Cisco Unified Communications Operating System Administration Guide, Release 10.0(1)

First Published: December 03, 2013

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

Text Part Number: OL-27832-01

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)

© 2015 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface — Preface xi

Purpose xi

Audience xi

Organization xi

Related Documentation xii

Conventions xii

Obtain Support xiii

Security Overview xiii

PART I — Cisco Cisco Unified Communications Manager OS platform 1

CHAPTER 1 — Cisco Unified Operating System Overview 3

Cisco Unified Operating System Administration Overview 3

Operating System Status 3

Settings 4

Security Configuration 4

Software Upgrades 4

Services 5

CLI 5

CHAPTER 2 — Operating System Administration 7

Log In 7

Reset Passwords 8

CHAPTER 3 — Status and Configuration 11

Show Cluster Nodes 11

Show Hardware Status 12

Show Network Configuration 13
Show Installed Software 14
Show System Status 15
Show IP Preferences 16

CHAPTER 4 Settings 19
IP Settings 19
Set Up Ethernet Settings 19
Set Up IPv6 20
Set Up Publisher Settings 21
Set Up IP Address 22
Set Up NTP Servers 22
Set Up SMTP Settings 23
Set Up Time Settings 23

CHAPTER 5 System Restart 25
Switch Software Versions 25
Restart Current Version 26
Shut Down System 26

CHAPTER 6 Security 29
Set Up Internet Explorer Security Options 29
Manage Certificates 29
Show Certificates 30
Download Certificate 30
Install Intermediate Certificate 31
Delete and Regenerate Certificate 32
Delete Trust Certificate 32
Regenerate Certificate 33
Certificate Regeneration If Intracluster Communication Is Enabled Using EMCC 34
Upload Certificate 35
Upload Certificate or Certificate Chain 35
Upload Third-Party CA Certificates 35
Third-Party Signed Certificate or Certificate Chain 36

Generate Certificate Signing Request 37
Download Certificate Signing Request 38
Third-Party CA Certificates 38
Monitor Certificate Expiration 39
Certificate Revocation 40
Configure Online Certificate Status Protocol 40
Troubleshoot Certificate Errors 40
IPsec 41
Set Up IPsec Policy 41
Migration Characteristics 46
Manage IPsec Policies 47
Bulk Certificate Management 48
Export Certificates 48
Import Certificates 49
Configure OpenAM SSO Application 49

CHAPTER 7 Services 51
Ping 51
Set Up Remote Support 52

CHAPTER 8 Software Upgrades 55
Getting Started 56
About Cisco Unified Communications Manager 56
About the IM and Presence Service 56
About the System Topology 56
Upgrade Planning 57
Requirements and Limitations 57
System Limitations 57
Subnet Limitations 57
Cluster Size 57
Support for intercluster peers 57
Network Requirements 57
IP Address Requirements 58
DNS requirements 58
SFTP Server Support 58

Platform Requirements 59
Supported Platforms 59
ESXi and VMware Tools 59
OVA Templates 59
Power Supply 60
Software Requirements 60
Browser Requirements 60
Upgrade time requirements 60
Throttling affects time required to upgrade 61
System availability after upgrade 61
Supported Upgrade Paths 61
Version Requirements 61
Upgrade Paths For Cisco Unified Communications Manager 61
Upgrade Paths for IM and Presence Service 62
Upgrade From Cisco Unified Presence Release 8.5(4) 62
Licensing 63
Cisco Unified Communications Manager License Requirements 63
IM and Presence license requirements 63
Upgrade Overview 64
Types of upgrades 64
Standard upgrades 64
Refresh upgrades 64
COP Files 65
COP File Installation 66
Upgrade Process 66
Accessing the Upgrade File 68
Upgrade Task Lists 68
Standard Upgrade of Unified Communications Manager and IM and Presence Nodes 68
Refresh Upgrade of Unified Communications Manager and IM and Presence Nodes 70
Standard Upgrade of Unified Communications Manager Nodes Only 72
Refresh Upgrade Of Unified Communications Manager Nodes Only 73
Standard Upgrade of IM and Presence Nodes Only 74
Refresh Upgrade of IM and Presence Nodes Only 75

Parallel Upgrades 76
Pre-Upgrade Tasks 77
Perform Pre-Upgrade Tasks 77
Change Virtual Machine Configuration Specifications 79
Upgrade vSphere ESXi 80
Obtain Upgrade File 81
Upgrade Tasks 81
Before You Begin 81
Upgrade Procedures 82
Upgrade From a Local Source 82
Upgrade From a Remote Source 83
Change Virtual Machine Configuration Specifications 85
Version Switching 86
Switch Software Version 87
Switch to Previous Version 88
Switch Cluster to Previous Version 88
Switch Node to Previous Version 89
Reset Database Replication 89
Switch version back to Cisco Unified Presence 8.6(3) or earlier 89
Post-Upgrade Tasks 90
Post-Upgrade Tasks for All Nodes 91
Update VMWare Tools 91
Locale Installation 91
Install Locale Installer on Cisco Unified Communications Manager 92
Install Locale Installer on IM and Presence Service 93
Error Messages 95
Supported Products 96
Post-Upgrade Tasks for Cisco Unified Communications Manager Nodes 97
Restore Settings 97
Test Functionality 97
Dial Plan Installation 98
Manage TFTP Server Files 98
Set Up a Custom Log-On Message 99
Configure IPSec Policies 99
Post-Upgrade Tasks for IM and Presence Nodes 100

Post-upgrade tasks 100
High Availability 100
Verify IM and Presence Service Data Migration 100
Troubleshooting 101
Troubleshooting Unified Communications Manager Upgrades 101
Upgrade Failure 101
Upgrade Fails with Insufficient Disk Space 101
Reduced Permissions for Access Control Groups 102
Loss of Phone Settings 102
Post-Upgrade Failure of Unified Communications Manager Publisher Node 102
Post-Upgrade Failure of Unified Communications Manager Subscriber Nodes 102
Troubleshooting IM and Presence Upgrades 103
Upgrade Failure of IM and Presence Database Publisher Node 103
Upgrade Failure of IM and Presence Subscriber Node 103
IM and Presence user phone presence problems 104
Presence User Experiences Issues Obtaining Availability 104
Real-Time Monitoring Tool alert for Cisco SIP proxy service 104
Cannot find upgrade file on remote server 104
Upgrade file checksum values do not match 105
Database replication did not complete 105
Cisco UP Presence Engine database does not restart 105
Version Errors 105
Failed refresh upgrade 106
Cancelled or failed upgrade 106
Directory Was Located and Searched but No Valid Options or Upgrades Were Available 106
Common Partition Full Upgrade Failure 107

PART II IM and Presence Service OS platform 109

CHAPTER 9 Getting started 111
Sign in to Cisco Unified IM and Presence Operating System Administration 111
Recover Administrator password 112
Create customized log-on message 113

CHAPTER 10 Settings 115

IP settings 115

Change Ethernet settings 115

Change publisher node IP address on subscriber nodes 116

Troubleshoot publisher node IP address change on subscriber node 117

NTP settings 117

Change SMTP settings 118

Change time settings 118

Correct time zone data 118

CHAPTER 11 Shutdown and restart 119

Shut down system 119

Work with Disk Partitions 120

Revert IM and Presence node to previous version 120

Restart current version 120

CHAPTER 12 Security 123

Browser security 123

Verify Internet Explorer Security Settings 123

Create login banner 123

IPsec policy management 124

Create IPsec policy 124

Enable or Disable existing IPsec policy 126

Delete IPsec policy 127

CHAPTER 13 Security certificate management 129

Certificates and certificate trust list management 129

View Certificates 129

Download certificate or certificate trust list 130

Delete certificate 131

Regenerate certificate 131

Upload certificate or certificate trust list 133

Configure Certificate Revocation 134

Troubleshoot certificate errors 135

Third Party CA certificates 135
Third-party certificate process management 136
Generate certificate signing request 137
Download certificate signing request 137
Monitor certificate expiration dates 138

CHAPTER 14 OpenAM Single Sign-On 139
OpenAM Single Sign-On 139
Introduction 139
Set up OpenAM Single Sign-On 139

CHAPTER 15 Software Upgrades 141
Software upgrades 141
Locale-specific upgrades 141
Locale installer 141
Locale file installation 142
Error Messages 142

CHAPTER 16 Utilities 145
Ping another node 145
Set up a remote account 146
Configure remote support 146

APPENDIX A Component status in Cisco Unified Operating System 149
View Cluster Nodes Status 149
View Hardware Status 150
View Network Status 151
View Installed Software 152
View System Status 152
View IP Preferences 153

Preface

- Purpose, page xi
- Audience, page xi
- Organization, page xi
- Related Documentation, page xii
- Conventions, page xii
- Obtain Support, page xiii

Purpose

This document provides information about using the Cisco Unified Communications Operating System graphical user interface (GUI).

For information about the command line interface (CLI), which can be used to perform many common system- and network-related tasks, see the Command Line Interface Reference Guide for Cisco Unifed Communications Solutions.

Audience

This document provides information for network administrators who are responsible for managing and supporting the Cisco Unified Communications Operating System. Network engineers, system administrators, or telecom engineers use this guide to learn about, and administer, the operating system features. This guide requires knowledge of telephony and IP networking technology.

Organization

The following table shows how this guide is organized:

Chapter	Description
Part 1	“Cisco Unified Communications Manager OS platform” Describes the Cisco Unified Communications operating system functions and provides information to manage the operating system using the Graphical User Interface.
Part 2	“IM and Presence service OS platform” Provides functional descriptions and instructions for the management of the IM and Presence service operating system.

Related Documentation

For further information about related Cisco IP telephony applications and products, refer to the Cisco Unified Communications Manager Documentation Guide for your release at

`http://cisco.com/en/US/products/sw/voicesw/ps556/products_documentation_roadmaps_list.html`

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in italics.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
screen font	Terminal sessions and information the system displays are in screen font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in italic screen font.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.

Convention	Description
< >	Nonprinting characters, such as passwords, are in angle brackets.

Notes use the following conventions:

Note Means reader take note. Notes contain helpful suggestions or references to material not covered in the publication.

Timesavers use the following conventions:

Timesaver Means the described action saves time. You can save time by performing the action described in the paragraph.

Tips use the following conventions:

Tip Means the information contains useful tips.

Cautions use the following conventions:

Caution Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

Warnings use the following conventions:

Warning This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents.

Obtain Support

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at

`http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html`

Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority

to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

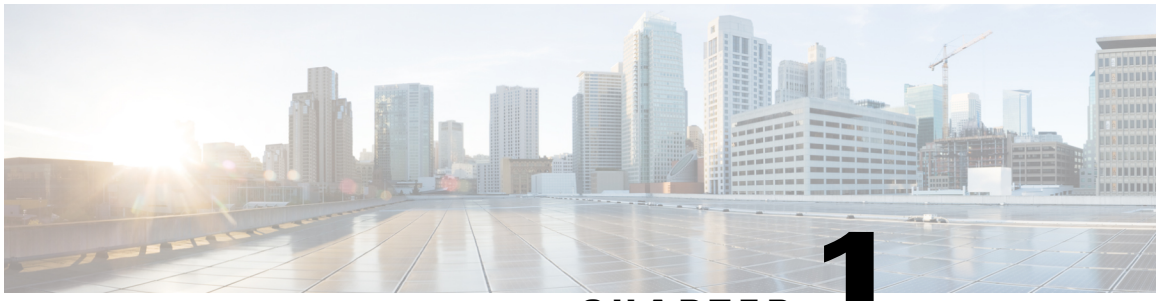
Further information regarding U.S. export regulations may be found at

`http://www.access.gpo.gov/bis/ear/ear_data.html`

PART I

Cisco Cisco Unified Communications Manager OS platform

- Cisco Unified Operating System Overview, page 3
- Operating System Administration, page 7
- Status and Configuration, page 11
- Settings, page 19
- System Restart, page 25
- Security, page 29
- Services, page 51
- Software Upgrades, page 55



CHAPTER 1

Cisco Unified Operating System Overview

- Cisco Unified Operating System Administration Overview, page 3
- Operating System Status, page 3
- Settings, page 4
- Security Configuration, page 4
- Software Upgrades, page 4
- Services, page 5
- CLI, page 5

Cisco Unified Operating System Administration Overview

Cisco Unified Communications Operating System Administration allows you to configure and manage the Cisco Unified Communications Operating System. You can perform these 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

From the **Show** menu, you can check the status of various operating system components:

- Clusters and nodes

- Hardware
- Network
- System
- Installed software and options

Settings

From the **Settings** menu, you can view and update the following operating system settings:

- IP—Updates the IP addresses and DHCP client settings that were entered when the application was installed.
- NTP Server settings—Configures the IP addresses of an external NTP server; add a new NTP server.
- SMTP settings—Configures the Simple Mail Transfer Protocol (SMTP) host that the operating system will use for sending email notifications.

From the **Settings** > **Version** window, you can choose from the following options for restarting or shutting down the system:

- Switch Versions—Switches the active and inactive disk partitions and restarts the system. You normally choose this option after the inactive partition has been updated and you want to start running a newer software version.
- Current Version—Restarts the system without switching partitions.
- Shutdown System—Stops all running software and shuts down the node.

Security Configuration

The operating system security options enable you to manage security certificates and Secure Internet Protocol (IPsec). From the **Security** menu, you can choose the following security options:

- Certificate Management—Manages certificates and Certificate Signing Requests (CSR). 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

Use the software upgrade options to 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 detailed tasks, 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 do all software installations and upgrades by using the software upgrade features that are included in the Cisco Unified Communications Operating System GUI and CLI. The system can upload and process only software that is approved by Cisco Systems. You cannot install or use third-party or Windows-based software applications that you may have been using with a previous version of Cisco Unified Communications Manager.

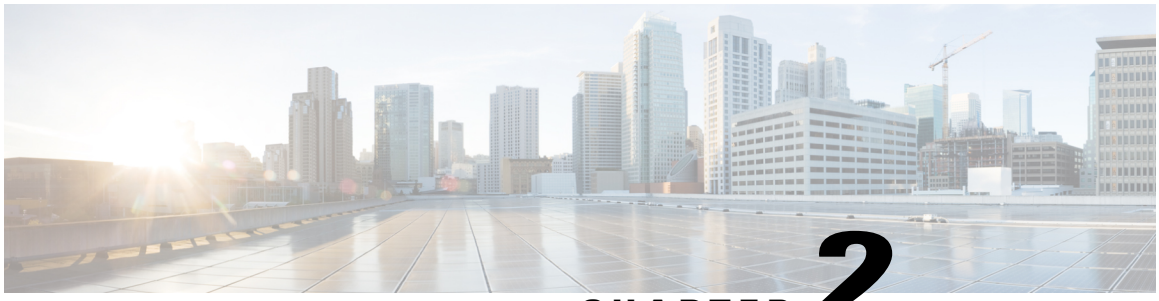
Services

The application provides the following operating system utilities:

- Ping —Checks connectivity with other devices in your network.
- 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 console or through a secure shell connection to the server. For more information, see the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*.



CHAPTER 2

Operating System Administration

This chapter describes the procedure for accessing the Cisco Unified Communications Operating System Administration and also provides procedures for resetting a lost password.

- Log In, page 7
- Reset Passwords, page 8

Log In

To access Cisco Unified Communications Operating System Administration and log in, follow this procedure.

Note Do not use the browser controls (for example, the Back button) while you are using Cisco Unified Communications Operating System Administration.

Procedure

Step 1 Log in to Cisco Unified Communications Manager Administration.

Step 2 From the Navigation menu in the upper, right corner of the Cisco Unified Communications Manager Administration window, choose **Cisco Unified OS Administration** and click **Go**.
The Cisco Unified Communications Operating System Administration Logon window displays.

Note You can also access Cisco Unified Communications Operating System Administration directly by entering the following URL:

```
http://node-name/cmplatform
```

Step 3 Enter your Administrator username and password.

Note The Administrator username and password get established during installation or created by using the command line interface.

Step 4 Click **Submit.**
The Cisco Unified Communications Operating System Administration window displays.

Reset Passwords

If you lose the administrator password or security password, use the following procedure to reset these passwords.

To perform the password reset process, you must be connected to the system through the system console, that is, you must have a keyboard and monitor connected to the server. You cannot reset a password when connected to the system through a secure shell session.

Caution 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.

Caution 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 Cisco Unified Communications Manager Administration windows on the subscriber nodes.

Note During this procedure, you must remove and then insert a valid CD or DVD in the disk drive to prove that you have physical access to the system.

Procedure

Step 1 Log in to the system with the following username and password:
a) Username: pwrecovery
b) Password: pwreset
The Welcome to platform password reset window displays.

Step 2 Press any key to continue.

Step 3 If you have a CD or DVD in the disk drive, remove it now.

Step 4 Press any key to continue.
The system tests to ensure that you have removed the CD or DVD from the disk drive.

Step 5 Insert a valid CD or DVD into the disk drive.
Note For this test, you must use a data CD, not a music CD.
The system tests to ensure that you have inserted the disk.

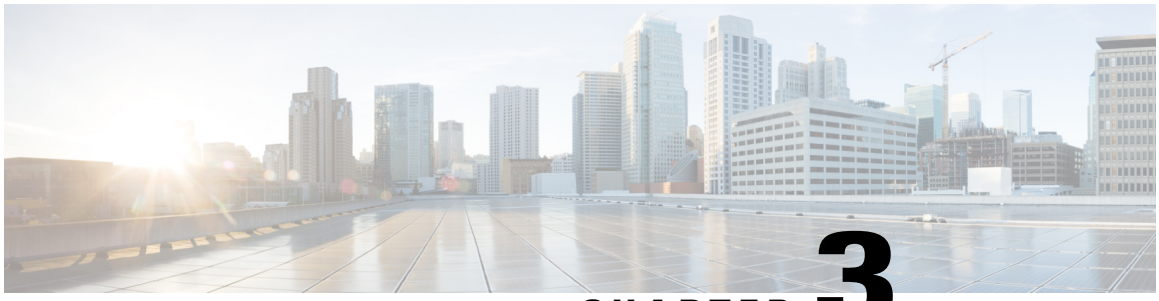
Step 6 After the system verifies that you have inserted the disk, you get prompted to enter one of the following options to continue:
a) Enter a to reset the administrator password.
b) Enter s to reset the security password.
c) Enter q to quit.

Step 7 Enter a new password of the type that you chose.

Step 8 Reenter the new password.

The password must contain at least 6 characters. The system checks the new password for strength. If the password does not pass the strength check, you get prompted to enter a new password.

Step 9 After the system verifies the strength of the new password, the password gets reset, and you get prompted to press any key to exit the password reset utility.



CHAPTER 3

Status and Configuration

This chapter provides information on administering the system.

- Show Cluster Nodes, page 11
- Show Hardware Status, page 12
- Show Network Configuration, page 13
- Show Installed Software, page 14
- Show System Status, page 15
- Show IP Preferences, page 16

Show Cluster Nodes

To view information about the nodes in the cluster, follow this procedure.

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Show** > **Cluster**.
The Cluster Nodes window appears.

Step 2 For a description of the fields on the Cluster Nodes window, see the following table.

Table 1: Cluster Nodes Field Descriptions

Field	Description
Hostname	Displays the complete hostname of the node.
IP Address	Displays the IP address of the node.
Alias	Displays the alias name of the node, when defined.

Field	Description
Server Type	Displays the following node types in the cluster: • Cisco Unified Communications Manager Voice/Video • Cisco Unified Communications Manager IM and Presence
Database Replication	Indicates whether the node is a Cisco Unified Communications Manager database publisher node or a Cisco Unified Communications manager subscriber node.

Show Hardware Status

To view the hardware status, follow this procedure:

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Show** > **Hardware**.
The Hardware status window displays.

Step 2 For descriptions of the fields on the Hardware Status window, see the following table.

Table 2: Hardware Status Field Descriptions

Field	Description
Platform Type	Displays the model identity of the platform server.
Processor Speed	Displays the processor speed.
CPU Type	Displays the type of processor in the platform server.
Memory	Displays the total amount of memory in MBytes.
Object ID	Displays the object ID.
Unified OS Version	Displays the operating system version.
RAID Details	Displays details about the RAID drive, including controller information, logical drive information, and physical device information.

Show Network Configuration

The network status information that displays depends on whether Network Fault Tolerance is enabled. When Network Fault Tolerance is enabled, Ethernet port 1 automatically takes over network communications if Ethernet port 0 fails. If Network Fault Tolerance is enabled, network status information displays for the network ports Ethernet 0, Ethernet 1, and Bond 0. If Network Fault Tolerance is not enabled, status information displays only for Ethernet 0.

