “tomcat-trust”, “CallManager-trust” or “Phone-SAST-trust”, the certificate is deleted across all servers in the cluster.

Regenerate a Certificate

Regenerate a certificate if it is expired. Follow this procedure 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**.

Step 2 Configure the fields on the **Generate New Self-Signed Certificate** window. See the 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. See the Related Topics section for more information about the certificate names and their descriptions.

Step 5 Rerun the CTL client (if configured) after you regenerate the CAPF or CallManager certificates.

Note When a Tomcat certificate is regenerated, the TFTP service should be deactivated and later activated. Else, the TFTP will continue to offer the old cached self-signed tomcat certificate.

What to Do Next

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. See Backup the System, on page 85.

Related Topics

Certificate Names and Descriptions, on page 130

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 7: Certificate Names and Descriptions

Name	Description	Related Services
tomcat tomcat-ECDSA	This self-signed root certificate is generated during installation for the HTTPS node.	Tomcat and TFTP
ipsec	This self-signed root certificate is generated during installation for IPsec connections with MGCP and H.323 gateways.	Cisco Disaster Recovery System (DRS) Local and Cisco DRF Master
CallManager	This self-signed root certificate is installed automatically when you install Cisco Unified Communications Manager. This certificate provides node identification, including the node name and the global unique identifier (GUID).	CallManager, CAPF, and CTI
CAPF	The system copies this root certificate to your node or to all nodes in the cluster after you complete the Cisco client configuration.	CallManager and CAPF
TVS	This is a self-signed root certificate.	TVS

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 133	Generate a certificate signing request (CSR) which is a block of encrypted text that contains your certificate application information, including your 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 133	Download the CSR to your computer so that you 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 133	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 131	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 134	Restart the services that are affected by the new certificate. For all certificate types, restart the 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 your certificate application information, including your 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 the 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 CSR**.

Download a Certificate Signing Request

Download the CSR to your computer so that you 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

When using a certificate authority-signed CAPF Certificate, follow these steps to add the root certificate to the CallManager trust store.

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 After the certificate appears in the **Upload File** field, click **Upload**.

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**.

Monitor Certificate Expiration

Use this procedure to configure your system to automatically send you an email message when a certificate is close to its expiration date.

Procedure

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

Step 2 In the **Notification Start Time**, enter a numeric value. This value is the number of days before you receive a notification through email.

Step 3 In the **Notification Frequency**, enter a numeric value and choose **Days** or **Hours**.

Step 4 (Optional) Check **Enable E-mail notification**, and then enter email addresses in the **E-mail IDs** field.

Step 5 Click **Save**.

Configure the Online Certificate Status Protocol

Use the online certificate status protocol (OCSP) to obtain the revocation status of the certificate.

Note The certificate revocation status check is performed only during an upload of a certificate or certificate chain. The applicable alarm is raised if a certificate is revoked.

Before You Begin

Caution Before you enable OSCP, you must upload the OCSP responder certificate to tomcat-trust.

Procedure

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

Step 2 Check the **Enable OCSP** check box, and perform one of the following tasks:

- Choose **Use configured OCSP URI** if an external or configured URI is used to contact the OCSP responder. In the **OCSP Configured URI** field, enter the URI of the OCSP responder where certificate revocation status is verified.
- Choose **Use OCSP URI from Certificate** if the certificate is configured with an OCSP URI that will be used to contact the OCSP responder.

Step 3 Check the **Enable Revocation Check** check box to perform the revocation check.

Note The certificate revocation service is active for LDAP and IPsec connections, when the revocation and expiry check enterprise parameter is set to enabled.

Step 4 Enter the **Check Every** value to configure the frequency of the certificate revocation status check.

a) Click **Hours** or **Days** to check the revocation status hourly or daily.

Step 5 Click **Save**.

Troubleshoot Certificate Errors

If you encounter an error when you attempt to access Cisco Unified Communications Manager services from an IM and Presence Service node or IM and Presence Service functionality from a Cisco 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. In some cases, you may only have to complete the first step to resolve the error; in other cases, you will have to complete all 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.

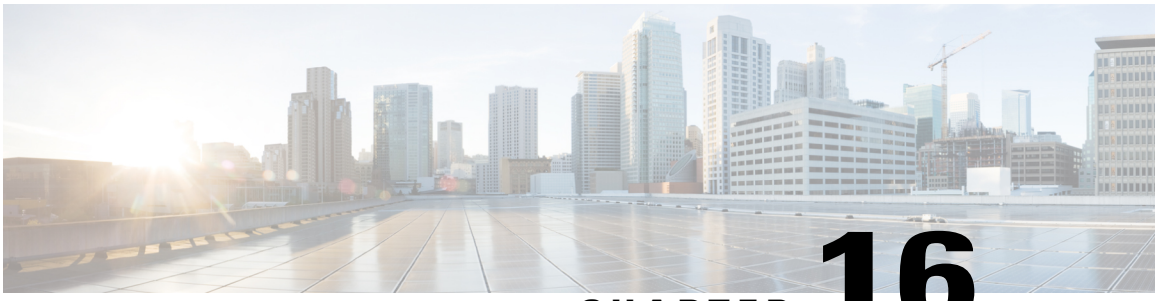
Step 2 Choose a certificate to view its information. Verify that the content matches with the corresponding certificate on the remote node.