To view the network status, follow this procedure:

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Show** > **Network.**
The Network Settings window displays.

Step 2 See the following table for descriptions of the fields on the Network Settings window.

Table 3: Network Configuration Field Descriptions

Field	Description
Ethernet Details	
DHCP	Indicates whether DHCP is enabled for Ethernet port 0.
Status	Indicates whether the port is Up or Down for Ethernet ports 0 and 1.
IP Address	Shows the IP address of Ethernet port 0 [and Ethernet port 1 if Network Fault Tolerance (NFT) is enabled].
IP Mask	Shows the IP mask of Ethernet port 0 (and Ethernet port 1 if NFT is enabled).
Link Detected	Indicates whether an active link exists.
Queue Length	Displays the length of the queue.
MTU	Displays the maximum transmission unit.
Mac Address	Displays the hardware address of the port.
Receive Statistics (RX)	Displays information on received bytes, packets, and errors, as well as dropped and overrun statistics.

Field	Description
Transmit Statistics (TX)	Displays information on transmitted bytes, packets, and errors, as well as dropped, carrier, and collision statistics.
DNS Details	
Primary	Displays the IP address of the primary domain name server.
Secondary	Displays the IP address of the secondary domain name server.
Options	Displays the configured DNS options.
Domain	Displays the domain of the server.
Gateway	Displays the IP address of the network gateway on Ethernet port 0.

Show Installed Software

To view the software versions and installed software options, follow this procedure:

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Show** > **Software**.
The Software Packages window displays.

Step 2 For a description of the fields on the Software Packages window, see the following table.

Table 4: Software Packages Field Descriptions

Field	Description
Partition Versions	Displays the software version that is running on the active and inactive partitions.
Active Version Installed Software Options	Displays the versions of installed software options, including locales and dial plans, that are installed on the active version.

Field	Description
Inactive Version Installed Software Options	Displays the versions of installed software options, including locales and dial plans, that are installed on the inactive version.

Show System Status

To view the system status, follow this procedure:

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Show** > **System**.
The System Status window displays.

Step 2 See the following table for descriptions of the fields on the Platform Status window.

Table 5: System Status Field Descriptions

Field	Description
Host Name	Displays the name of the host where Cisco Unified Communications Operating System is installed.
Date	Displays the date and time based on the continent and region that were specified during operating system installation.
Time Zone	Displays the time zone that was chosen during installation.
Locale	Displays the language that was chosen during operating system installation.
Product Version	Displays the operating system version.
Unified OS Version	Displays the Unified OS version.
Uptime	Displays system uptime information.
CPU	Displays the percentage of CPU capacity that is idle, the percentage that is running system processes, and the percentage that is running user processes.
Memory	Displays information about memory usage, including the amount of total memory, free memory, and used memory in KBytes.

Field	Description
Disk/active	Displays the amount of total, free, and used disk space on the active disk.
Disk/inactive	Displays the amount of total, free, and used disk space on the inactive disk.
Disk/logging	Displays the amount of total, free, and disk space that is used for disk logging.

Show IP Preferences

You can use the IP Preferences window to display a list of registered ports that the system can use. The IP Preferences window contains the following information:

- Application
- Protocol
- Port Number
- Type
- Translated Port
- Status
- Description

To access the IP Preferences window, follow this procedure.

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, choose **Show** > **IP Preferences**.
The IP Preferences window displays. Records from an active (prior) query may also display in the window.

Step 2 To find all records in the database, ensure the dialog box is empty and click **Find**.
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.

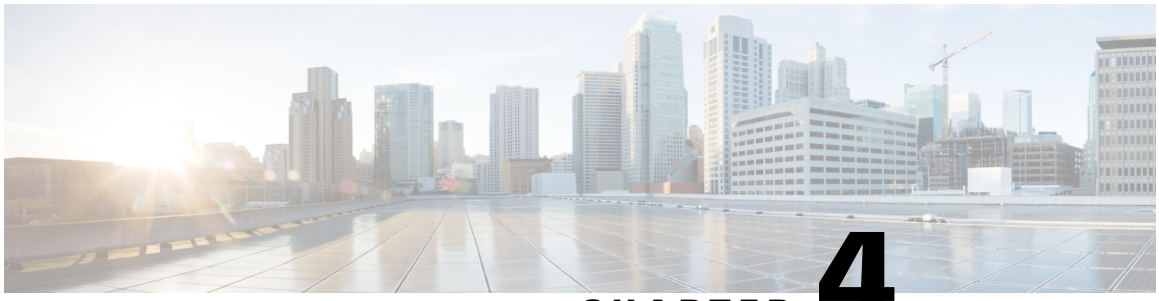
Note To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the **Clear Filter** button to remove all added search criteria.

Step 3 Click **Find**.
All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

For a description of the IP Preferences fields, see the following table.

Table 6: IP Preferences Field Descriptions

Field	Description
Application	Name of the application using (listening on) the port.
Protocol	Protocol used on this port (TCP, UDP, and so on).
Port Number	Numeric port number.
Type	Type of traffic allowed on this port: • Public - All traffic allowed • Translated - All traffic allowed but forwarded to a different port • Private - Traffic only allowed from a defined set of remote servers, for example, other nodes in the cluster
Translated Port	Traffic destined for this port get forwarded to the port listed in the Port Number column. This field applies to Translated type ports only.
Status	Status of port usage: • Enabled - In use by the application and opened by the firewall • Disabled - Blocked by the firewall and not in use
Description	Brief description of how the port is used.



CHAPTER 4

Settings

This chapter provides information about using the Settings options to display and change IP settings, host settings, and Network Time Protocol (NTP) settings.

- IP Settings, page 19
- Set Up NTP Servers, page 22
- Set Up SMTP Settings, page 23
- Set Up Time Settings, page 23

IP Settings

The IP Settings options allow you to view and change IP and port setting for the Ethernet connection and, on Cisco Unified Communications Manager subscriber nodes, to set the IP address of the Cisco Unified Communications Manager database publisher node.

Set Up Ethernet Settings

The IP Settings window indicates whether Dynamic Host Configuration Protocol (DHCP) is active and also provides the related Ethernet IP addresses, as well as the IP address for the network gateway.

All Ethernet settings apply only to Eth0. You cannot configure any settings for Eth1. The Maximum Transmission Unit (MTU) on Eth0 defaults to 1500.

To view or change the IP settings, follow this procedure:

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Settings** > **IP** > **Ethernet**.
The Ethernet Settings window appears.

Step 2 To modify the Ethernet settings, enter the new values in the appropriate fields. For a description of the fields on the Ethernet Settings window, see the following table.

Table 7: Ethernet Configuration Fields and Descriptions

Field	Description
DHCP	Indicates whether DHCP is Enabled or Disabled. **Note** If you enable DHCP, the Port and Gateway settings get disabled and cannot be changed.
Hostname	Displays the host name of the node.
IP Address	Displays the IP address of the system.
Subnet Mask	Displays the IP subnet mask address.
Default Gateway	Shows the IP address of the network gateway.

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

Caution Changing IP address or host of a node can affect system performance. For detailed information, see *Changing the IP Address and Host Name for Cisco Unified Communications Manager* at http://cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Set Up IPv6

Use the following procedure to enable and configure IPv6 on the node.

Note All Ethernet settings apply only to Eth0. You cannot configure any settings for Eth1. The Maximum Transmission Unit (MTU) on Eth0 defaults to 1500.

Procedure

Step 1 From the Cisco Unified Operating System Administration window, navigate to **Settings** > **IP** > **Ethernet IPv6**.
The Ethernet IPv6 Configuration window displays.

Step 2 To modify the Ethernet settings, enter the new values in the appropriate fields. For a description of the fields on the Ethernet IPv6 Configuration window, see the following table.

Table 8: Ethernet IPv6 Configuration Fields and Descriptions

Field	Description
Enable IPv6	Check this check box to enable IPv6 on the node.

Field	Description
Address Source	Choose one of the following IP address sources: • Router Advertisement • DHCP • Manual Entry/Mask Be aware that the three IP address sources are mutually exclusive. **Note** Unless you specify Manual Entry, the IP Address and Mask fields remain read only.
IPv6 Address	If you chose Manual Entry, enter the IPv6 address of the node; for example: fd6:2:6:96:21e:bff:fecc:2e3a
IPv6 Mask	If you chose Manual Entry, enter the IPv6 mask; for example: 64
Update with Reboot	If you want the system to reboot immediately after you click Save, check this check box. If you want to reboot later, leave the check box blank. **Note** For the IPv6 settings to take effect, you must reboot the system.

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

Note If you check the Update with Reboot check box, the system reboots after you click Save. For the IPv6 settings to take effect, you must reboot the system.

Set Up Publisher Settings

Be aware that this feature is only applicable if Cisco Unified Communications Manager is installed alone on the node.

On Cisco Unified Communications Manager subscriber nodes, you can view or change the IP address of the Cisco Unified Communications Manager database publisher node.

Note For detailed instructions about changing the IP address and hostname of nodes in a cluster, see *Changing the IP Address and Host Name for Cisco Unified Communications Manager*.

To view or change the IP settings of the Cisco Unified Communications Manager database publisher node, follow this procedure:

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Settings** > **IP** > **Publisher**.
The Publisher Settings window displays.

Note You can only view and change the IP address of the Cisco Unified Communications Manager database publisher node on Cisco Unified Communications Manager subscriber nodes of the cluster, not on the Cisco Unified Communications Manager database publisher node itself.

Step 2 Enter the new IP address of the Cisco Unified Communications Manager database publisher node.

Step 3 Click **Save**.

Set Up IP Address

If the IP address of the Cisco Unified Communications Manager database publisher node gets changed while a Cisco Unified Communications Manager subscriber node is offline, you may not be able to log in to Cisco Unified Communications Manager Administration on the subscriber node. If this occurs, follow this procedure:

Procedure

Step 1 Log in directly to operating system administration on the Cisco Unified Communications Manager subscriber node by using the following IP address:
`http://node-name/iptplatform`

where node-name specifies the host name or IP address of the Cisco Unified Communications Manager subscriber node.

Step 2 Enter your Administrator user name and password and click **Submit**.

Step 3 Navigate to **Settings** > **IP** > **Publisher**.

Step 4 Enter the new IP address for the Cisco Unified Communications Manager database publisher node and click **Save**.

Step 5 Restart the Cisco Unified Communications Manager subscriber node.

Set Up NTP Servers

Ensure that external NTP servers are stratum 5 or lower.

We recommend that the NTP for the publisher is set to stratum 1, 2, or 3, and that you use only a Linux or IOS NTP source. Windows Time Services as an NTP server is not recommended or supported.

Note You can only configure the NTP server settings on the Cisco Unified Communications Manager database publisher node.

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Settings** > **NTP Servers**.
The NTP Server Settings window displays.

Step 2 You can add, delete, or modify an NTP server:

Note To avoid potential compatibility, accuracy, and network jitter problems, the external NTP servers that you specify for the primary node must be NTP v4 (version 4). If you are using IPv6 addressing, external NTP servers must be NTP v4.

a) To delete an NTP server, check the check box in front of the appropriate server and click **Delete**.
b) To add an NTP server, click **Add**, enter the hostname or IP address, and then click **Save**.
c) To modify an NTP server, click the IP address, modify the hostname or IP address, and then click **Save**.

Note Any change that you make to the NTP servers can take up to 5 minutes to complete. Whenever you make any change to the NTP servers, you must refresh the window to display the correct status.

Step 3 To refresh the NTP Server Settings window and display the correct status, choose **Settings** > **NTP**.

Note After deleting, modifying, or adding the NTP server, you must restart all other nodes in the cluster for the changes to take affect.

Set Up SMTP Settings

The SMTP Settings window allows you to view or set the SMTP hostname and indicates whether the SMTP host is active.

Tip If you want the system to send you e-mail, you must configure an SMTP host.

To access the SMTP settings, follow this procedure:

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Settings** > **SMTP**.
The SMTP Settings window displays.

Step 2 Enter or modify the SMTP hostname or IP address.

Step 3 Click **Save**.

Set Up Time Settings

To manually configure the time, follow this procedure:

Note Before you can manually configure the server time, you must delete any NTP servers that you have configured.

Caution If you enter a time that is before the time when Cisco Unified Communications Manager was installed on the server, the digital certificates that the server uses for security become invalid, causing the web server (Tomcat) to stop working. If this happens, you must regenerate the certificates.

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Settings** > **Time**.

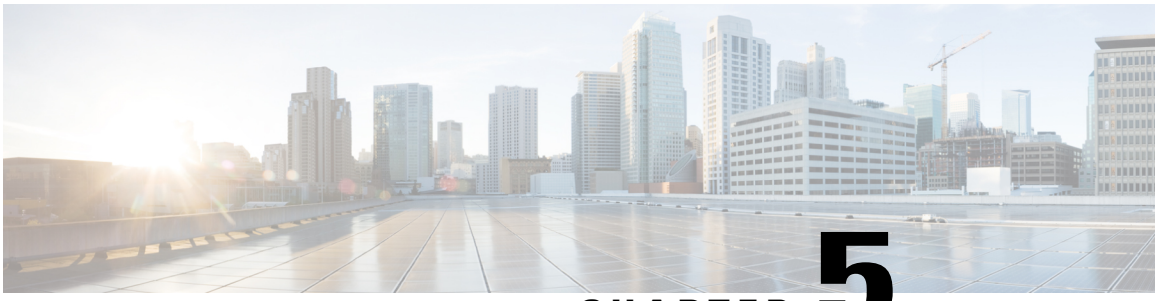
Step 2 Enter the date and time for the system.

Step 3 Click **Save**.

Step 4 On a Cisco Unity Connection server, if you changed the date or if you changed the time by more than two minutes, use the CLI command **utils system restart** to restart the server.

Related Topics

Set Up NTP Servers, on page 22



CHAPTER 5

System Restart

This chapter provides procedures for using the restart options.

- Switch Software Versions, page 25
- Restart Current Version, page 26
- Shut Down System, page 26

Switch Software Versions

You can use this option both when you are upgrading to a newer software version and when you need to fall back to an earlier software version. To shut down the system that is running on the active disk partition and then automatically restart the system by using the software version on the inactive partition, follow this procedure:

Note If you downgrade a cluster to a nonsecure previous release of Cisco Unified Communications Manager (prior to release 8.0), you must prepare the cluster for rollback before you switch versions. If you do not prepare the cluster for rollback before you revert to a previous release, you have to manually delete the ITL file on each Cisco Unified IP Phone in the system. For more information, see the *Cisco Unified Communications Manager Security Guide*.

Caution This procedure causes the system to restart and become temporarily out of service.

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Settings** > **Version**.
The Version Settings window, which shows the software version on both the active and inactive partitions, displays.

Step 2 To switch versions and restart, click **Switch Versions**. To stop the operation, click **Cancel**.
If you click **Switch Versions**, the system restarts, and the partition that is currently inactive becomes active.

Restart Current Version

To restart the system on the current partition without switching versions, follow this procedure:

Caution This procedure causes the system to restart and become temporarily out of service.

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Settings** > **Version**.
The Version Settings window, which shows the software version on both the active and inactive partitions, displays.

Step 2 To restart the system, click **Restart** or, to stop the operation, click **Cancel**.
If you click **Restart**, the system restarts on the current partition without switching versions.

Shut Down System

Caution Do not press the power button on the server to shut down the server or to reboot the server. If you do, you may accidentally corrupt the file system, which may prevent you from being able to reboot your server.

To shut down the system, follow Procedure 1 or Procedure 2.

Caution This procedure causes the system to shut down.

Procedure

Perform one of the following:

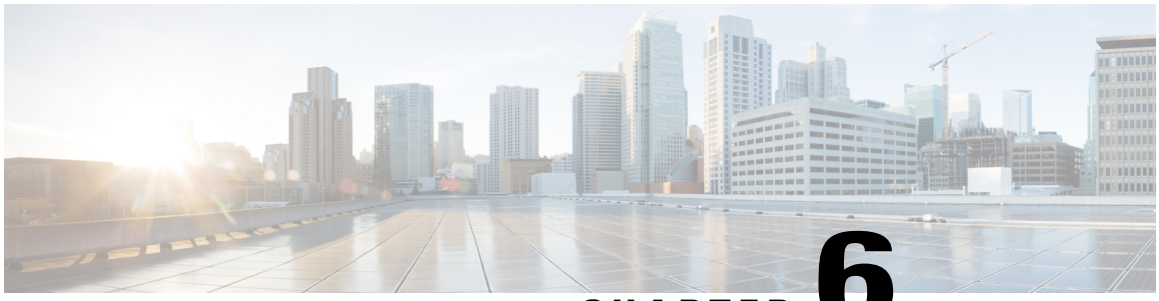
a) Shut down the system from the Cisco Unified Communications Operating System Administration window.

1. Navigate to **Settings** > **Version**. The **Version Settings** window displays, which shows the software version on both the active and inactive partitions.
2. Click **Shutdown** to shut down the system, or click **Cancel** to stop the operation.

   If you click **Shutdown**, the system halts all processes and shuts down.

b) Shut down the system using the CLI. Run the CLI command **utils system shutdown** or the command **utils system restart**.

For information on how to run CLI commands, refer to the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*.



CHAPTER 6

Security

This chapter provides information about certificate management and IPsec management and provides procedures for performing related tasks.

- Set Up Internet Explorer Security Options, page 29
- Manage Certificates, page 29
- IPsec, page 41
- Bulk Certificate Management, page 48
- Configure OpenAM SSO Application, page 49

Set Up Internet Explorer Security Options

To download certificates from the Cisco Unified Communications Manager node, ensure that your Internet Explorer security settings are configured as follows:

Procedure

Step 1 Start Internet Explorer.
Step 2 Choose **Tools** > **Internet Options**.
Step 3 Click the **Advanced** tab.
Step 4 Scroll down to the Security area on the Advanced tab.
Step 5 If necessary, uncheck the **Do not save encrypted pages to disk** check box.
Step 6 Click **OK**.

Manage Certificates

The following topics describe the functions that you can perform from the Certificate Management menu.

Note To access the Security menu items, you must sign in to Cisco Unified Communications Operating System Administration again using your administrator password.

Restart the following services after regenerating or uploading certificates:

Certificate	Services to restart
CUP	Cisco SIP Proxy, Cisco Presence Engine
cup-trust	Cisco SIP Proxy, Cisco Presence Engine
cup-xmpp	Cisco XCP Connection Manager, Cisco XCP Web Connection Manager
cup-xmpp-s2s	Cisco XCP XMPP Federation Connection Manager
cup-xmpp-trust	Cisco XCP Connection Manager, Cisco XCP Web Connection Manager, Cisco XCP XMPP Federation Connection Manager
tomcat	Cisco Tomcat
tomcat-trust	Cisco Tomcat

Show Certificates

To display existing certificates, follow this procedure:

Procedure

Step 1 Choose **Security** > **Certificate Management**.
The Certificate List window appears.

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

Step 3 To view details of a certificate or trust store, click the file name.
The Certificate Configuration window displays information about the certificate.

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

Download Certificate

To download a certificate from the Cisco Unified Communications Operating System to your PC, follow this procedure:

Procedure

Step 1 Navigate to **Security** > **Certificate Management**.
The Certificate List window displays.

Step 2 You can use the Find controls to filter the certificate list.

Step 3 Click the file name of the certificate.
The Certificate Configuration window displays.

Step 4 Click **Download**.

Step 5 In the File Download dialog box, click **Save**.

Install Intermediate Certificate

Unified Intelligence Center supports only one level of intermediate certificate. To install an intermediate certificate you must install a root certificate first and then upload the signed certificate.

Procedure

Step 1 Navigate to **Security** > **Certificate Management**.
The Certificate List window displays.

Step 2 Click **Upload Certificate**.
The Upload Certificate dialog box opens.

Step 3 Select intelligenceCenter-srvr-trust from the Certificate name drop down list to install the root certificate.

Step 4 Select the file to upload by performing one of the following steps:

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

Step 5 To upload the file to the server, click the **Upload File** button.

Step 6 Navigate to **Security** > **Certificate Management**.
The Certificate List window displays.

Step 7 Click **Upload Certificate**.
The Upload Certificate dialog box opens.

Step 8 In the Upload certificate pop up window, select IntelligenceCenter-srvr from the Certificate name drop down list and enter the root certificate name.
The root certificate name is the .pem filename that was generated when the root certificate was uploaded.

Step 9 Select the file to upload by performing one of the following steps:

- In the Upload File text box, enter the path to the file.

- Click the **Browse** button and navigate to the file; then click **Open**.

Step 10 To upload the file to the server, click the **Upload File** button.

Troubleshooting Tips

Note After installing 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 get the message **Click here to continue** even after successfully installing the custom certificate.

Delete and Regenerate Certificate

These sections describe how to delete and regenerate a certificate.

Delete Trust Certificate

To delete a trust certificate, follow this procedure:

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

Procedure

Step 1 From the Cisco Unified Serviceability webpage, navigate to **Tools** > **Control Center Network Services** and stop the Cisco Certificate Change Notification service.

Step 2 Navigate to **Security** > **Certificate Management**.
The Certificate List window displays.

Step 3 You can use the Find controls to filter the certificate list.

Step 4 Click the file name of the certificate.
The Certificate Configuration window displays.

Step 5 Click **Delete**.
For more information about deleting a certificate, see the caution.

Step 6 Click **OK.**

Step 7 Restart the Cisco Certificate Change Notification service.
The selected certificate has been permanently deleted.

Regenerate Certificate

You can regenerate certificates from the Cisco Unified Communications Operating System as an operating system security function. For more information about regenerating certificates, see the *Cisco Unified Communications Manager Security Guide*.

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.

Note Certificate regeneration or upload a of third party signed certificates should be performed during maintenance.

The following table describes the system security certificates you can regenerate from the Cisco Unified Communications Operating System and the related services that must be restarted. For information about regenerating the TFTP certificate, see the *Cisco Unified Communications Manager Security Guide*.

Table 9: Certificate Names and Descriptions

Name	Description	Related Services
tomcat	This self-signed root certificate is generated during installation for the HTTPS node.	tomcat
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

If you regenerated the certificate for Cisco Certificate Authority Proxy Function (CAPF) or Cisco Unified Communications Manager and a CTL client is configured, rerun the CTL client.

After you regenerate certificates in the Cisco Unified Communications Operating System, 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 with Cisco Unified Communications Manager. For information about performing a backup, see the *Disaster Recovery System Administration Guide*.

Procedure

Step 1 Navigate to **Security** > **Certificate Management**.
The Certificate List window displays.

Step 2 Click **Generate New**.
The Generate Certificate dialog box opens.

Step 3 From the Certificate Name drop-down list, choose a certificate name .
For details about certificate names, see the Certificate Names and Descriptions table.

Step 4 From the Key Length drop-down list, choose 1024 or 2048.

Step 5 From the Hash Algorithm drop-down list, choose SHA1 or SHA256.

Step 6 Click **Generate New**.

What to Do Next

Restart all services that are affected by the regenerated certificate as listed in the Certificate Names and Descriptions table.

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

Perform a system backup to capture the newly regenerated certificates. For information about performing a backup, see the *Disaster Recovery System Administration Guide*.

Certificate Regeneration If Intracluster Communication Is Enabled Using EMCC

If intracluster communication is enabled using EMCC complete the following steps during certificate regeneration.

Procedure

	Command or Action	Purpose
Step 1	Navigate to **Advanced Features** > **EMCC** > **Intercluster Service Profile** and deactivate **EMCC Service**.	
Step 2	Logout all remotely logged in devices from **Device** > **Related Link** > **Remotely Logged In Device**.	
Step 3	Regenerate certificates.	
Step 4	Perform the Bulk Certification operation.	
Step 5	Activate the EMCC Service.	

Upload Certificate

Caution Uploading a new certificate can affect your system operations. After you upload a new certificate or certificate trust list, you must restart the Cisco Unified Communications Manager service by navigating to **Cisco Unified Serviceability** > **Tools** > **Service Activation**. For more information, see the *Cisco Unified Serviceability Administration Guide*.

The following sections describe how to upload a Certificate Authority (CA) root certificate and application certificate to the node.

Upload Certificate or Certificate Chain

Note You can upload the certificate or certificate chain to Certificate Trust or for a third-party signed certificate.

Procedure

Step 1 Navigate to **Security** > **Certificate Management**.

Step 2 The Certificate List window displays.
Click **Upload Certificate/Certificate Chain**.

The Upload Certificate/Certificate Chain dialog box opens.

Step 3 Select the certificate name from the Certificate Name list.

Step 4 Select the file to upload by doing one of the following steps:

a) In the **Upload File** text box, enter the path to the file.

b) Click the **Browse** button and navigate to the file; then, click **Open**.
Cisco Unified Communications Manager Release 8.6 supports Privacy Enhanced Mail (PEM) Base64 encoded format of X.509 certificate (only one PEM certificate in a file), Distinguished Encoding Rules (DER) format of X509 Certificate and DER format of PKCS#7 (Public-Key Cryptography Standards) Certificate Chain. The system does not support PEM format of PKCS#7 Certificate Chain.

Step 5 To upload the file to the server, click the **Upload File** button.

Related Topics

Upload Third-Party CA Certificates, on page 35

Upload Third-Party CA Certificates

Cisco Unified Communications Operating System supports certificates that a third-party CA issues with PKCS#10 Certificate Signing Request (CSR).

Note Cisco Unified Communications Manager supports SHA1 signed certificates exclusively.

The following table provides an overview of this process, with references to additional documentation:

Procedure

Step 1 Generate a CSR on the server.

Step 2 Download the CSR to your PC.

Step 3 Use the CSR to obtain an application certificate from a CA or PKCS#7 format certificate chain, which may contain application certificate along with CA certificate.
Get information about obtaining a root certificate from your CA.

Step 4 Obtain the CA certificate or certificate chain.
Get information about obtaining a root certificate from your CA.

Step 5 Upload third-party certificate.

Step 6 If you updated the certificate for CAPF or Cisco Unified Communications Manager, generate a new CTL (Certificate Trust List) file.
See the *Cisco Unified Communications Manager Security Guide*.

Rerun CTL client (if configured) after uploading third-party signed CAPF or CallManager certificate.

Step 7 Restart the services that are affected by the new certificate.
For all certificate types, restart the corresponding service (for example, restart the Tomcat service after regenerating the Tomcat certificate). In addition, if you updated the certificate for CAPF or Cisco Unified Communications Manager, restart the Cisco Certificate Authority Proxy Function and Cisco CallManager service.

Note After regenerating IPsec certificate, you must restart Cisco DRF Local and Cisco DRF Master services.

See the *Cisco Unified Communications Manager Serviceability Administration Guide* for information about restarting services.

Related Topics

Generate Certificate Signing Request, on page 37
Download Certificate Signing Request, on page 38
Third-Party CA Certificates, on page 38
Third-Party Signed Certificate or Certificate Chain, on page 36

Third-Party Signed Certificate or Certificate Chain

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

You can upload CA root certificates and application certificates by using the same **Upload Certificate** dialog box. When you upload a CA root certificate or certificate chain that contains only CA 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 CA Certificates, choose the certificate name that includes only the certificate type.

For example, choose **tomcat-trust** when you upload a Tomcat CA Certificate or CA Certificate Chain; choose **tomcat** when you upload a Tomcat application certificate or Certificate chain that contains an application certificate and CA Certificates.

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

Note Successful upload of third-party CA 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 The Directory option no longer appears in the list of Certificate Names. However, you can still upload a Directory Trust certificate to tomcat-trust, which is required for the DirSync service to work in Secure mode.

Generate Certificate Signing Request

To generate a CSR, follow these steps:

Procedure

Step 1 Navigate to **Security** > **Certificate Management**.
The Certificate List window displays.

Step 2 Click **Generate CSR**.
The Generate Certificate Signing Request dialog box opens.

Step 3 From the Certificate Name drop-down list, choose a certificate name.
For details about certificate names, see the Certificate Names and Descriptions table.

Step 4 From the Key Length drop-down list, choose 1024 or 2048.

Step 5 From the Hash Algorithm drop-down list, choose SHA1 or SHA256.

Step 6 Click **Generate CSR**.

Note Generating CSR overwrites any existing CSR.

Download Certificate Signing Request

To download a Certificate Signing Request, follow this procedure:

Procedure

Step 1 Navigate to **Security** > **Certificate Management**.
The Certificate List window displays.

Step 2 Click **Download CSR**.
The Download Certificate Signing Request dialog box opens.

Step 3 Select the certificate name from the Certificate Name list.

Step 4 Click **Download CSR**.

Step 5 In the File Download dialog box, click **Save**.

Third-Party CA Certificates

To use an application certificate that a third-party CA issues, you must obtain both the signed application certificate and the CA root certificate from the CA or PKCS#7 Certificate Chain (DER format), which contains both the application certificate and CA certificates. Retrieve information about obtaining these certificates from your CA. The process varies among CAs.

Cisco Unified Communications Operating System generates CSRs in 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 CAPF, you must obtain and upload a CA root certificate and an application certificate on each node.

For CAPF, obtain and upload a CA 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 CA. If your CA does not support the ExtensionRequest mechanism, you must enable the X.509 extensions, as follows:

- The CAPF CSR uses the following extensions:

```
X509v3 extensions:X509v3 Key Usage:
Digital Signature, Key Encipherment, Certificate Sign
X509v3 Extended Key Usage:
TLS Web Server Authentication, IPsec End System
```

- The CSRs for Cisco Unified Communications Manager, Tomcat, and IPsec use the following extensions:

Note Tomcat does not require the Key Agreement or IPsec End System key usage.

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

```
TLS Web Server Authentication, TLS Web Client Authentication, IPsec
End System
```

Note You can generate a certificate signing request (CSR) for your certificates and have them signed by a third party CA with a SHA256 signature. You can then uploads this signed certificate back to Unified Communications Manager, allowing for Tomcat and other certificates to be support SHA256.

Monitor Certificate Expiration

The system can automatically send you an e-mail message when a certificate is close to its expiration date. To view and configure the Certificate Expiration Monitor, follow this procedure:

Procedure

Step 1 To view the current Certificate Expiration Monitor configuration, navigate to **Security** > **Certificate Monitor**. The Certificate Monitor window displays.

Step 2 Enter the required configuration information. See the following table for a description of the Certificate Monitor Expiration fields.

Table 10: Certificate Monitor Field Descriptions

Field	Description
Notification Start Time	Enter the number of days before the certificate expires that you want to be notified.
Notification Frequency	Enter the frequency for notification, either in hours or days.
Enable E-mail Notification	Check the check box to enable e-mail notification.
Email IDs	Enter the e-mail address to which you want notifications sent. You can enter multiple email addresses by separating the email addresses by a semicolon (;). There should be no space between the email addresses. For example, test@cisco.com;test1@cisco.com; test2@cisco.com, and so on. **Note** For the system to send notifications, you must configure an SMTP host.

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

Certificate Revocation

The following topic describes the function that you can perform with the Certificate Revocation menu.

Configure Online Certificate Status Protocol

You can use the Online Certificate Status Protocol (OCSP) to obtain the revocation status of the certificate.

To configure OCSP, follow this procedure:

Procedure

Step 1 Navigate to **Security** > **Certificate Revocation**.
The Certificate Revocation window displays.

Step 2 Check the **Enable OCSP** check box in the Online Certificate Status Protocol Configuration area.

Step 3 Choose **Use OCSP URI from Certificate** if the certificate is configured with OCSP URI and that to be used to contact OCSP Responder.

Step 4 Choose **Use configured OCSP URI** if external or configured URI is used to contact OCSP Responder. Enter the URI of the OCSP Responder, where certificate revocation status is verified, in the OCSP Configured URI field.

Step 5 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 revocation and expiry check enterprise parameter is set to enabled.

Step 6 Enter the **Check Every** value to check the periodicity of the certificate revocation status.

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

Step 7 Click **Save**.

Warning You must upload the OCSP Responder certificate to tomcat-trust before enabling OCSP.

Note The Certificate revocation status check is performed only during upload of a Certificate or Certificate chain and the appropriate alarm will be raised if a certificate is revoked.

Troubleshoot Certificate Errors

If you encounter an error when attempting to access Cisco Unified Communications Manager services from an IM and Presence node or IM and Presence services from a Cisco Unified Communications Manager node, there may be a problem with the tomcat-trust certificate. The error message "Connection to the Server cannot be established (unable to connect to Remote Node)" will appear on the following Serviceability interface pages:

- Service Activation
- Control Center - Feature Services
- Control Center - Network Services

This procedure provides steps 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 the Cisco Unified OS Administration interface, 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 Select the certificate to obtain information about the certificate and verify that the content matches the contents of the same certificate on the remote node.

Step 3 From Cisco Unified Serviceability Administration, choose **Tools** > **Control Center - Network Services**.

Step 4 Under Platform Services, choose **Cisco Certificate Change Notification**.

Step 5 Click **Restart**.

Step 6 Wait 30 minutes. If the previous steps have not addressed the certificate error and an IM and Presence tomcat-trust certificate is present, delete the certificate. After you delete the certificate, you must manually exchange it by downloading the Tomcat certificate for each node, and uploading it to its peers as a tomcat-trust certificate. After the certificate exchange is complete, restart the Cisco Certificate Change Notification service on each affected node.

IPsec

The following topics describe the functions that you can perform with the IPsec menu.

Note IPsec is not automatically set up between nodes in the cluster during installation.

Set Up IPsec Policy

To set up a new IPsec policy and association, follow this procedure:

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.

Note IPSEC requires bi-directional provisioning, one peer for each host (or gateway).

Note When provisioning the IPsec Policy on two Call Manager nodes with one Call Manager IPsec policy protocol set to ANY and the other Call Manager IPsec policy protocol set to UDP or TCP, the validation may result in a false negative if the validation is run from the Call Manager node using the "ANY" protocol.

Caution IPsec, especially with encryption, will affect the performance of your system.

Procedure

Step 1 Navigate to **Security** > **IPSEC Configuration**.
The IPSEC Policy List window displays.

Step 2 Click **Add New**.
The IPSEC Policy Configuration window displays.

Step 3 Enter the appropriate information in the IPSEC Policy Configuration window. For a description of the fields in this window, see the following table.

Table 11: IPsec Policy and Association Field Descriptions

Field	Description
Policy Group Name	Specifies the name of the IPsec policy group. The name can contain only letters, digits, and hyphens. **Note** Do not use more than one hyphen when creating the Policy Group Name.
Policy Name	Specifies the name of the IPsec policy. The name can contain only letters, digits, and hyphens. **Note** Do not use more than one hyphen when creating the Policy Name.
Authentication Method	Specifies the authentication method. The Authentication Method field has two options Preshared Key and Certificate. If Preshared Key is selected, the Preshared Key field is editable. If Certificate is selected, the Preshared Key field is dimmed and Certificate Name field is editable.

Field	Description
Preshared Key	Specifies the preshared key if you selected Preshared Key in the Authentication Name field. **Note** Preshared IPsec keys can contain alphanumeric characters and hyphens only, not white spaces or any other characters. If you are migrating from a Windows-based version of Cisco Unified Communications Manager, you may need to change the name of your preshared IPsec keys so they are compatible with current versions of Cisco Unified Communications Manager.
Peer Type	Specifies that the peer type is different.
Certificate Name	If you choose Different for the peer type, enter the new certificate name.
Destination Address	Specifies the IP address of the destination (FQDN is not supported).
Destination Port	Specifies the port number at the destination.
Source Address	Specifies the IP address of the source (FQDN is not supported).
Source Port	Specifies the port number at the source.
Mode	Specifies Transport mode.
Remote Port	Specifies the port number to use at the destination.
Protocol	Specifies the specific protocol, or Any: • TCP • UDP • Any
Encryption Algorithm	From the drop-down list, choose the encryption algorithm. Choices are: • DES • 3DES • AES 128 • AES 256

Field	Description
Hash Algorithm	Specifies the hash algorithm: • SHA1 - Hash algorithm that is used in Phase One IKE negotiation • MD5 - Hash algorithm that is used in Phase One IKE negotiation
ESP Algorithm	From the drop-down list, choose the ESP algorithm. Choices are: • NULL_ENC • AES 128 • AES 256 • DES • 3DES • BLOWFISH • RIJNDAEL
Phase One Life Time	Specifies the lifetime for Phase One IKE negotiation in seconds.
Phase One DH	From the drop-down list, choose the Phase One DH value. Choices include: 1, 2, and 5.
Phase Two Life Time	Specifies the lifetime for Phase Two IKE negotiation in seconds.
Phase Two DH	From the drop-down list, choose the Phase Two DH value. Choices include: 1, 2, and 5.
Enable Policy	Check the check box to enable the policy.

Step 4 To set up the new IPsec policy, click **Save**.
To validate the IPSEC, navigate to **Services** > **Ping** check the **Validate IPSec** check box and click **Ping**. This ping verifies the IPSec connection.

The following table lists the field names that are displayed when the system is in Non Federal Information Processing Standard (Non FIPS) mode.

The following table lists the field names that are displayed when the system is in FIPS mode.

Table 12: IPsec Policy and Association Field Descriptions

Field	Description
Policy Group Name	Specifies the name of the IPsec policy group. The name can contain only letters, digits, and hyphens.

Field	Description
Policy Name	Specifies the name of the IPsec policy. The name can contain only letters, digits, and hyphens.
Authentication Method	Specifies the authentication method. By default, certificate is selected. **Note** Preshared key is not present in FIPS mode.
Peer Type	Specifies the peer type is different.
Certificate Name	If you choose Different for the Peer Type, enter the new certificate name.
Destination Address	Specifies the IP address or FQDN of the destination.
Destination Port	Specifies the port number at the destination.
Source Address	Specifies the IP address or FQDN of the source.
Source Port	Specifies the port number at the source.
Mode	Specifies Transport mode.
Remote Port	Specifies the port number to use at the destination.
Protocol	Specifies the specific protocol, or Any: • TCP • UDP • Any
Encryption Algorithm	From the drop-down list, choose the encryption algorithm. Choices are: • 3DES (default) • AES 128 • AES 256
Hash Algorithm	Specifies the hash algorithm SHA1 - Hash algorithm that is used in Phase One IKE negotiation

Field	Description
ESP Algorithm	From the drop-down list, choose the ESP algorithm. Choices are: • 3DES (default) • AES 128 • AES 256
Phase One Life Time	Specifies the lifetime for Phase One IKE negotiation in seconds.
Phase One DH	From the drop-down list, choose the Phase One DH value. Choices include: 1, 2, and 5.
Phase Two Life Time	Specifies the lifetime for Phase Two IKE negotiation in seconds.
Phase Two DH	From the drop-down list, choose the Phase Two DH value. Choices include: 1, 2, and 5.
Enable Policy	Check the check box to enable the policy.

Migration Characteristics

When the system switches from Non FIPS to FIPS mode, the following changes occur:

- If there is an existing IPsec policy that uses preshared keys authentication mode then the user has to remove this policy to move to FIPS mode.
- If there is an existing IPsec policy that uses certificate authentication mode and weak Encryption Algorithm as DES then the policy is migrated to stronger cipher AES128 to become operational in FIPS mode. The user is informed about this migration in the CLI.
- If there is an existing IPsec policy that uses certificate authentication mode and weak Hash Algorithm as MD5, then the policy is migrated to stronger cipher SHA1.
- If there is an existing IPsec policy that uses certificate authentication mode and weak ESP Algorithm as NULL, DES, BLOWFISH 448, RJINDAEL then the policy is migrated to stronger cipher AES128.

When system switches from FIPS to Non FIPS mode, the IPsec policy does not change.

Note The migration from FIPS to Non FIPS or vice versa causes certificate regeneration for IPsec. Therefore, after importing the remote node's regenerated certificate, the IPsec policies need to be disabled and enabled explicitly.

Note Compatible algorithm and authentication mode is required to set up an IPsec policy between two Non-FIPS systems or between a FIPS and a Non-FIPS system.

Note Compatible authentication mode is required to set up a FIPS-based IPsec policy.

Manage IPsec Policies

To display, enable or disable, or delete an existing IPsec policy, follow this procedure:

Note 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 IPsec, especially with encryption, affects the performance of your system.

Caution Any changes that you make to existing IPsec policies can affect your normal system operations.

Caution Any changes that you make to the existing IPsec certificate due to hostname/domain/IP address change would need the administrator to delete the IPsec policies and recreate IPsec policies if certificate names are changed. If certificate names are unchanged, then after importing the remote node's regenerated certificate, the IPsec policies need to be disabled and enabled explicitly.

Note To access the Security menu items, you must sign in to Cisco Unified Communications Operating System Administration again using your Administrator password.

Procedure

Step 1 Navigate to **Security** > **IPSEC Configuration**.
The IPSEC Policy List window displays.

Step 2 To display, enable, or disable a policy, follow these steps:

a) Click the policy name.
The IPSEC Policy Configuration window displays.