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 16

Manage Bulk Certificates

- Manage Bulk Certificates, page 137

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 137	This procedure creates a PKCS12 file that contains certificates for all nodes in the cluster. **Note** • Every participating cluster must export certificates to the same SFTP server and SFTP directory. • You must export certificates on the cluster whenever the Tomcat, Tomcat-ECDSA, TFTP, or CAPF certificates are regenerated on any of the cluster nodes.
Step 2	Import Certificates, on page 138	Import the certificates back into the home and remote (visiting) clusters. **Note** After an upgrade, these certificates are preserved. You do not need to reimport or reconsolidate certificates.

Export Certificates

This procedure creates a PKCS12 file that contains certificates for all nodes in the cluster.

Note

- Every participating cluster must export certificates to the same SFTP server and SFTP directory.
- You must export certificates on the cluster whenever the Tomcat, Tomcat-ECDSA, TFTP, or CAPF certificates are regenerated on any of the cluster nodes.

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**.

Import Certificates

Import the certificates back into the home and remote (visiting) clusters.

Note After an upgrade, these certificates are preserved. You do not need to reimport or reconsolidate certificates.

Before You Begin

Before the Import button appears, you must complete the following activities:

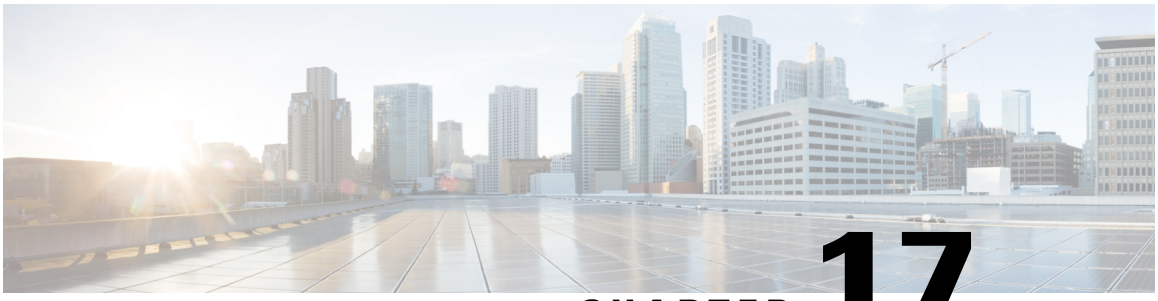
- Export the certificates from at least two clusters to the SFTP server.
- Consolidate the exported certificates.

Procedure

Step 1 From 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**.



CHAPTER 17

Manage IPsec Policies

- IPsec Policies Overview, page 139
- Configure IPsec Policies, page 139
- Manage IPsec Policies, page 140

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 Cisco 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.

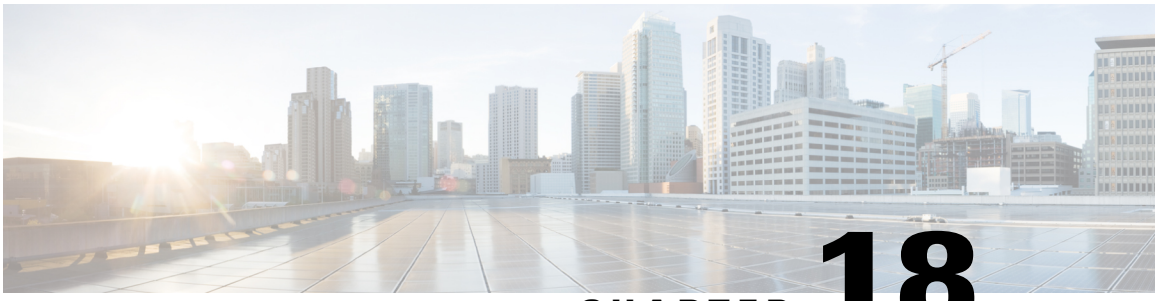
b) To enable or disable the policy, check or uncheck the **Enable Policy** check box.

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 18

Manage Credential Policies

- Credential Policy and Authentication, page 141
- Configure a Credential Policy, page 142
- Configure a Credential Policy Default, page 142
- Monitor Authentication Activity, page 143
- Configuring Credential Caching, page 144

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 Cisco 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 Cisco 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** > **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** > **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.

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**.