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**.

Bulk Certificate Management

To support the Extension Mobility Cross Cluster (EMCC) feature, the system allows you to execute a bulk import and export operation to and from a common SFTP server that has been configured by the cluster administrator.

Note If you have Cisco Unified IP Phone 8961, 9951, or 9971 Firmware Release 9.0(2) and your cluster is running in mixed mode, the Trust Certificate(s) for all clusters must be signed by a common set of security tokens in order for the EMCC feature to operate. If you manage cluster security using the Cisco CTL Client, you must have a minimum of one token that is the same among all clusters.

The minimum token requirement does not apply if you manage cluster security using the CLI.

Export Certificates

To use Bulk Certificate Management to export certificates, use the following procedure:

Procedure

Step 1 Navigate to **Security** > **Bulk Certificate Management**.
The Bulk Certificate Management window displays.

Step 2 Enter the appropriate information on the Bulk Certificate Management window.

Step 3 To save the values you entered, click **Save**.

Step 4 To export certificates, click **Export**.
The Bulk Certificate Export popup window displays.

Step 5 From the drop-down menu, choose the type of certificate you want to export:

- Tomcat
- TFTP
- Capf
- All

Step 6 Click **Export**.
The system exports and stores the certificates you chose on the central SFTP server.

Related Topics

Import Certificates, on page 49

Import Certificates

You can also use the Bulk Certificate Management window to import certificates that you have exported from other clusters. However, before the **Import** button displays, you must complete the following activities:

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

Field	Description
IP Address	Enter the IP address of the common node where you want to export the certificates.
Port	Enter the port number. Default: 22
User ID	Enter the User ID you want to use to log into the node.
Password	Enter the appropriate password.
Directory	Enter a directory on the node where you want to save the certificates. Example: /users/cisco

Configure OpenAM SSO Application

There are two types of Single Sign On (SSO): OpenAM SSO and Security Assertion Markup Language (SAML) SSO. The Cisco Unified Communications Manager Operating System interface is used to configure OpenAM SSO only. For information about SAML SSO, see the *Features and Services Guide for Cisco Unified Communications Manager*.

To configure OpenAM SSO, click **Cisco Unified OS Administration** > **Security** > **Single Sign On**.

Note SSO is supported only for End User accounts, such as Agent Flow or SAML. SSO is not supported for Application User accounts.

This application is split into three components:

- Status
- Select Applications

- Server Settings

Status

A warning message displays indicating that the change in SSO settings causes Tomcat restart.

The following error messages may display when enabling the SSO application:

- Invalid Open Access Manager (Open AM) server URL - This error message displays when you give and invalid OpenAM server URL.
- Invalid profile credentials - This error message displays when you give a wrong profile name or wrong profile password or both.
- Security trust error - This error message displays when the OpenAM certificate has not been imported.

If you get any of the above error messages while enabling SSO, then the status changes to the above errors.

Select Applications

You can select or deselect the application for enabling or disabling SSO for a specific application.

The following applications are available:

- Cisco Cisco Unified Communications Manager Administration - Enables SSO for Cisco Cisco Unified Communications Manager Administration, Cisco Unified Serviceability, and Cisco Unified Reporting
- Cisco Unified Communications Self Care Portal - Enables SSO for Cisco Unified Communications Self Care Portal
- Cisco Unified Operating System Administration - Enables SSO for Cisco Unified Operating System Administration and Disaster Recovery System
- Cisco Unified Data Service - Enables SSO for Cisco UC Integration for Microsoft Office Communicator
- RTMT - Enables the web application for Real-Time Monitoring Tool

Server Settings

The server settings are editable only when SSO is disabled for all applications.

Use the following procedure:

Procedure

Step 1 Enter the following URL of the Open Access Manager (OpenAM) server:
http://opensso.sample.com:443/opensso

Step 2 Enter the relative path where the policy agent should be deployed. The relative path must be alphanumeric.

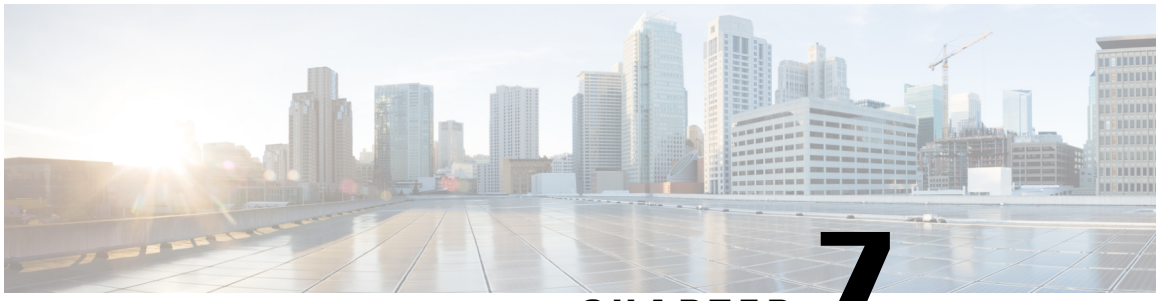
Step 3 Enter the name of the profile that is configured for this policy agent.

Step 4 Enter the password of the profile name.

Step 5 Enter the login Module instance name that is configured for Windows Desktop SSO.

Step 6 Click **Save.**

Step 7 Click **OK** on the confirmation dialog box to restart Tomcat.



CHAPTER 7

Services

This chapter provides information about the utility functions that are available on the operating system, which include pinging another system and setting up remote support.

- Ping, page 51
- Set Up Remote Support, page 52

Ping

The Ping Utility window enables you to ping another node in the network.

To ping another system, follow this procedure:

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Services** > **Ping**.
The Ping Remote window displays.

Step 2 Enter the IP address or network name for the system that you want to ping.

Step 3 Enter the ping interval in seconds.

Step 4 Enter the packet size.

Step 5 Enter the ping count, the number of times that you want to ping the system.

Note When you specify multiple pings, the ping command does not display the ping date and time in real time. Be aware that the Ping command displays the data after the number of pings that you specified completes.

Step 6 Choose whether you want to validate IPsec.

Step 7 Click **Ping**.
The Ping Remote window displays the ping statistics.

Set Up Remote Support

From the Remote Access Configuration window, you can set up a remote account that Cisco support personnel can use to access the system for a specified time.

The remote support process works like this:

1. The customer sets up a remote support account. This account includes a time limit on how long Cisco personnel can access it. This time limit can be configured to various values.
2. When the remote support account is set up, a pass phrase gets generated.
3. The customer calls Cisco support and provides the remote support account name and pass phrase.
4. Cisco support enters the pass phrase into a decoder program that generates a password from the pass phrase.
5. Cisco support logs into the remote support account on the customer system by using the decoded password.
6. When the account time limit expires, Cisco support can no longer access the remote support account.

To set up remote support, follow this procedure:

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Services** > **Remote Support**.
The Remote Access Configuration window displays.

Step 2 Enter an account name for the remote account in the **Account Name** field.
The account name must comprise at least six-characters that are all lowercase, alphabetic characters.

Step 3 Enter the account duration, in days, in the **Account Duration** field.
The default account duration specifies 30 days.

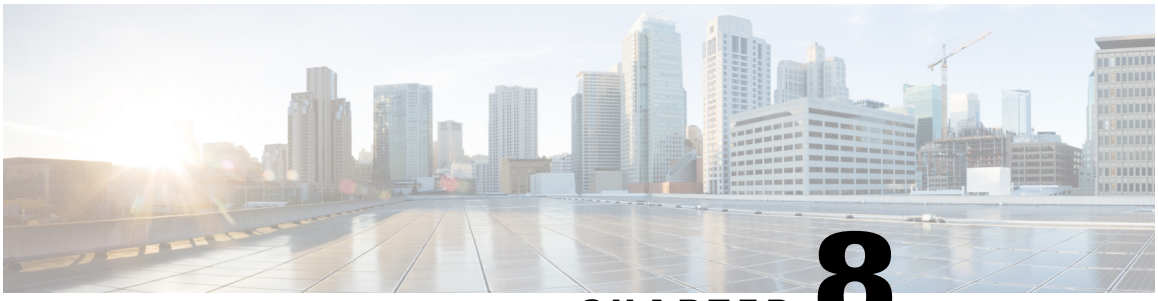
Step 4 Click **Save**.
The Remote Support Status window displays. For descriptions of fields on the Remote Support Status window, see the following table.

Table 13: Remote Support Status Fields and Descriptions

Field	Description
Decode version	Indicates the version of the decoder in use.
Account name	Displays the name of the remote support account.
Expiration	Displays the date and time when access to the remote account expires.
Pass phrase	Displays the generated pass phrase.

Step 5 To access the system by using the generated pass phrase, contact your Cisco personnel.

Step 6 To delete the remote access support account, click the **Delete** button.



CHAPTER 8

Software Upgrades

You can use the Software Upgrades options to perform the following types of installations and upgrades:

- Install/Upgrade - Use this option to upgrade the application software, install Cisco Unified Communications Manager Locale Installers and dial plans, or install Cisco Unity Connection locales, and upload and install device packs, phone firmware loads, and other COP files.
- TFTP File Management - Use this option to upload various device files for use by the phones to the TFTP server. The TFTP server files that you can upload include custom phone rings, callback tones, and phone backgrounds.

For information on upgrading Cisco Unity Connection to the shipping version, see the applicable chapter in the Reconfiguration and Upgrade Guide for Cisco Unity Connection Release 7.x at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/upgrade/guide/7xcucrugx.html.

For information on installing Cisco Unity Connection languages, see the “Installing Additional Languages” chapter of the Reconfiguration and Upgrade Guide for Cisco Unity Connection Release 7.x at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/upgrade/guide/7xcucrug027.html.

Caution 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. Note that IP phone security configurations will be modified to disable signaling and media encryption (including encryption provided by the VPN phone feature).

- Getting Started, page 56
- Upgrade Planning, page 57
- Upgrade Overview, page 64
- Pre-Upgrade Tasks, page 77
- Upgrade Tasks, page 81
- Post-Upgrade Tasks, page 90
- Troubleshooting, page 101

Getting Started

The following sections provide information about Cisco Unified Communications Manager and the IM and Presence Service, and the relationship between these nodes when they are installed together in a cluster.

About Cisco Unified Communications Manager

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

About the IM and Presence Service

IM and Presence, which is a service of Cisco Unified Communications Manager, provides native standards-based dual-protocol enterprise instant messaging (IM) and network-based availability as part of Cisco Unified Communications. This secure, scalable, and easy-to-manage service offers users feature-rich communications capabilities both within and external to the enterprise.

About the System Topology

This section provides an overview of the system topology and describes the relationship between the types of nodes in the topology.

Clusters

Clusters provide a mechanism for distributing call processing and database replication among multiple servers. They provide transparent sharing of resources and features and enable system scalability.

A cluster comprises a set of Cisco Unified Communications Manager (Unified Communications Manager) nodes and IM and Presence nodes that run compatible software versions.

Publisher Nodes and Subscriber Nodes

Within a cluster, there is a database publisher for each type of node that you install.

When you install Unified Communications Manager, the installation wizard prompts you to specify whether the node you are installing is the first node in the cluster. The first Unified Communications Manager node that you install becomes the publisher node, because it publishes the voice and video database to the other Unified Communications Manager nodes in the cluster. All subsequent nodes in the cluster are called subscriber nodes. Each subscriber node must be associated with the publisher node. You must set up all subscriber nodes in the system topology on the publisher node before you install the software on the subscriber nodes.

When you install IM and Presence nodes, the first node that you install functions as the server for the IM and Presence database. Because this node publishes the database for all of the IM and Presence nodes in the cluster, it is referred to as the IM and Presence database publisher; however, you must install this and all other IM and Presence nodes as subscribers of the Unified Communications Manager publisher node. As with other subscriber nodes, you must add these in the system topology before you install the software.

Upgrade Planning

This chapter provides the following information:

Requirements and Limitations

The following sections provide information about the requirements that your system must meet, and limitations that apply when you install or upgrade Cisco Unified Communications Manager or IM and Presence Service.

Caution Do not modify any of the IM and Presence Service server entries on the Application Server or Server configuration pages of the Cisco Unified CM Administration interface. The IM and Presence Service upgrade process automatically updates these entries on the Cisco Unified Communications Manager cluster during the final stages (switch version) of the upgrade process.

For upgrades from Release 8.x or 9.x to Release 10.x or later, any manual modification of these entries during the upgrade process will result in data migration failures between IM and Presence Service and Cisco Unified Communications Manager. If such failures occur, you must restart the entire upgrade process for both Cisco Unified Communcations Manager and IM and Presence Service clusters.

System Limitations

This section describes the limitations that apply when you install or upgrade Cisco Unified Communications Manager or the IM and Presence Service.

Subnet Limitations

Do not install Cisco Unified Communications Manager in a large Class A or Class B subnet that contains a large number of devices.

Cluster Size

The number of call processing subscriber nodes in a cluster cannot exceed 4 subscriber nodes and 4 standby nodes, for a total of 8 subscribers. The total number of servers in a cluster, including the publisher node, TFTP server, media servers, and IM and Presence nodes can not exceed 20.

Note The maximum number of IM and Presence nodes in a cluster is 6.

Support for intercluster peers

This release of IM and Presence supports intercluster peers to clusters running Cisco Unified Presence Release 8.6 and IM and Presence Release 9.x. Intercluster peers to clusters running Release 8.0(x) or Release 8.5(x) are not supported.

Network Requirements

This section lists the requirements that your network must meet before you can deploy Cisco Unified Communications Manager and the IM and Presence Service.

IP Address Requirements

You must configure the server to use static IP addressing to ensure that the server obtains a fixed IP address. Using a static IP address also ensures that Cisco Unified IP Phones can register with the application when you plug the phones into the network.

DNS requirements

Note the following DNS requirements:

- Mixed-mode DNS deployments not supported—Cisco does not support mixed-mode deployments. Both Cisco Unified Communications Manager (Unified Communications Manager) and IM and Presence must either use or not use DNS.
- If your deployment uses DNS—Unified Communications Manager and IM and Presence should use the same DNS server. If you use different DNS servers between IM and Presence and Unified Communications Manager, it is likely to cause abnormal system behavior.
- If your deployment does not use DNS—You must modify the **Host Name/IP Address** field in the service profile for the Presence and IM UC service. If DNS is not supported, you must change the **Host Name/IP Address** field to the IP address of the IM and Presence publisher node. For more information about configuring services, see *Cisco Unified Communications Manager Administration Guide*.
- Multinode considerations—If you are using the multinode feature in IM and Presence, see the section regarding multinode deployments in the *Deployment Guide for IM and Presence on Cisco Unified Communications Manager* for DNS configuration options.

SFTP Server Support

Cisco allows you to use any SFTP server product but recommends SFTP products that have been certified with Cisco through the Cisco Technology Developer Partner program (CTDP). CTDP partners, such as GlobalSCAPE, certify their products with specified versions of Cisco Unified Communications Manager. For information on which vendors have certified their products with your version of Cisco Unified Communications Manager, refer to the following URL:

`http://www.cisco.com/pcgi-bin/ctdp/Search.pl`

For information on using GlobalSCAPE with supported Cisco Unified Communications versions, refer to the following URL:

`http://www.globalscape.com/gsftps/cisco.aspx`

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 (refer to `http://sshwindows.sourceforge.net/`)
- Cygwin (refer to `http://www.cygwin.com/`)
- Titan (refer to `http://www.titanftp.com/`)

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

For issues with third-party products that have not been certified through the CTDP process, contact the third-party vendor for support.

Platform Requirements

In this release, you cannot install or run Cisco Unified Communications Manager and the IM and Presence Service directly on server hardware; you must run these applications on virtual machines.

Before you can install or upgrade the software on a virtual machine, you must:

- configure the platform
- install and configure ESXi virtualization software
- deploy the correct OVA template for the release

This section provides information about the platform requirements that you must meet before you can deploy Cisco Unified Communications Manager and the IM and Presence Service on virtual machines.

Supported Platforms

Cisco supports virtualized deployments of Unified Communications Manager and the IM and Presence Service on Cisco Unified Computing System servers, or on a Cisco-approved third-party server configuration.

Whether you use a Cisco Unified Computing System server or a Cisco-approved third-party server configuration, you must ensure that the server meets the configuration requirements of the release. The following options are available:

- a tested reference configuration (TRC)
- a specifications-based configuration

For information about the platform configuration specifications, such as CPU, memory, and storage specifications, see UC Virtualization Supported Hardware.

Information about supported platforms is also available in the following documentation:

- *Cisco Unified Communications Manager on Virtualized Servers*
- *Release Notes* for your product release
- *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*

ESXi and VMware Tools

You must install a version of vSphere ESXi hypervisor that meets the requirements of the release, as well as VMWare Tools. VMware Tools are specialized drivers for virtual hardware that is installed in the UC applications when they are running virtualized. It is very important that the VMware tools version be in sync with the version of ESXi being used. For more information, see *Cisco Unified Communications Manager on Virtualized Servers*.

If the server is running VMware EX/ESXi and the motherboard has an ICH10 onboard SATA controller, you must disable the SATA controller in the BIOS. The ICH10 onboard SATA controller is not supported by EX/ESXi.

OVA Templates

Once ESXi is running on the hardware platform, it is ready to host the virtual machines. The first step is to create the virtual machines on the host. You must use Cisco-generated OVA templates to create the virtual machines to run the Unified Communications Manager application. These OVA templates contain aligned disk partitions and other specific configurations that are required. See Virtualization for Cisco Unified Communications Manager to download the OVA file for your release.

Power Supply

Ensure that you connect each node to an uninterruptible power supply (UPS) to provide backup power and protect your system. Failure to do so may result in damage to physical media and require a new installation.

If you want the node to automatically monitor UPS signaling and automatically initiate a graceful shutdown upon power loss, Cisco Unified Communications Manager is dependent on the capabilities of the virtualization software or physical server's service processor. Please see documentation for those products for support, if any.

Software Requirements

The following sections provide information about the software requirements that your deployment must meet.

Browser Requirements

Cisco Unified Communications Manager and the IM and Presence Service both provide interfaces that you can use to configure and manage the system. You can access the interfaces by using the browsers and operating systems listed in the following table. Cisco does not support or test other browsers.

Table 14: Supported Browsers and Operating Systems

You can access Cisco Unified Communications Manager with this browser...	...if you use one of these operating systems
Microsoft Internet Explorer 8	• Microsoft Windows XP SP3 • Microsoft Windows Vista SP2 (or latest service pack available) • Microsoft Windows 7 (32-bit) (with latest service pack available)
Mozilla Firefox 3.x or 4.x (if available)	• Microsoft Windows XP SP3 • Microsoft Windows Vista SP2 (or latest service pack available) • Microsoft Windows 7 (32-bit) (latest service pack available) • Apple Mac OS X (latest service pack available)
Safari 4.x or 5.x (if available)	Apple Mac OS X (or newest OS release available)

Upgrade time requirements

The time required to upgrade the software is variable and depends on a number of factors. For large deployments, installation of the upgrade software may take several hours.

Throttling affects time required to upgrade

To preserve system stability during upgrades, the system throttles the upgrade process, which may increase the time required to complete the upgrade.

If the upgrade process is taking much longer than you would like, you can disable throttling. Although disabling throttling decreases the time it takes to perform the upgrade, it may degrade system performance.

To disable throttling, use the following command in the CLI before you start the upgrade:

```
utils iothrottle disable
```

If you want to restart throttling after you start the upgrade, you must cancel the upgrade, restart throttling, and then restart the upgrade.

System availability after upgrade

For standard upgrades, when you activate the upgraded software, the system restarts and is out of service for up to 30 minutes on the publisher node, depending on the size of the database. The length of the outage on subscriber nodes depends on how long database replication takes to complete.

If you need to revert to an earlier software version, you must restart the system which results in a similar service outage period.

Supported Upgrade Paths

The following sections provide information about the supported upgrade paths for the Cisco Unified Communications Manager and the IM and Presence Service.

Version Requirements

All servers in a cluster must run the same release of Cisco Unified Communications Manager. The only exception is during a cluster software upgrade, during which a temporary mismatch is allowed.

If you are installing IM and Presence nodes, the software version of the first IM and Presence node (the IM and Presence database publisher node) must match the first two numbers of the software version installed on the Unified Communications Manager publisher node. For example, IM and Presence Service software version 10.0.1.10000-1 is compatible with Cisco Unified Communications Manager software version 10.0.1.30000-2.

After you install the first IM and Presence node, the software version of any IM and Presence subscriber nodes that you install must match all five version numbers of the first IM and Presence node.

Upgrade Paths For Cisco Unified Communications Manager

The following table lists the range of upgrade paths that are supported for Cisco Unified Communications Manager. For more detailed information about supported upgrade paths, see the *Cisco Unified Communications Manager Software Compatibility Matrix*.

Table 15: Cisco Cisco Unified Communications Manager Upgrade Paths

From	To	Upgrade Type
8.5(x) or older	10.0(1)	Refresh upgrade, COP file needed
8.6(x) to 9.x	10.0(1)	Refresh upgrade

From	To	Upgrade Type
10.0(1)x	10.0(1)y	Standard upgrade

Upgrade Paths for IM and Presence Service

The following table lists the range of upgrade paths that are supported for the IM and Presence Services. For more detailed information about supported upgrade paths, see the *Cisco Unified Communications Manager Software Compatibility Matrix*.

Table 16: IM and Presence Service Upgrade Paths

From Cisco Unified Presence Release	To IM and Presence Release	Upgrade Type
8.5(4)	10.0(1)	Refresh upgrade, COP file needed
8.6(3) to 9.x	10.0(1)	Refresh upgrade
10.0.1.x	10.0.1.y	Standard upgrade

If you are upgrading from IM and Presence Service 10.0(1) Export Unrestricted to any higher release of IM and Presence Service Export Unrestricted (including Service Updates), you must install the following COP file before you begin the upgrade: `ciscocm.cup.unrst_upgrade_10_0_1_v1.2.cop.sgn`. You can download this file from Cisco.com.

For upgrades from Cisco Unified Presence 8.5(4), you must install a COP file on all nodes before you begin the upgrade process. You can download the COP file from Cisco.com. The name of the COP file is: `cisco.com.cup.refresh_upgrade_v<latest_version>.cop`. This COP file delivers functionality to allow the upgrade path to be supported and provides various enhancements to the user experience.

Caution If you do not install the `cisco.com.cup.refresh_upgrade_v<latest_version>.cop` COP file on all nodes for the required releases, the upgrade will fail.

Upgrade From Cisco Unified Presence Release 8.5(4)

If you upgrade from Cisco Unified Presence Release 8.0(x) or Release 8.5 to the current release, note the following:

- If you have intercluster peers to Cisco Unified Presence Release 8.0(x) or Release 8.5 clusters, you will not have intercluster availability until you upgrade all of these clusters to Release 8.6 or to Release 9.x and later. After the upgrade is complete, the previously configured peers will start working and intercluster availability will be restored.
- If you upgrade a Cisco Unified Presence Release 8.5 cluster that has High Availability (HA) enabled to Release 9.x or later, Cisco recommends that you disable HA on each presence redundancy group before you begin the upgrade. You can reenable HA on each cluster after the switch version is complete, database replication is complete, and all services are back up and running.

- During a software upgrade, the Cisco Replication Watcher service delays feature service startup on the publisher node for up to 20 minutes and on subscriber nodes indefinitely until replication is established.

Note In IM and Presence Release 10.0(1), the Cisco Replication Watcher service has been renamed to the Cisco IM and Presence Data Monitor service.

Licensing

The following sections provide information about the licensing requirements for Cisco Unified Communications Manager and the IM and Presence Service.

Cisco Unified Communications Manager License Requirements

Use the Cisco Prime License Manager to allocate and monitor the licenses for Cisco Unified Communications Manager, its applications and endpoints. See the *Cisco Prime License Manager User Guide* for information about generating and installing licenses.

Important Unused PAKs and/or licenses for versions prior to Release 9.0 cannot be installed once your system has been upgraded to Release 9.0 or later. If you have uninstalled PAKs, install all licenses before upgrading.

IM and Presence license requirements

The IM and Presence Service does not require a server license or software version license. However, you must assign users and enable the IM and Presence Service for each assigned user.

Note With the Jabber for Everyone Offer, no end user licenses are required to enable IM and Presence functionality. See the *Jabber for Everyone Quick Start Guide* for more information.

You can assign IM and Presence on a per user basis, regardless of the number of clients you associate with each user. When you assign IM and Presence to a user, this enables the user to send and receive IMs and also to send and receive availability updates. If users are not enabled for IM and Presence, they will not be able to log in to the IM and Presence server to view the availability of other users, send or receive IMs, and other users will not see their availability status.

You can enable a user for IM and Presence using any of the following options:

- The **End User Configuration** window in Cisco Unified Communications Manager. See the *Cisco Unified Communications Manager Administration Guide* for more information.
- The Bulk Administration Tool (BAT)
- Assign IM and Presence to a feature group template which you can reference from the **Quick User/Phone Add** window in Unified Communications Manager.

See the IM and Presence chapter in the *Cisco Unified Communications Manager Features and Services Guide* for more information.

IM and Presence capabilities are included within both User Connect Licensing (UCL) and Cisco Unified Workspace Licensing (CUWL). IM and Presence capabilities can also be acquired for users that are not Cisco Unified Communications Manager IP Telephony users through the Jabber for Everyone Offer. See the *Jabber for Everyone Quick Start Guide* for more information.

Upgrade Overview

This section provides the following information:

Types of upgrades

There are two types of upgrades:

- standard upgrades
- refresh upgrades

The server automatically determines whether you need to perform a standard upgrade or a refresh upgrade.

Standard upgrades

Standard upgrades are upgrades that do not require upgrades to the operating system. You can install upgrade software on your server while the system continues to operate.

For standard upgrades, you install the upgrade software as an inactive version. The system continues to function normally while you are installing the software. When the upgrade is complete, you can choose to automatically reboot the system to the upgraded software or you can manually switch to the new software at a later time. When you reboot to the new software, the old software version remains on the system. This allows you to switch back to the old version in the unlikely event of issues with the new software. During an upgrade your configuration information migrates automatically to the upgraded version.

Note You can only make changes to the database on the active software. The database for the inactive software is not updated. If you make changes to the database after an upgrade, you must repeat those changes after switching to the new software.

Refresh upgrades

Refresh upgrades are required in situations where incompatibilities exist between the old and new software releases. For example, a refresh upgrade is required when the major version of the operating system changes between the version you are upgrading from and the version that you are upgrading to. Refresh upgrades require multiple reboots during installation to upgrade the underlying operating system, causing a temporary server outage while the software is installed. The duration of this outage will depend on your configuration and the size of the database. A typical refresh upgrade takes between 1 and 4 hours per node.

Note You must perform all refresh upgrades during a maintenance window because the system will not be available during the upgrade.

For refresh upgrades, the upgrade wizard allows you to choose whether or not to automatically run the new upgrade software when the upgrade completes. If you select not to run the new software, the system will reboot to the old software version when the upgrade is complete and you can manually switch to the new software at a later time.

If for any reason you decide to revert to the prior software version, you can switch versions to the older version of the software. This switch version requires a reboot. Be aware that any configuration changes that you made after upgrading the software will be lost.

COP Files

When you perform a refresh upgrade, you must install COP files before you begin upgrading from any of the following releases:

- upgrades from Cisco Unified Communications Manager 8.5(x) and older to Cisco Unified Communications Manager 10.0(x)
- upgrades from Cisco Unified Presence 8.5(4) to IM and Presence 10.0(x)

You can download the following COP files from Cisco.com:

COP file	Purpose
ciscocm.refresh_upgrade_v<latest_version>.cop.sgn	Required. Install this file on all Unified Communications Manager nodes to update the operating system so that it supports the new release.
ciscocm.cup.refresh_upgrade_v<latest_version>.cop	Required. Install this file on all IM and Presence Service nodes to update the operating system so that it supports the new release.
ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn	Optional. This COP file expands the vDisk size. Install this COP file on either Unified Communications Manager nodes or IM and Presence Service nodes if you need to increase the vDisk space to meet the space requirements of a refresh upgrade. This option requires a reboot.
ciscocm.free_common_space_<latest_version>.cop.sgn	Optional. This COP file removes the inactive side in the common partition to increase available disk space without requiring a system rebuild. Install this COP file on Unified Communications Manager nodes or IM and Presence Service nodes as required to perform an upgrade. You can use this COP file as an alternative to the COP file listed above, or in conjunction with it. This option does not require a reboot. **Note** You will not be able to switch back to the inactive version after installing this file.

To find COP files on Cisco.com, navigate to **Support > Downloads > Cisco Unified Communications Manager Version 10.0 > Unified Communications Manager/CallManager/Cisco Unity Connection Utilities**.

Caution If you do not install the COP file on all nodes for the required releases, the upgrade will fail.

COP File Installation

The following guidelines apply to installing COP files. If the documentation for a specific COP file contradicts these general guidelines, follow the COP file documentation:

- Install the appropriate COP file on every node in a cluster. Perform this task before you install new software on each node in the cluster and set up the database.
- After you install a COP file, you must restart the node.
- Restart Cisco Unified Communications Manager to ensure that configuration changes that are made during the COP file installation get written into the database.
- Restart the IM and Presence Service to ensure that configuration changes that are made during the COP file installation get written into the database.

Upgrade Process

You can begin an upgrade using either the command line interface or graphical user interface. You can monitor progress of the upgrade using the console until the command line interface and graphical user interface access has been restored. Once these interfaces are restored, you can use the command line interface or graphical user interface to continue to monitor upgrade progress.

When you upgrade a node, the new software is installed as an inactive version. To activate the new software, you must switch the node to the new software version. There are two ways to switch to the new software version:

- automatic switching—the system switches the version automatically as part of the upgrade process
- manual switching—you switch the version using the OS Administration interface after the upgrade process is complete

The method that you choose depends on the type of upgrade that you are doing. During the upgrade process, the wizard prompts you to choose whether to switch the software version automatically by rebooting to the upgraded partition, or whether to switch the version manually at a later time. The table below lists the switching method to use for each type of upgrade.

Upgrade type	Switching type	When prompted, choose . . .	Result
Standard upgrade	Automatic	Reboot to upgraded partition	When you choose this option, the system reboots to the new software version.
	Manual	Do not reboot after upgrade	When you choose this option, the system continues to run the old software version when the upgrade is complete. You can manually switch to the new software at a later time.
Refresh upgrade	Manual	Do not switch to new version after upgrade	Use this option only if you are performing a refresh upgrade in stages. When you choose this option the system reboots to the old software version when the upgrade is complete and you manually switch to the new software at a later time. When you use this upgrade method, you must switch your publisher node to the new software version before you upgrade your subscriber nodes.
	Automatic	Switch to new version after upgrade	Choose this option to use the new software version immediately following the upgrade. When you use this upgrade method, you must switch your publisher node to the new software version before you upgrade your subscriber nodes.

When you switch versions, your configuration information migrates automatically to the upgraded version on the active partition.

If for any reason you decide to back out of the upgrade, you can restart the system to the inactive partition that contains the older version of the software. However, any configuration changes that you made since you upgraded the software will be lost.

For a short period of time after you install Cisco Unified Communications Manager or switch over after upgrading to a different product version, settings changes made by phone users may be lost. Examples of phone user settings include call forwarding and message waiting indication light settings. This can occur because Cisco Unified Communications Manager synchronizes the database after an installation or upgrade, which can overwrite phone user settings changes.

Accessing the Upgrade File

The method that you use to access the upgrade file depends on your network environment. The following options are available:

- access the upgrade file on a remote FTP or SFTP server
- access the upgrade file on the physical DVD drive of a VMware ESXi server host
- upgrade from a data store ISO file on the local ESXi host; for this option, you must edit the virtual machine's CD/DVD drive to map to the file
- upgrade from a data store ISO file on a storage area network (SAN) that is connected to the ESXi host;for this option, you must edit the virtual machine's CD/DVD drive to map to the file

Upgrade Task Lists

The following sections provide a list of the high-level tasks that you must perform for each of the supported upgrade scenarios:

- upgrade the software on both Unified Communications Manager nodes, and IM and Presence nodes
- upgrade the software on Unified Communications Manager nodes only
- upgrade the software on IM and Presence nodes only

Perform the tasks in the order shown in these high-level task lists. For detailed information about how to perform the tasks outlined in these task lists, refer to the Related Topics section included at the end of each task list.

Standard Upgrade of Unified Communications Manager and IM and Presence Nodes

Complete the high-level tasks listed in this section when you want to perform a standard upgrade on both the Unified Communications Manager nodes and the IM and Presence nodes in your network.

Procedure

Step 1 Perform all pre-upgrade tasks that apply to your site.

Step 2 Stop all configuration tasks. Do not perform any configuration tasks during the upgrade.

Caution Do not modify any of the IM and Presence Service server entries on the Application Server or Server configuration pages of the Cisco Unified CM Administration interface. The IM and Presence Service upgrade process automatically updates these entries on the Cisco Unified Communications Manager cluster during the final stages (switch version) of the upgrade process.

For upgrades from Release 8.x or 9.x to Release 10.x or later, any manual modification of these entries during the upgrade process will result in data migration failures between IM and Presence Service and Cisco Unified Communications Manager. If such failures occur, you must restart the entire upgrade process for both Cisco Unified Communcations Manager and IM and Presence Service clusters.

Step 3 Upgrade the Unified Communications Manager publisher node. The Unified Communications Manager publisher node is the first node in the cluster.

Step 4 Upgrade the Unified Communications Manager subscriber nodes.

Step 5 Switch the first node to the upgraded partition.

Step 6 Switch the subscriber nodes to the upgraded partition.

Note You can switch the subscriber nodes to the upgraded partition either all at once or one at a time, depending on your site requirements.

Step 7 Ensure that database replication is functioning between the first node (the Unified Communications Manager publisher node) and the subscriber nodes. You can check database replication status by using one of the following methods:

- In Cisco Unified Reporting, access the Unified Communications Manager Database Status report. Before you proceed, ensure the report indicates that you have a good database replication status with no errors. For more information about using Cisco Unified Reporting, see the *Cisco Unified Reporting Administration Guide*.
- In the Cisco Real Time Monitoring Tool, access the Database Summary service under the CallManager tab to monitor database replication status. The following list indicates the database replication status progress:
  - 0 - Initializing; replication setup is in process.
  - 1 - Replication setup script running on this node; transitional state.
  - 2 - Set-up complete; replication is setup and in a good state.
  - 3 - Out of sync; replication is setup, but some data is going out of sync.
  - 4 - Failed; replication setup did not succeed.

Before you proceed, ensure that the database replication is setup and in a good state. For more information about using the Real Time Monitoring Tool, see the *Cisco Unified Real Time Monitoring Tool Administration Guide*.

Step 8 Perform post-upgrade tasks for Unified Communications Manager nodes.

Step 9 Upgrade the IM and Presence database publisher node. The IM and Presence database publisher node is the first node in the IM and Presence cluster.

Step 10 Upgrade the IM and Presence subscriber nodes.

Step 11 Switch the software to the new software release on the IM and Presence database publisher node (the first IM and Presence node). Wait until the first node has successfully restarted and is at the sign in prompt before you proceed to the next step.

Step 12 On the IM and Presence subscriber node, switch the software to the new software release. After the IM and Presence subscriber node has restarted and has come back online with the new software release, switch the software release on the next node. Wait until each of the nodes has successfully restarted (is at the sign in prompt) before you proceed with the software switch on the next node. Repeat until the new software release is running on all nodes.

Step 13 Run the following CLI command to check if the database replication is active on a node:

```
utils dbreplication runtimestate
```

If database replication is active on all nodes, the output lists all the nodes and the **replication setup** value for each node is **2**.

Note If database replication is not complete (a value other than 2 is returned), core services will not start on the subscriber nodes until replication is complete. Select **Cisco Unified CM IM and Presence Administration** > **System** > **Notifications** to determine whether database replication is complete.

Step 14 Perform post-upgrade tasks for the IM and Presence Service.

Refresh Upgrade of Unified Communications Manager and IM and Presence Nodes

Complete the high-level tasks listed in this section when you want to perform a refresh upgrade on both the Unified Communications Manager nodes and the IM and Presence Service nodes in your network.

Procedure

Step 1 Perform all pre-upgrade tasks that apply to your site.

Step 2 Stop all configuration tasks. Do not perform any configuration tasks during the upgrade.

Caution Do not modify any of the IM and Presence Service server entries on the Application Server or Server configuration pages of the Cisco Unified CM Administration interface. The IM and Presence Service upgrade process automatically updates these entries on the Cisco Unified Communications Manager cluster during the final stages (switch version) of the upgrade process.

For upgrades from Release 8.x or 9.x to Release 10.x or later, any manual modification of these entries during the upgrade process will result in data migration failures between IM and Presence Service and Cisco Unified Communications Manager. If such failures occur, you must restart the entire upgrade process for both Cisco Unified Communcations Manager and IM and Presence Service clusters.

Step 3 If you are performing a refresh upgrade that requires a COP file, install the required COP file.
If you are unsure whether you need to install a COP file, review the information about supported upgrade paths.

Step 4 Upgrade the Unified Communications Manager publisher node. The Unified Communications Manager publisher node is the first node in the cluster.

Step 5 Switch the software to the new software release. To do this, select **Switch to new version after upgrade**. The publisher node must be running the new software before you upgrade each subscriber node.

Step 6 Upgrade each Unified Communications Manager subscriber node.

Step 7 Switch the software on the subscriber nodes to the new software release. To do this, select **Switch to new version after upgrade**.

Note You can switch the subscriber nodes to the upgraded partition either all at once or one at a time, depending on your site requirements.

Step 8 Ensure that database replication is functioning between the first node (the Unified Communications Manager publisher node) and the subscriber nodes. You can check database replication status by using one of the following methods:

- In Cisco Unified Reporting, access the Cisco Unified Communications Manager Database Status report. Before you proceed, ensure the report indicates that you have a good database replication status with no errors. For more information about using Cisco Unified Reporting, see the *Cisco Unified Reporting Administration Guide*.
- In the Cisco Real Time Monitoring Tool, access the Database Summary service under the CallManager tab to monitor database replication status. The following list indicates the database replication status progress:
  - 0 - Initializing; replication setup is in process.
  - 1 - Replication setup script running on this node; transitional state.
  - 2 - Set-up complete; replication is setup and in a good state.
  - 3 -Out of sync; replication is setup, but some data is going out of sync.
  - 4 - Failed; replication setup did not succeed.

Before you proceed, ensure that the database replication is setup and in a good state. For more information about using the Real Time Monitoring Tool, see the *Cisco Unified Real Time Monitoring Tool Administration Guide*.

Step 9 Perform post-upgrade tasks for Unified Communications Manager nodes.

Step 10 If you are performing a refresh upgrade that requires a COP file, install the required COP file on every IM and Presence node in the cluster and restart the nodes.
If you are unsure whether you need to install a COP file, review the information about supported upgrade paths. See the Related Topics section below for more information.

Step 11 Upgrade the IM and Presence database publisher node. The IM and Presence database node is the first node in the IM and Presence cluster.

Step 12 Switch the software to the new software release. To do this, select **Switch to new version after upgrade**. The IM and Presence database publisher node must be running the new software before you upgrade the IM and Presence subscriber nodes.

Step 13 Upgrade each IM and Presence subscriber node.

Step 14 Switch the software on the subscriber nodes to the new software release. To do this, select **Switch to new version after upgrade**.

Step 15 Run the following CLI command (on the publisher or subscriber node) to check if the database replication is active on a node:

```
utils dbreplication runtimestate
```

If database replication is active on all nodes, the output lists all the nodes and the **replication setup** value for each node is **2**.

Note If database replication is not complete (a value other than 2 is returned), core services will not start on the subscriber node until replication is complete. Select **Cisco Unified CM IM and Presence Administration** > **System** > **Notifications** to determine whether database replication is complete.

Step 16 Perform post-upgrade tasks for the IM and Presence Service.

Standard Upgrade of Unified Communications Manager Nodes Only

Complete the high-level tasks listed in this section when you want to perform a standard upgrade of only the Unified Communications Manager nodes in your network. When you upgrade Unified Communications Manager nodes without upgrading IM and Presence nodes, ensure that the installed version of the IM and Presence Service is compatible with the new version of the Unified Communications Manager software.

Note When Cisco Unified Communications Manager 10.0(x) is upgraded as part of a service update or a maintenance release, Cisco Sync Agent sends a notification to Cisco Unified CM IM and Presence Administration that the IM and Presence Service database publisher node and subscriber nodes must be rebooted. You must manually clear this notification after the reboots are complete. A warning message about the upgrade is also raised in the Cisco Unified Communications Manager OS Administration GUI.

Procedure

Step 1 Perform all pre-upgrade tasks that apply to your site.

Step 2 Stop all configuration tasks. Do not perform any configuration tasks during the upgrade.

Step 3 Upgrade the Unified Communications Manager publisher node. The Unified Communications Manager publisher node is the first node in the cluster.

Step 4 Upgrade the Unified Communications Manager subscriber nodes.

Step 5 When you have completed the upgrade of all the subscriber nodes, switch the publisher node to the upgraded software version.

Step 6 When the publisher node is switched to the new version, switch the subscriber nodes to the upgraded software version.

Step 7 Ensure that database replication is functioning between the first node (the Unified Communications Manager publisher node) and the subscriber nodes. You can check database replication status by using one of the following methods:

- In Cisco Unified Reporting, access the Cisco Unified Communications Manager Database Status report. Before you proceed, ensure the report indicates that you have a good database replication status with no errors. For more information about using Cisco Unified Reporting, see the *Cisco Unified Reporting Administration Guide*.
- In the Cisco Real Time Monitoring Tool, access the Database Summary service under the CallManager tab to monitor database replication status. The following list indicates the database replication status progress:

- 0 - Initializing; replication setup is in process.
- 1 - Replication setup script running on this node; transitional state.
- 2 - Set-up complete; replication is setup and in a good state.
- 3 -Out of sync; replication is setup, but some data is going out of sync.
- 4 - Failed; replication setup did not succeed.

Before you proceed, ensure that the database replication is setup and in a good state. For more information about using the Real Time Monitoring Tool, see the *Cisco Unified Real Time Monitoring Tool Administration Guide*.

Step 8 Perform post-upgrade tasks for Unified Communications Manager nodes.

Step 9 If you upgraded Cisco Unified Communications Manager to a Maintenance Release (MR) or an Engineering Special (ES) Release and you do not upgrade the IM and Presence Service, you must reboot all IM and Presence nodes after the Unified Communications Manager upgrade is complete.

Refresh Upgrade Of Unified Communications Manager Nodes Only

Complete the high-level tasks listed in this section when you want to perform a refresh upgrade of only the Unified Communications Manager nodes in your network. When you upgrade Unified Communications Manager nodes without upgrading IM and Presence nodes, ensure that the installed version of the IM and Presence Service is compatible with the new version of the Unified Communications Manager software.

Procedure

Step 1 Perform all pre-upgrade tasks that apply to your site.

Step 2 Stop all configuration tasks. Do not perform any configuration tasks during the upgrade.

Step 3 If you are performing a refresh upgrade that requires a COP file, install the required COP file.
If you are unsure whether you need to install a COP file, review the information about supported upgrade paths.

Step 4 Upgrade the Unified Communications Manager publisher node. The Unified Communications Manager publisher node is the first node in the cluster.

Step 5 Switch the software to the new software release. To do this, select **Switch to new version after upgrade**. The publisher node must be running the new software before you upgrade each subscriber node.

Step 6 Upgrade the Unified Communications Manager subscriber nodes.

Step 7 Switch the software to the new software release. To do this, select **Switch to new version after upgrade**.

Step 8 Ensure that database replication is functioning between the first node (the Unified Communications Manager publisher node) and the subscriber nodes. You can check database replication status by using one of the following methods:

- In Cisco Unified Reporting, access the Unified Communications Manager Database Status report. Before you proceed, ensure the report indicates that you have a good database replication status with no errors. For more information about using Cisco Unified Reporting, see the *Cisco Unified Reporting Administration Guide*.

- In the Cisco Real Time Monitoring Tool, access the Database Summary service under the CallManager tab to monitor database replication status. The following list indicates the database replication status progress:
  - 0 - Initializing; replication setup is in process.
  - 1 - Replication setup script running on this node; transitional state.
  - 2 - Set-up complete; replication is setup and in a good state.
  - 3 -Out of sync; replication is setup, but some data is going out of sync.
  - 4 - Failed; replication setup did not succeed.

Before you proceed, ensure that the database replication is setup and in a good state. For more information about using the Real Time Monitoring Tool, see the *Cisco Unified Real Time Monitoring Tool Administration Guide*.

Step 9 Perform post-upgrade tasks for Cisco Unified Communications Manager nodes.

Step 10 If you upgraded Unified Communications Manager to a Maintenance Release (MR) or an Engineering Special (ES) Release and you do not upgrade IM and Presence Service, you must reboot all IM and Presence nodes after the Unified Communications Manager upgrade is complete.

Standard Upgrade of IM and Presence Nodes Only

Complete the high-level tasks listed in this section when you want to perform a standard upgrade the IM and Presence nodes in your network without upgrading Unified Communication Manager subscriber nodes.

When you upgrade IM and Presence nodes without upgrading Unified Communication Manager subscriber nodes, ensure that the installed version of Unified Communication Manager is compatible with the new version of the Unified Communication Manager software. The software version of the first IM and Presence node (the IM and Presence database publisher node) must match the first two numbers of the software version installed on the Unified Communications Manager publisher node. For example, IM and Presence Service software version 10.0.1.10000-1 is compatible with Cisco Unified Communications Manager software version 10.0.1.30000-2.

Procedure

Step 1 Perform all pre-upgrade tasks that apply to your site.

Step 2 Stop all configuration tasks. Do not perform any configuration tasks during the upgrade.

Step 3 Upgrade the Unified Communications Manager publisher node. The Unified Communications Manager publisher node is the first node in the cluster.

Step 4 Upgrade the IM and Presence database publisher node. The IM and Presence database publisher node is the first node in the IM and Presence cluster.

Step 5 Upgrade the IM and Presence subscriber nodes.

Step 6 Switch the software to the new software release. To do this, select **Switch to new version after upgrade**. You must switch the software to the upgraded version in the following order:

- Switch the software on the Unified Communications Manager publisher node.

- Switch the software on the IM and Presence database publisher node.
- Switch the software on the IM and Presence subscriber nodes.

Wait until each of the nodes has successfully restarted and is at the sign in prompt before you proceed with the software switch on the next node. Repeat until the new software release is running on all nodes.

Step 7 Run the following CLI command to check if the database replication is active on a node:

```
utils dbreplication runtimestate
```

If database replication is active on all nodes, the output lists all the nodes and the **replication setup** value for each node is **2**.

Note If database replication is not complete (a value other than 2 is returned), core services will not start on the subscriber nodes until replication is complete. Select **Cisco Unified CM IM and Presence Administration** > **System** > **Notifications** to determine whether database replication is complete.

Step 8 Perform post-upgrade tasks for the IM and Presence Service.

In the event of an IM and Presence upgrade failure

If the upgrade of Cisco Unified Communications Manager nodes is successful but the upgrade of IM and Presence nodes fails, you must either:

- perform another upgrade of both the Cisco Unified Communications Manager nodes and the IM and Presence nodes after you address the issues that caused the failure
- perform a DRS restore on the Cisco Unified Communications Manager node where the backup was taken from to restore it to the configuration it had before the attempted upgrade of the IM and Presence nodes

Refresh Upgrade of IM and Presence Nodes Only

Complete the high-level tasks listed in this section when you want to perform a refresh upgrade the IM and Presence nodes in your network without upgrading Cisco Unified Communication Manager subscriber nodes. When you upgrade IM and Presence nodes without upgrading Cisco Unified Communications Manager subscriber nodes, ensure that the installed version of Cisco Unified Communications Manager is compatible with the new version of the IM and Presence Service software.

Procedure

Step 1 Perform all pre-upgrade tasks that apply to your site.

Step 2 Stop all configuration tasks. Do not perform any configuration tasks during the upgrade.

Step 3 If you are performing a refresh upgrade that requires a COP file, install the required COP file.
If you are unsure whether you need to install a COP file, review the information about supported upgrade paths. See the Related Topics section below for more information.

Step 4 Upgrade the Cisco Unified Communications Manager publisher node. The Cisco Unified Communications Manager publisher node is the first node in the cluster.

Step 5 Switch the software to the new software release. To do this, select **Switch to new version after upgrade**. The Cisco Unified Communications Manager publisher node must be running the new software before you upgrade each IM and Presence subscriber node.

Step 6 Upgrade the IM and Presence database node. The IM and Presence database node is the first node in the IM and Presence cluster.

Step 7 Switch the software to the new software release. To do this, select **Switch to new version after upgrade**.

Step 8 Upgrade the IM and Presence subscriber nodes.

Step 9 Switch the software on the subscriber nodes to the new software release. To do this, select **Switch to new version after upgrade**.
Wait until each of the nodes has successfully restarted and is at the sign in prompt before you proceed with the software switch on the next node. Repeat until the new software release is running on all nodes.

Step 10 Run the following CLI command to check if the database replication is active on a node:
```
utils dbreplication runtimestate
```
If database replication is active on all nodes, the output lists all the nodes and the **replication setup** value for each node is **2**.

Note If database replication is not complete (a value other than 2 is returned), core services will not start on the subscriber nodes until replication is complete. Select **Cisco Unified CM IM and Presence Administration** > **System** > **Notifications** to determine whether database replication is complete.

Step 11 Request that all IM and Presence client users in the local and remote cluster sign out, and sign back in to the application.

Step 12 Perform post-upgrade tasks for the IM and Presence Service.

In the event of an IM and Presence upgrade failure

If the upgrade of Cisco Unified Communications Manager nodes is successful but the upgrade of IM and Presence nodes fails, you must either:

- perform another upgrade of both the Cisco Unified Communications Manager nodes and the IM and Presence nodes after you address the issues that caused the failure
- perform a DRS restore on the Cisco Unified Communications Manager node where the backup was taken from to restore it to the configuration it had before the attempted upgrade of the IM and Presence nodes

Parallel Upgrades

Complete the high-level tasks listed in this section when you want to upgrade nodes in a cluster in parallel.

You can begin upgrading subscriber nodes after the publisher node has finished upgrading. If you are performing a refresh upgrade, there will be a temporary server outage until all subscriber nodes get upgraded to the new software version.

Procedure

Step 1 Perform all pre-upgrade tasks that apply to your site.

Step 2 Stop all configuration tasks. Do not perform any configuration tasks during the upgrade.

Step 3 Upgrade the Unified Communications Manager publisher node. The Unified Communications Manager publisher node is the first node in the cluster.

Step 4 View the installation log to monitor the status of the upgrade by using the Software Installation/Upgrade window in Cisco Unified Communications Operating System Administration or by using the command line interface (CLI).

- List the install log:

```
file list install install_* date
install_log_2008-10-01.09.41.57.log
install_log_2008-10-08.12.59.29.log
install_log_2008-10-14.09.31.06.log
dir count = 0, file count = 3
```

- Search the most recent install log for the string PRODUCT_VERSION; for example:

```
admin:file search install install_log_2013-01-07.09.39.11.log
PRODUCT_VERSION

Searching path: /var/log/install/install_log_2013-01-07.09.39.11.log
Searching file: /var/log/install/install_log_2013-01-07.09.39.11.log
01/07/2013 09:53:54 post_upgrade|PRODUCT_VERSION is
9.1.1.10000-11|<LVL::Info>
01/07/2013 09:53:54 post_upgrade|PRODUCT_VERSION_DISPLAY is
9.1.1.10000-11|<LVL::Info>
Search completed
```

Step 5 When the upgrade on the publisher node is complete, begin the upgrade on the subscriber nodes.

Step 6 Activate the new software on the publisher node.

Step 7 Activate the new software on the subscriber nodes.

Pre-Upgrade Tasks

Perform Pre-Upgrade Tasks

Before you begin the upgrade, perform the following tasks:

Procedure

Step 1 Read the release notes for the new release and be sure that you understand the new features and how the upgrade interacts with the other products that are associated with your system.

Step 2 Familiarize yourself with the requirements and limitations listed in this document. Ensure that your system meets all requirements, including network requirements, platform requirements, and software requirements.

Step 3 Ensure that the software version you are upgrading from is running on a virtual machine. If your current deployment is running on MCS hardware, see the *Cisco Prime Collaboration Deployment Administration Guide* for information about how to migrate an existing cluster to a virtualized cluster.

Step 4 Use the Real-Time Monitoring Tool (RTMT) to verify that you have enough common partition space for the upgrade. Typically, you need at least 25G of common partition space; however, your deployment may require more space if you have a lot of TFTP data (device firmware loads), music-on-hold (MOH) files, or if you have many locale files installed. If you do not have enough space, perform one or more of the following steps to create enough space:

- Use the Cisco Log Partition Monitoring Tool to adjust the low and high watermarks to reduce the traces and remove unnecessary log files. Cisco recommends that you adjust the low watermark value to 30, and the high watermark value to 40. After the upgrade, you must restore the high and low watermarks to their original values in order to avoid premature purging of traces. The default value for the high watermark is 85. The default value for the low watermark is 80. For more information about using the Cisco Log Partition Monitoring Tool, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.
- Use the Disk Expansion COP file (ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn) to expand the vDisk size if your virtual environment has additional available disk space. Ensure that you review the Readme file that supports this COP file before you proceed.
- Use the Free Common Space COP file (ciscocm.free_common_space_v<latest_version>.cop.sgn). This COP file removes the inactive side in the common partition to increase available disk space without requiring a system rebuild. Ensure that you review the Readme file that supports this COP file before you proceed.
- Manually remove outdated or unused firmware files from the TFTP directory. You can remove these files using the TFTP File Management page in the OS Administration interface, or you can use the `file list tftp` and `file delete tftp` commands from the command line interface.

You can download COP files and their Readme files from Cisco.com. Navigate to **Support > Downloads > Cisco Unified Communications Manager Version 10.0 > Unified Communications Manager/CallManager/Cisco Unity Connection Utilities**.

Caution Performing an upgrade without sufficient disk space can cause the system to fail.

Step 5 Download any upgrade COP files that are required. COP files are required for refresh upgrades only. To determine which COP files you need, see the information about COP files and supported upgrade paths listed in the Related Topics section below.

Step 6 Ensure that you have the necessary license files for the new release.

Step 7 Back up your system, ensuring 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.
For more information, see the *Disaster Recovery System Administration Guide.*

Step 8 Perform these additional tasks when you upgrade Cisco Unified Communications Manager:

a) Use the **utils dbreplication setrepltimeout** CLI command to increase the database replication timeout value when upgrading large clusters so that more Cisco Unified Communications Manager subscriber nodes have sufficient time to request replication. When the timer expires, the first Cisco Unified Communications Manager subscriber node, plus all other Cisco Unified Communications Manager subscriber nodes that requested replication within that time period, begin a batch data replication with the Cisco Unified Communications Manager database publisher node. The default database replication timeout value is 300 (5 minutes). Restore the timeout to the default value after the entire cluster upgrades and the Cisco Unified Communications Manager subscriber nodes have successfully set up replication. For more information, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

b) Ensure that the device name for the Cisco Unified Mobile Communicator device contains 15 or fewer characters. If the device name contains more than 15 characters for the Cisco Unified Mobile Communicator, the device does not migrate during the upgrade.

c) Ensure that the IP subnet mask of the device is set using the following format:255.255.255.0. You can change the subnet mask by executing the **set network ip eth0 <server_IP_address> 255.255.255.0** command.

d) Before you upgrade a Cisco Unified Communications Manager cluster, execute the **utils network ipv6 ping** CLI command to verify IPv6 networking on the first node (Cisco Unified Communications Manager database publisher node) and Cisco Unified Communications Manager subscriber nodes. If IPv6 is configured incorrectly on the Cisco Unified Communications Manager subscriber nodes, load detection may take 20 minutes.

e) Apply all pre-9.0 licenses to Cisco Unified Communications Manager before you upgrade to Release 9.0 or later software. After you upgrade to Release 9.0 or later software, you cannot apply these licenses to Cisco Unified Communications Manager and you cannot apply them using the Cisco Prime License Manager. Ensure that you install all unused licenses or Product Authorization Keys (PAKs) before you upgrade the system. The Cisco Unified Communications Manager displays a warning to prompt you to install any unused licenses before proceeding.

Step 9 Perform these additional tasks when you upgrade the IM and Presence Service:

a) Disable High Availability on the IM and Presence presence redundancy group. Select **Cisco Unified CM Administration** > **System** > **Presence Redundancy Group.**
For more information, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.

b) If you have to upgrade Cisco Unified Communications Manager as part of your IM and Presence upgrade, you must stop and restart the IM and Presence Sync Agent service. To restart the Sync Agent service, navigate to Cisco Unified IM and Presence Serviceability and select **Tools** > **Control Center - Network Services**.

c) Check that the IM and Presence Service node has connectivity with Cisco Unified Communications Manager.
You can use the Cisco Unified CM IM and Presence Administration System Troubleshooter to check node connectivity.

Change Virtual Machine Configuration Specifications

Use the following procedure when you need to change the configuration specifications on your virtual machine (VM) in order to upgrade to a new release of Unified Communications Manager or IM and Presence Service. Configuration specifications include the vCPU, vRAM, and vDisk size. For information about VM requirements, see the Readme file with the OVA template that supports your release. Details about OVA templates are

available on the Virtualization Docwiki at
http://docwiki.cisco.com/wiki/Implementing_Virtualization_Deployments.

Procedure

Step 1 Perform a Disaster Recovery System (DRS) backup.
For more information about performing a backup, see the *Cisco Unified Communications Manager Disaster Recovery Administration Guide.*

Step 2 (Optional.) If you need to increase the vDisk space to meet the space requirements of a refresh upgrade, install the following COP file:
`ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn`

Step 3 Shut down the virtual machine.

Step 4 Change the configuration of the virtual machine as needed:

a) Change the Guest OS version to match the requirements of the new release (Red Hat Enterprise Linux 6 (64-bit).

b) To change the vCPU, make the change in vSphere Client. Ensure that you change the reservation value to match the specifications of the new release.

c) To change the vRAM, make the change in vSphere Client. Ensure that you change the reservation value to match the specifications of the new release.

d) To increase the vDisk space, edit the disk size using vDisk. If the virtual machine has two disks, expand the second one.
The new space is automatically added to the common partition when you restart the virtual machine.

Note You need to change the disk size changes only if you need additional space to complete the upgrade. The disk space requirements are specified in the Readme file for the OVA template.

Expanding the disk size to add space to the common partition will not increase the user capacity of your system. If you need to extend the user capacity of your system, you must migrate from a single-disk to a multi-disk virtual machine; see*Replace a Single Server or Cluster for Cisco Unified Communications Manager* for more information.

For more information about making configuration changes using vSphere Client, refer to the user manual for the product.

Step 5 Upgrade the software to the latest version.

Step 6 Modify the Network Adapter to use the VMXNET 3 Adapter type.
For information about modifying the Network Adapter to meet the requirements of this release, see the Readme file for the OVA template.

Step 7 Power on the virtual machine.

Upgrade vSphere ESXi

Use the following procedure when you need to update your vSphere ESXi hypervisor in order to upgrade to a new release of Unified Communications Manager.

Procedure

Step 1 Move the virtual machine that is running Unified Communications Manager off the host server using one of the following methods:

- If you have a hot standby host, use vMotion to migrate the virtual machine from one physical server to another.
- If you do not have a hot standby host, power down the virtual machine and copy it to a different location.

Step 2 Upgrade the vSphere ESXi using the upgrade procedures provided by VMware.

Step 3 Verify that the vSphere ESXi upgraded successfully.

Step 4 Move the virtual machine that is running Unified Communications Manager back to the host server using one of the following methods:

- If you have a hot standby host, use vMotion to migrate the virtual machine from one physical server to another.
- If you do not have a hot standby host, power down the virtual machine and copy it the host server.

What to Do Next

If you need to update the virtual machine version or the VMware compatibility version in order to upgrade the vSphere ESXi, proceed to Change Virtual Machine Configuration Specifications, on page 79

Obtain Upgrade File

Before you begin the upgrade process, you must obtain the appropriate upgrade file from Cisco.com.

For more information, see the *Cisco Unified Communications Manager Release Notes*.

You can access the upgrade file during the installation process from either a local DVD or from a remote FTP or SFTP server. Be aware that directory names and filenames that you enter to access the upgrade file are case-sensitive.

Upgrade Tasks

This section contains the procedures for performing an upgrade.

Before You Begin

- Review the pre-installation tasks and ensure that you have performed all the steps.
- Stop all configuration tasks. Do not make any configuration changes during an upgrade. Any configuration changes that you make during an upgrade may be lost, and some configuration changes can cause the upgrade to fail.

- Do not rename the upgrade file before you install it because the system will not recognize it as a valid file.
- Do not decompress the file. If you do, the system may not be able to read the upgrade file.
- For upgrades to the IM and Presence Service software, check that the contact list size for users has not reached the maximum value. The System Troubleshooter in Cisco Unified CM IM and Presence Administration indicates if there are users who have reached the contact list limit.

Caution During a refresh upgrade, traffic is no longer processed and several reboots are required, therefore, you must perform a refresh upgrade during a maintenance window.

Upgrade Procedures

You can access the upgrade file during the installation process from either a local CD or DVD or from a remote FTP or SFTP server. Be aware that directory names and filenames that you enter to access the upgrade file are case-sensitive.

Note If you cancel an upgrade at any stage, or if an upgrade fails, you must reboot the server before you attempt another upgrade.

Upgrade From a Local Source

Follow this procedure to upgrade to a new release of Unified Communications Manager or theIM and Presence Service using a CD or DVD in a local disk drive.

Procedure

Step 1 Ensure that you can access the upgrade file. Choose one of the following options:

- Insert the CD or DVD into the disc drive on the local server that is to be upgraded.
- Create a data store ISO file on the local ESXi host.
- Create a data store ISO file on a storage area network (SAN) that is connected to the ESXi host.

Step 2 Log in to the management software for the node that you are upgrading:

- If you are upgrading an IM and Presence node, log in to Cisco Unified IM and Presence Operating System Administration.
- If you are upgrading a Cisco Unified Communications Manager node, log in to Cisco Unified Communications Operating System Administration.

Step 3 If you are performing a refresh upgrade that requires a COP file, install the required COP file.
If you are unsure whether you need to install a COP file, review the information about supported upgrade paths. See the Related Topics section below for more information.

Step 4 Select **Software Upgrades** > **Install/Upgrade**.

Step 5 Select **DVD/CD** from the **Source** list, or edit the virtual machine to map to the ISO file.

Step 6 In the **Directory** field, enter the path to the location of the patch file. If the file is in the root directory, enter a slash (/).

Step 7 Enter your email address and IP address in the **Email Notification** and **SMTP Server** fields. This will enable you to receive an email notification upon successful completion of the upgrade.

Note These fields are only visible for refresh upgrades.

Step 8 Select **Next** to continue the upgrade process.

Step 9 Select the upgrade version that you want to install and select **Next**.

Step 10 Monitor the progress of the download, which includes the filename and the number of megabytes that are being transferred.

Step 11 When the download completes, verify the checksum value against the checksum for the file that you downloaded from Cisco.com.

Step 12 Perform one of the following actions:

For standard upgrades:

- If this is a single-node deployment and you want to install the upgrade and automatically reboot to the upgraded software, select **Reboot to upgraded partition.**
- If this is a multinode deployment, select **Do not reboot after upgrade**. This allows you to install the upgrade and then manually reboot to the upgraded software at a later time. For more information about how to manually reboot the system and activate the upgrade, see the Related Topics section below.

For refresh upgrades:

- Select **Do not switch to new version after upgrade** only if you are performing a staged upgrade.
- Select **Switch to new version after upgrade** to remain on the new active software version.

Note See the the Related Topics section below for more information about the rules for switching during an upgrade.

Step 13 Select **Next** and select **Finish** when the installation completes.

Upgrade From a Remote Source

Follow this procedure to upgrade to a new release of Cisco Cisco Unified Communications Manager or the IM and Presence Service using software from a network drive or remote node. The network drive or remote node must be running a SFTP/FTP server that can be accessed by each node that you want to upgrade.

Procedure

Step 1 Log in to the management software for the node that you are upgrading:

- If you are upgrading an IM and Presence node, log in to Cisco Unified IM and Presence Operating System Administration.

- If you are upgrading a Cisco Unified Communications Manager node, log in to Cisco Unified Communications Operating System Administration.

Step 2 If you are performing a refresh upgrade that requires a COP file, install the required COP file.
If you are unsure whether you need to install a COP file, review the information about supported upgrade paths. See the Related Topics section below for more information.

Step 3 Select **Software Upgrades** > **Install/Upgrade**.

Step 4 Select **Remote Filesystem** from the **Source** list.

Step 5 In the **Directory** field, enter the path to the patch file on the remote system.

Step 6 In the **Server** field, enter the FTP or SFTP server name.

Step 7 In the **User Name** field, enter the user name for the remote node.

Step 8 In the **User Password** field, enter the password for the remote node.

Step 9 Enter your email address and IP address in the **Email Notification** and **SMTP Server** fields. This will enable you to receive an email notification upon successful completion of the upgrade.

Note These fields are only visible for refresh upgrades.

Step 10 From the **Transfer Protocol** field, select the transfer protocol, for example, SFTP.

Step 11 Select **Next** to continue the upgrade process.

Step 12 Select the upgrade version that you want to install and select **Next**.

Step 13 Monitor the progress of the download, which includes the filename and the number of megabytes that are being transferred.

Step 14 When the download completes, verify the checksum value against the checksum for the file that you downloaded from Cisco.com.

Step 15 Perform one of the following actions:
For standard upgrades:

- If this is a single-node deployment and you want to install the upgrade and automatically reboot to the upgraded software, select **Reboot to upgraded partition.**
- If this is a multinode deployment, select **Do not reboot after upgrade.**This allows you to install the upgrade and then manually reboot to the upgraded software at a later time. For more information about how to manually reboot the system and activate the upgrade, see the Related Topics section below.

For refresh upgrades:

- Select **Do not switch to new version after upgrade** only if you are performing a staged upgrade.
- Select **Switch to new version after upgrade** to remain on the new active software version.

Note See the topic called *Version switching during upgrade rules* for more information about the rules for switching during an upgrade.

Step 16 Select **Next** and select **Finish** when the installation completes.

Change Virtual Machine Configuration Specifications

Use the following procedure when you need to change the configuration specifications on your virtual machine (VM) in order to upgrade to a new release of Unified Communications Manager or IM and Presence Service. Configuration specifications include the vCPU, vRAM, and vDisk size. For information about VM requirements, see the Readme file with the OVA template that supports your release. Details about OVA templates are available on the Virtualization Docwiki at http://docwiki.cisco.com/wiki/Implementing_Virtualization_Deployments.

Procedure

Step 1 Perform a Disaster Recovery System (DRS) backup.
For more information about performing a backup, see the *Cisco Unified Communications Manager Disaster Recovery Administration Guide.*

Step 2 (Optional.) If you need to increase the vDisk space to meet the space requirements of a refresh upgrade, install the following COP file:
`ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn`

Step 3 Shut down the virtual machine.

Step 4 Change the configuration of the virtual machine as needed:

a) Change the Guest OS version to match the requirements of the new release (Red Hat Enterprise Linux 6 (64-bit).

b) To change the vCPU, make the change in vSphere Client. Ensure that you change the reservation value to match the specifications of the new release.

c) To change the vRAM, make the change in vSphere Client. Ensure that you change the reservation value to match the specifications of the new release.

d) To increase the vDisk space, edit the disk size using vDisk. If the virtual machine has two disks, expand the second one.
The new space is automatically added to the common partition when you restart the virtual machine.

Note You need to change the disk size changes only if you need additional space to complete the upgrade. The disk space requirements are specified in the Readme file for the OVA template.

Expanding the disk size to add space to the common partition will not increase the user capacity of your system. If you need to extend the user capacity of your system, you must migrate from a single-disk to a multi-disk virtual machine; see*Replace a Single Server or Cluster for Cisco Unified Communications Manager* for more information.

For more information about making configuration changes using vSphere Client, refer to the user manual for the product.

Step 5 Upgrade the software to the latest version.

Step 6 Modify the Network Adapter to use the VMXNET 3 Adapter type.
For information about modifying the Network Adapter to meet the requirements of this release, see the Readme file for the OVA template.

Step 7 Power on the virtual machine.

Version Switching

A number of rules apply when you are manually switching versions and when you switch versions during an upgrade. The table below outlines the version switching rules for activating the release 10.x software version and for switching back to a previous software version.

Note You cannot switch the version of any node if doing so violates the version matching requirements. This rule applies whether you are switching forward to a new software version, or switching back to a previous software version.

Product	Node type	Switch from	Switch to	Switching rule
Activate the new software version				
Unified Communications Manager	Publisher	8.x or 9.x	10.x	You must switch the software version on the publisher node before you switch the software version on subscriber nodes.
		10.x	10.y	
Unified Communications Manager	Subscriber	8.x or 9.x	10.x	Supported when the publisher node has been switched to the new version. The software version you are switching to must match the version number of the active partition on the Unified Communications Manager publisher node.
		10.x	10.y	
IM and Presence Service	Database publisher	8.x or 9.x	10.x	Supported when the software version you are switching to matches the major and minor version number of active partition on the Unified Communications Manager publisher node.
		10.x	10.y	
IM and Presence Service	Subscriber	8.x or 9.x	10.x	Supported when the software version of this node matches the five version numbers of the IM and Presence database publisher node.
		10.x	10.y	
Switch back to a previous software version				
Unified Communications Manager	Publisher	10.x	8.x or 9.x	Supported. You must switch the software version on the publisher node before you switch the software version on subscriber nodes.
		10.y	10.x	

Product	Node type	Switch from	Switch to	Switching rule
Unified Communications Manager	Subscriber	10.x	8.x or 9.x	Supported when the CUCM publisher node has been switched to the previous version. The software version you are switching to must match the version number of the active partition on the Unified Communications Manager publisher node. You cannot switch a subscriber node to a previous version when the publisher node is running new version.
		10.y	10.x	
IM and Presence Service	Database publisher	10.x	8.x or 9.x	Not supported when the Unified Communications Manager publisher node is running a software version that is newer than the one that you are switching back to. Switching the IM and Presence database publisher node to a previous release after the Unified Communications Manager has been upgraded to a newer release violates the version matching requirements. Switching back to a previous release is supported only when the software version you are switching to matches the major and minor version number of active partition on the Unified Communications Manager publisher node.
		10.y	10.x	
IM and Presence Service	Subscriber	10.x	8.x or 9.x	Not supported when the IM and Presence database publisher node is running a software version that is newer than the one that you are switching back to. Switching back to a previous release is supported only when the software version of this node matches the five version numbers of the IM and Presence database publisher node.
		10.y	10.x	

Switch Software Version

When you perform a standard upgrade, the new software is installed as an inactive version. You can reboot to the new software during the upgrade process or you can switch to the new version later.

When you switch versions, the system restarts, and the inactive software becomes active. The system restart may take up to 15 minutes. When you perform this procedure both the active and inactive software versions are indicated.

Caution This procedure causes the system to restart and become temporarily out of service.

Before You Begin

The software versions on Cisco Unified Communications Manager and IM and Presence nodes must match according to the manual switching rules. Therefore, you must switch Unified Communications Manager before you switch IM and Presence.

Procedure

Step 1 If you switch versions in a multinode deployment, you must switch the publisher node first.

Step 2 Log in to the management software for the node that you are upgrading:

- If you are upgrading an IM and Presence node, log in to Cisco Unified IM and Presence Operating System Administration.
- If you are upgrading a Unified Communications Manager node, log in to Cisco Unified Communications Operating System Administration.

Step 3 Select **Settings** > **Version**.
It may take some time for all the services on the IM and Presence nodes to move to the Started state. Select **Cisco Unified CM IM and Presence Administration** > **System** > **Cluster Topology** and select a node from the tree view to monitor the status of the services on the node.

Step 4 Verify the version of the active software and the inactive software.

Step 5 Select **Switch Versions** to switch versions and restart the system.

After you perform a switch version when you upgrade Unified Communications Manager, IP phones request a new configuration file. This request results in an automatic upgrade to the device firmware.

Switch to Previous Version

If you need to revert to the software version that was running before the upgrade, you can do so by using the Switch Version option to switch the system to the software version on the inactive partition.

Switch Cluster to Previous Version

To switch a cluster back to a previous version, complete these high-level tasks:

Procedure

Step 1 Switch back the publisher node.

Step 2 Switch back all backup subscriber nodes.

Step 3 Switch back all primary subscriber nodes.

Step 4 If you are reverting to an older product release, reset database replication within the cluster.

Switch Node to Previous Version

Procedure

Step 1 Log in to the management software for the node that you are upgrading:

- If you are upgrading an IM and Presence node, log in to Cisco Unified IM and Presence Operating System Administration.
- If you are upgrading a Cisco Unified Communications Manager node, log in to Cisco Unified Communications Operating System Administration.

Step 2 Choose **Settings** > **Version**.
The Version Settings window displays.

Step 3 Click the **Switch Versions** button.
After you verify that you want to restart the system, the system restarts, which might take up to 15 minutes.

Step 4 To verify that the version switch was successful, follow these steps:

a) Log in again to the management software for the node that you are upgrading.
b) Choose **Settings** > **Version**.
The Version Settings window displays.
c) Verify that the correct product version is now running on the active partition.
d) Verify that all activated services are running.
e) For the publisher node, log in to Cisco Unified CM Administration.
f) Verify that you can log in and that your configuration data exists.

Reset Database Replication

If you switch back the servers in a cluster to run an older product release, you must manually reset database replication within the cluster. To reset database replication after you revert all the cluster servers to the older product release, enter the CLI command **utils dbreplication reset all** on the publisher server.

When you switch versions by using Cisco Unified Communications Operating System Administration or the CLI, you get a message that reminds you about the requirement to reset database replication if you are reverting to an older product release.

Switch version back to Cisco Unified Presence 8.6(3) or earlier

Cisco Unified Presence releases 8.6(4) and later do not support the Cisco Presence Engine database. If you upgrade from Release 8.6(3) or earlier and you subsequently want to revert to the previous release, you must install a COP file that will reinstall the Cisco Presence Engine database. The COP filename is `ciscocm.cup.pe_db_install.cop` and you can download it from Cisco.com.

Note In a multinode environment, you must install the COP file on every node in the cluster after you switch versions from Cisco Unified Presence Release 8.6(4) or later.

In this release, you cannot downgrade to a version earlier than Release 8.6(3).

Note You must restart the system after you install the COP file.

Before you begin

Switch versions on Cisco Unified Communications Manager.

Procedure

Step 1 Download the following COP file from Cisco.com: `ciscocm.cup.pe_db_install.cop`.

Step 2 Sign in to Cisco Unified IM and Presence Operating System Administration.

Step 3 Select **Settings** > **Version**.

Step 4 Verify the version of the active and inactive software.

Note This procedure only applies if you want to switch from Release 9.0 or later back to a release earlier than 8.6(4).

Step 5 Select **Switch Versions** to switch back to the earlier release and restart the system.

Step 6 After the system has restarted, install the COP file.

Note In a multinode environment, you must install the COP file on every node in the cluster.

Step 7 After you have installed the COP file, manually restart the system. To do this, select **Settings** > **Version** and select **Restart**.

Step 8 Run the following CLI command (on the publisher or subscriber node) to check if the database replication is active on the node: `utils dbreplication runtimestate`
If database replication is active on all nodes, the output lists all the nodes and the replication setup value for each node is 2. If database replication is not complete (a value other than 2 is returned), core services will not start on the subscriber node until replication is complete.

Step 9 Select **Cisco Unified CM IM and Presence Administration** > **System** > **Notifications** to determine whether database replication is complete.

Step 10 If database replication cannot be established, use the following CLI command on the publisher node to reset replication: `utils dbreplication reset all`

Post-Upgrade Tasks

The following sections provide information about the tasks that you must complete after you upgrade Cisco Unified Communications Manager nodes or IM and Presence nodes.

Post-Upgrade Tasks for All Nodes

This section describes post-upgrade tasks that you must perform for both Unified Communications Manager nodes and IM and Presence Service nodes.

Update VMWare Tools

You must update the VMWare Tools after you complete and upgrade. There are two options for updating the VMWare Tools:

- configure the tool to use the Automatic Tools Upgrade option
- configure the tool to automatically check the tools version during a VM power-on and upgrade the tools

For information about how to configure these options, see the VMWare documentation.

Locale Installation

You can configure Cisco Unified Communications Manager and IM and Presence Service to support multiple languages. There is no limit to the number of supported languages you can install.

Cisco provides locale-specific versions of the Cisco Unified Communications Manager Locale Installer and the IM and Presence Service Locale Installer on www.cisco.com. Installed by the system administrator, the locale installer allows the user to view/receive the chosen translated text or tones, if applicable, when a user works with supported interfaces.

After you upgrade Cisco Unified Communications Manager or the IM & Presence Service, you must reinstall all the locales. Install the latest version of the locales that match the major.minor version number of your Cisco Unified Communications Manager node or IM and Presence Service node.

Install locales after you have installed Cisco Unified Communications Manager on every node in the cluster and have set up the database. If you want to install specific locales on IM and Presence Service nodes, you must first install the Cisco Unified Communications Manager locale file for the same country on the Cisco Unified Communications Manager cluster.

Use the information in the following sections to install locales on Cisco Unified Communications Manager nodes and on IM and Presence Service nodes after you complete the software upgrade.

User Locales

User locale files contain language information for a specific language and country. They provide translated text and voice prompts, if available, for phone displays, user applications, and user web pages in the locale that the user chooses. These files use the following naming convention:.

- cm-locale-language-country-version.cop (Cisco Unified Communications Manager)
- ps-locale-language_country-version.cop (IM and Presence Service)

If your system requires user locales only, install them after you have installed the CUCM locale.

Network Locales

Network locale files provide country-specific files for various network items, including phone tones, annunciators, and gateway tones. The combined network locale file uses the following naming convention:

- cm-locale-combinednetworklocale-version.cop (Cisco Unified Communications Manager)

Cisco may combine multiple network locales in a single locale installer.

Note Virtualized deployments of Cisco Unified Communications Manager on Cisco-approved, customer-provided servers can support multiple locales. Installing multiple locale installers ensures that the user can choose from a multitude of locales.

You can install locale files from either a local or a remote source by using the same process for installing software upgrades. You can install more than one locale file on each node in the cluster. Changes do not take effect until you reboot every node in the cluster. Cisco strongly recommends that you do not reboot the nodes until you have installed all locales on all nodes in the cluster. Minimize call-processing interruptions by rebooting the nodes after regular business hours.

Install Locale Installer on Cisco Unified Communications Manager

User locale files provide translated text for user applications and user web pages in the locale that the user chooses. User locales are country-specific. Use the following procedure to install locales on the node. Optionally, you can follow the software upgrade procedure to install locale files from either a local or a remote source.

Before You Begin

- Install Cisco Unified Communications Manager on every node in the cluster before you install the Cisco Unified Communications Manager Locale Installer.
- If you want to use a locale other than English, you must install the appropriate language installers on both Cisco Unified Communications Manager and on IM and Presence. Ensure the locale installer is installed on every node in the cluster (install on the Cisco Unified Communications Manager database publisher node before the subscriber nodes).
- User locales should not be set until all appropriate locale installers are loaded on both systems. Users may experience problems if they inadvertently set their user locale after the locale installer is loaded on Cisco Unified Communications Manager but before the locale installer is loaded on IM and Presence. If issues are reported, we recommend that you notify each user to sign into Cisco Unified Communications Manager user options pages and change their locale from the current setting to English and then back again to the appropriate language. You can also use the BAT tool to synchronize user locales to the appropriate language.
- You must restart the nodes for the changes to take effect. After you complete all locale installation procedures, restart each node in the cluster. Updates do not occur in the system until you restart all nodes in the cluster; services restart after the node reboots.

Procedure

Step 1 Download the locale installer from `www.cisco.com`.

Step 2 Click the version of the Cisco Unified Communications Manager Locale Installer.

Step 3 Click **Download** to download the installer file to the node.

Step 4 After downloading the file, save the file to the hard drive and note the location of the saved file.

Step 5 Double-click the file to begin the installation.

Step 6 Perform these actions to complete the installation:

a) Read and accept the license agreement, and then click **Next** to display the **Readme Notes** window.

Note The readme notes contain build-time information such as components and devices that are supported in the released build. The readme may be printed for reference.

b) Examine and accept the readme notes, and then click **Next**. The **Setup Type** window appears.

c) Select a custom setup type in the **Setup Type** window to allow you to select or deselect user locales as required, and then click **Next.**. The **Start Copying Files** window appears.

d) Review the setup options, and then click **Next.**. The **Ready to Install the Program** window appears.

a) Click **Install** to start the installation of the selected user locales.

Note The speed of installation depends on the performance of the node. It is estimated to take between two to ten minutes to complete the database update. Observe the progress bar and text above it to determine the status of installation.

Step 7 When the installation is complete, a new dialog requests confirmation of a restart. Should you wish to apply another locale installer, repeat this procedure before restarting the node in order to reduce downtime.

Step 8 Click **Finish**. The **Setup** dialog box displays. Do not click any buttons or press any keys.

Step 9 When the **Setup** dialog box automatically closes, you have completed the installation on the node. Install the Cisco Unified Communications Manager Locale Installer on every node in the cluster.

Step 10 After you complete all locale installation procedures, perform these actions:

a) Run the following command on the CLI: run sql update enduser set cucm_cdrtime=0

b) Restart the Sync Agent service in Cisco Unified Serviceability (select **Tools** > **Service Activation**).

c) Restart each node in the cluster.

Step 11 Verify that your users can select the locale(s) for supported products.

Troubleshooting Tip

Make sure that you install the same components on every node in the cluster.

What to Do Next

Install Locale Installer on IM and Presence Service, on page 93

Install Locale Installer on IM and Presence Service

Before You Begin

- Install the Locale Installer on Cisco Unified Communications Manager. If you want to use a locale other than English, you must install the appropriate language installers on both Cisco Unified Communications Manager and on IM and Presence Service.

- If your IM and Presence Service cluster has more than one node, make sure that the locale installer is installed on every node in the cluster (install on the IM and Presence database publisher node before the subscriber nodes).
- User locales should not be set until all appropriate locale installers are loaded on both systems. Users may experience problems if they inadvertently set their user locale after the locale installer is loaded on Cisco Unified Communications Manager but before the locale installer is loaded on IM and Presence Service. If issues are reported, we recommend that you notify each user to sign into the Cisco Unified Communications Self Care Portal and change their locale from the current setting to English and then back again to the appropriate language. You can also use the BAT tool to synchronize user locales to the appropriate language.
- You must restart the server for the changes to take effect. After you complete all locale installation procedures, restart each server in the cluster. Updates do not occur in the system until you restart all servers in the cluster; services restart after the server reboots.

Procedure

Step 1 Navigate to `cisco.com` and choose the locale installer for your version of IM and Presence Service.
http://software.cisco.com/download/navigator.html?mdfid=285971059

Step 2 Click the version of the IM and Presence Locale Installer that is appropriate for your working environment.

Step 3 After downloading the file, save the file to the hard drive and note the location of the saved file.

Step 4 Copy this file to a server that supports SFTP.

Step 5 Sign into Cisco Unified IM and Presence Operating System Administration using the administrator account and password.

Step 6 Choose **Software Upgrades** > **Install/Upgrade**.

Step 7 Choose Remote File System as the software location source.

Step 8 Enter the file location, for example `/tmp`, in the Directory field.

Step 9 Enter the IM and Presence Service server name in the Server field.

Step 10 Enter your username and password credentials in the User Name and User Password fields.

Step 11 Choose SFTP for the Transfer Protocol.

Step 12 Click **Next**.

Step 13 Choose the IM and Presence Service locale installer from the list of search results.

Step 14 Click **Next** to load the installer file and validate it.

Step 15 After you complete the locale installation, restart each server in the cluster.

Step 16 The default setting for installed locales is "English, United States". While your IM and Presence Service node is restarting, change the language of your browser, if necessary, to match the locale of the installer that you have downloaded.

Note IM and Presence Service does not currently support Safari browser.

a) If you use Internet Explorer Version 6.x, perform the following steps:

1. Choose **Tools** > **Internet Options**.
2. Choose the General tab.
3. Click **Languages.**

4 Use the Move Up button to move your preferred language to the top of the list.

5 Click **OK**.

b) If you use Mozilla Firefox Version 3.x, perform the following steps:

1 Choose **Tools** > **Options**.

2 Choose the Content tab.

3 Click **Choose** in the Languages section of the window.

4 Use the Move Up button to move your preferred language to the top of the list.

5 Click **OK**.

Step 17 Verify that your users can choose the locales for supported products.

Tip Make sure that you install the same components on every server in the cluster.

Error Messages

See the following table for a description of the messages that can occur during Locale Installer activation. If an error occurs, you can view the messages in the installation log.

Table 17: Locale Installer Error Messages and Descriptions

Message	Description
[LOCALE] File not found: <language>_<country>_user_locale.csv, the user locale has not been added to the database.	This error occurs when the system cannot locate the CSV file, which contains user locale information to add to the database. This indicates an error with the build process.
[LOCALE] File not found: <country>_network_locale.csv, the network locale has not been added to the database.	This error occurs when the system cannot locate the CSV file, which contains network locale information to add to the database This indicates an error with the build process.

Message	Description
[LOCALE] Communications Manager CSV file installer installdb is not present or not executable	This error occurs because a Cisco Unified Communications Manager application called installdb must be present; it reads information that is contained in a CSV file and applies it correctly to the Cisco Unified Communications Manager database. If this application is not found, it either was not installed with Cisco Unified Communications Manager (very unlikely), has been deleted (more likely), or the node does not have Cisco Unified Communications Manager installed (most likely). Installation of the locale will terminate because locales will not work without the correct records that are held in the database.
[LOCALE] Could not create /usr/local/cm/application_locale /cmservices/ipma/com/cisco/ipma /client/locales/maDialogs_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maMessages_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maGlobalUI_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/LocaleMasterVersion.txt.Checksum.	These errors could occur when the system fails to create a checksum file; causes can include an absent Java executable, `/usr/local/thirdparty/java/j2sdk/jre/bin/java`, an absent or damaged Java archive file, /usr/local/cm/jar/cmutil.jar, or an absent or damaged Java class, com.cisco.ccm.util.Zipper. Even if these errors occur, the locale will continue to work correctly, with the exception of Cisco Unified Communications Manager Assistant, which cannot detect a change in localized Cisco Unified Communications Manager Assistant files.
[LOCALE] Could not find /usr/local/cm/application_locale/cmservices/ipma/LocaleMasterVersion.txt in order to update Unified CM Assistant locale information.	This error occurs when the file does not get found in the correct location, which is most likely due to an error in the build process.
[LOCALE] Addition of <RPM-file-name> to the Cisco Unified Communications Manager database has failed!	This error occurs because of the collective result of any failure that occurs when a locale is being installed; it indicates a terminal condition.

Supported Products

For a list of products that Cisco Unified Communications Manager Locale Installers support, see the Cisco IP Telephony Locale Installer for Cisco Unified Communications Manager, which is available at this URL:

`http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-locale-51`

Post-Upgrade Tasks for Cisco Unified Communications Manager Nodes

This section describes the post-upgrade tasks that you must perform for Cisco Unified Communication Manager nodes.

Restore Settings

When the upgrade is complete, restore the following settings:

- If you changed the database replication timeout value for the upgrade using the **utils dbreplication setrepltimeout** CLI command, restore the timeout to the default value of 300 (5 minutes). For more information, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.
- Enable the Cisco Extension Mobility service by navigating to **Cisco Unified Serviceability** > **Tools** > **Service Activation**. For more information, see the *Cisco Unified Serviceability Administration Guide*.

Note If you do not enable the Cisco Extension Mobility service, Cisco Extension Mobility users cannot log in and log out of phones that support Cisco Extension Mobility.

Test Functionality

After the upgrade, perform the following tasks:

- Verify phone functions by making the following types of calls:
  - Voice mail
  - Interoffice
  - Mobile phone
  - Local
  - National
  - International
  - Shared line
- Test the following phone features:
  - Conference
  - Barge
  - Transfer
  - C-Barge
  - Ring on shared lines
  - Do Not Disturb
  - Privacy

- Presence
- CTI call control
- Busy Lamp Field

- If necessary, reinstall the Real Time Monitoring Tool.

Dial Plan Installation

You can install dial plan files from either a local or a remote source by using the same process for installing software upgrades. See the *Upgrade Guide for Cisco Unified Communications Manager* for more information about upgrading from a local or remote source.

After you install the dial plan files on the system, log in to Cisco Unified CM Administration and then navigate to **Call Routing** > **Dial Plan Installer** to complete installing the dial plans.

Manage TFTP Server Files

You can upload files for use by the phones to the TFTP server. Files that you can upload include custom phone rings, callback tones, and backgrounds. This option uploads files only to the specific server to which you connected, and other nodes in the cluster do not get upgraded.

Files upload into the tftp directory by default. You can also upload files to a subdirectory of the tftp directory.

If you have two Cisco TFTP servers that are configured in the cluster, you must perform the following procedure on both servers. This process does not distribute files to all nodes, nor to both Cisco TFTP servers in a cluster.

To upload and delete TFTP server files, follow this procedure:

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Software Upgrades** > **TFTP** > **File Management**.
The TFTP File Management window displays and shows a listing of the current uploaded files. You can filter the file list by using the Find controls.

Step 2 To upload a file, follow this procedure:

a) Click **Upload File**.
The Upload File dialog box opens.

b) To upload a file, click **Browse** and then choose the file that you want to upload.

c) To upload the file to a subdirectory of the tftp directory, enter the subdirectory in the **Directory** field.

d) To start the upload, click **Upload File**.
The Status area indicates when the file uploads successfully.

e) After the file uploads, restart the Cisco TFTP service.

Note If you plan to upload several files, restart the Cisco TFTP service only once, after you have uploaded all the files.

For information about restarting services, refer to *Cisco Unified Serviceability Administration Guide*.

Step 3 To delete files, follow this procedure:

a) Check the check boxes next to the files that you want to delete.
You can also click **Select All** to select all of the files, or **Clear All** to clear all selection.

b) Click **Delete Selected**.

Note If you want to modify a file that is already in the tftp directory, you can use the CLI command **file list tftp** to see the files in the TFTP directory and **file get tftp** to get a copy of a file in the TFTP directory. For more information, see the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*.

Set Up a Custom Log-On Message

You can upload a text file that contains a customized log-on message that appears in Cisco Unified Communications Operating System Administration, Cisco Unified CM Administration, Cisco Unified Serviceability, Disaster Recovery System Administration, and the command line interface.

To upload a customized log-on message, follow this procedure:

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to Software **Upgrades** > **Customized Logon Message**.
The Customized Logon Message window displays.

Step 2 To choose the text file that you want to upload, click **Browse**.

Step 3 Click **Upload File**.

Note You cannot upload a file that is larger than 10kB.

The system displays the customized log-on message.

Step 4 To revert to the default log-on message, click **Delete**.
Your customized log-on message gets deleted, and the system displays the default log-on message.

Note Check the **Require User Acknowledgment** checkbox if you want the custom message to be displayed on the login screens of the Cisco Unified Communications Operating System Administration, Cisco Unified CM Administration, Cisco Unified Serviceability, Disaster Recovery System Administration, Cisco Prime License Manager, and the command line interface.

Configure IPSec Policies

If you are upgrading from Unified Communications Manager release 6.1(5) or earlier, you must re-create your IPSec policies after the upgrade is complete. The configuration information for IPSec policies from release 6.1(5) and earlier will not be migrated as part of the upgrade process. For information about how to create IPSec policies, see the *Cisco Unified Communications Manager Operating System Administration Guide*.

Post-Upgrade Tasks for IM and Presence Nodes

This section describes the post-upgrade tasks for the IM and Presence Service.

Post-upgrade tasks

This section describes the post-upgrade tasks for the IM and Presence Service.

High Availability

If your deployment supports high-availability, you must turn high-availability back on in each presence redundancy group after a system upgrade. Do this after you switch versions, finish the database replication and restart all services. For information about how to turn on high-availability, see the *Cisco Unified Communications Manager Administration Guide*.

Verify IM and Presence Service Data Migration

When you upgrade from Cisco Unified Presence Release 8.x to IM and Presence Service Release 9.x and later, user profiles are migrated to Cisco Cisco Unified Communications Manager. The user profile information is stored as new service profiles on Cisco Unified Communications Manager with the following name and description format:

Name: UCServiceProfile_Migration_x (where x is a number starting at 1)

Description: Migrated Service Profile Number x

To ensure that users can successfully log into Cisco Jabber after an upgrade from Cisco Unified Presence Release 8.x, you must verify that the user profile data migration was successful.

Profiles that are created but that are not assigned to users are *not* migrated to Cisco Unified Communications Manager.

Procedure

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

Step 2 Select **Find** to list all service profiles.

Step 3 Verify that there are migrated service profiles with the following name format: *UCServiceProfile_Migration_x*

Step 4 If there are no migrated service profiles, check the `installdb log` file for any errors.

Step 5 If the data migration fails, an import error alarm is raised on Cisco Unified Communications Manager and the Cisco Sync Agent sends a failure notification to the Cisco Unified CM IM and Presence Administration GUI.

Tip To view the alarm details, log into RTMT for Cisco Unified Communications Manager.

What to Do Next

You can edit these service profiles to give them more meaningful names. See *Cisco Unified Communications Manager Administration Guide* for more information about configuring service profiles.

Troubleshooting

This section contains the following information:

Troubleshooting Unified Communications Manager Upgrades

This section provides information about troubleshooting Unified Communications Manager upgrades.

Upgrade Failure

Problem The upgrade of a subscriber node fails after you upgrade the Unified Communications Manager publisher node and switch it to the new version, or the upgrade of one of the subscriber nodes in your cluster failed during the upgrade cycle.

Solution Do one of the following:

- Correct the errors that caused the upgrade failure on the subscriber node. You may want to check the network connectivity of the nodes in your cluster, reboot the subscriber node, and ensure that the server memory and CPU usage on the subscriber node is not too high. Upgrade the subscriber node again.
- Make sure that the active partition of the Unified Communications Manager publisher node runs the newest version of software installed on the server. Perform a fresh installation on the subscriber node using the same software version as that running on the active partition of the publisher node. If you are reinstalling the subscriber node, you should delete the server from Cisco Unified CM Administration and add the server again as described in the *Cisco Unified Communications Manager Administration Guide*.

Upgrade Fails with Insufficient Disk Space

Problem The upgrade of Unified Communications Manager fails with an error stating that the common partition is full.

Solution Typically, you need at least 25G of common partition space; however, your deployment may require more space if you have a lot of TFTP data (device firmware loads), music-on-hold (MOH) files, or if you have many locale files installed. Perform one or more of the following actions to create additional disk space:

- Use the Cisco Log Partition Monitoring Tool to adjust the low and high watermarks to reduce the traces and remove unnecessary log files. Cisco recommends that you adjust the low watermark value to 30, and the high watermark value to 40. After the upgrade, you must restore the high and low watermarks to their original values in order to avoid premature purging of traces. The default value for the high watermark is 85. The default value for the low watermark is 80. For more information about using the Cisco Log Partition Monitoring Tool, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.
- Use the Disk Expansion COP file (ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn) to expand the vDisk size if your virtual environment has additional available disk space. Ensure that you review the Readme file that supports this COP file before you proceed.
- Use the Free Common Space COP file (ciscocm.free_common_space_v<latest_version>.cop.sgn). This COP file removes the inactive side in the common partition to increase available disk space without requiring a system rebuild. Ensure that you review the Readme file that supports this COP file before you proceed.

- Manually remove outdated or unused firmware files from the TFTP directory. You can remove these files using the TFTP File Management page in the OS Administration interface, or you can use the `file list tftp` and `file delete tftp` commands from the command line interface.

You can download COP files and their Readme files from Cisco.com. Navigate to **Support > Downloads > Cisco Unified Communications Manager Version 10.0 > Unified Communications Manager/CallManager/Cisco Unity Connection Utilities**.

Reduced Permissions for Access Control Groups

Problem When you add a new access control group to existing users, the level of privileges for some pre-existing access control groups is unexpectedly reduced.

Solution Users can belong to multiple access control groups. When you add a new access control group to existing users, the current level of privileges for some pre-existing access control groups may be reduced if the new access control group has the "Effective Access Privileges for Overlapping User Groups and Roles" Enterprise parameter set to minimum.

Access privilege reduction can occur inadvertently, for example, during an upgrade of Cisco Unified CM Administration. If the upgrade version supports the Standard RealTimeAndTrace Collection user group, which has the "Effective Access Privileges for Overlapping User Groups and Roles" Enterprise parameter set to minimum, all users are automatically added to that user group during the upgrade. To resolve the permissions issue in this example, you can remove users from the Standard RealTimeAndTrace Collection user group.

Loss of Phone Settings

For a short period of time after you install Cisco Unified Communications Manager or switch over after upgrading to a different product version, settings that were configured by phone users may be reset. Examples of settings configured by phone users include call forwarding and message waiting indication settings. This situation can occur when Cisco Unified Communications Manager synchronizes the database after an installation or upgrade, which can overwrite setting changes made by phone users.

Post-Upgrade Failure of Unified Communications Manager Publisher Node

Problem The upgrade is successful and the cluster is running the new release, but the Unified Communications Manager publisher node subsequently fails.

Solution Do one of the following:

- restore the Unified Communications Manager publisher node use a DRS backup file
- if you do not have a DRS backup file, you must reinstall the entire cluster, including any IM and Presence Service nodes

Post-Upgrade Failure of Unified Communications Manager Subscriber Nodes

Problem The upgrade is successful and the cluster is running the new release, but a Unified Communications Manager subscriber node subsequently fails.

Solution Do one of the following:

- Restore the Unified Communications Manager subscriber node use a DRS backup file.

- If you do not have a DRS backup file, you must perform the upgrade on the subscriber node again. You do not need to remove the subscriber node from the Unified Communications Manager publisher node's server page before you reinstall it.

Troubleshooting IM and Presence Upgrades

This section provides information about troubleshooting IM and Presence Service upgrades.

Upgrade Failure of IM and Presence Database Publisher Node

Problem You are upgrading a multinode cluster that includes both Unified Communications Manager and IM and Presence nodes, and the upgrade of the IM and Presence database publisher node fails.

Solution The action that you take depends on the point at which the failure occurred:

- if the upgrade on the IM and Presence database publisher node fails before the refresh upgrade causes the node to reboot (that is, if the node failed before switching to the new partition), perform the upgrade again on the IM and Presence database publisher node
- If the failure occurred after the IM and Presence database publisher node switched to the new software version, you must switch back all the nodes and perform the upgrade again. Complete the following tasks in the order listed:
    - switch back the Unified Communications Manager publisher node
    - switch back the Unified Communications Manager subscriber nodes
    - switch back the IM and Presence database publisher node
    - upgrade the Unified Communications Manager publisher node again
    - switch the Unified Communications Manager publisher node forward to the new software version
    - upgrade the Unified Communications Manager subscriber nodes again
    - switch the Unified Communications Manager subscriber nodes forward to the new software version
    - upgrade the IM and Presence database publisher node again

Upgrade Failure of IM and Presence Subscriber Node

Problem You are upgrading a multinode cluster that includes both Unified Communications Manager and IM and Presence nodes, and the upgrade of the IM and Presence subscriber node fails.

Solution The action that you take depends on the point at which the failure occurred:

- if the upgrade on the IM and Presence subscriber node before the refresh upgrade causes the node to reboot (that is, if the node failed before switching to the new partition), perform the upgrade again on the IM and Presence subscriber node
- if the upgrade on the IM and Presence subscriber node fails after the node switched to the new version, you must complete the following tasks in the order listed:
    - switch the Unified Communications Manager publisher node back to the earlier software version
    - switch the Unified Communications Manager subscriber node back to the earlier software version

- switch the IM and Presence database publisher node back to the earlier software version
- switch the IM and Presence subscriber nodes back to the earlier software version
- switch the Unified Communications Manager publisher node pub forward to the new software version
- switch the IM and Presence database publisher node forward to the new software version
- perform the upgrade again on the IM and Presence subscriber node

IM and Presence user phone presence problems

Problem After an IM and Presence server upgrade, when all activated feature services and network services are started, IM and Presence phone presence from users is delayed or slow to update.

Solution You must restart the Cisco SIP Proxy service. In Cisco Unified IM and Presence Serviceability, select **Tools** > **Control Center - Features Services**.

Presence User Experiences Issues Obtaining Availability

Problem After an IM and Presence Service server upgrade, when all activated feature services and network services are started, a user experiences inconsistent presence availability. The user can log in to IM and Presence Service but experiences issues obtaining availability information mainly from SIP-based clients.

Solution This issue is caused when users are provisioned while IM and Presence Service is being upgraded. You must unassign and then reassign the user.

Real-Time Monitoring Tool alert for Cisco SIP proxy service

Problem After an IM and Presence server upgrade, when all activated feature services and network services are started, a Real-Time Monitoring Tool CoreDumpFileFound alert was generated for the Cisco SIP Proxy service.

Solution You must restart the Cisco SIP Proxy service. In Cisco Unified IM and Presence Serviceability, select **Tools** > **Control Center - Features Services**.

Cannot find upgrade file on remote server

Problem You cannot find the upgrade file on the remote server.

Solution If the upgrade file is located on a Linux or Unix server, you must enter a forward slash at the beginning of the directory path that you want to specify. For example, if the upgrade file is in the patches directory, you must enter /patches. If the upgrade file is located on a Windows server, check with your system administrator for the correct directory path.

Upgrade file checksum values do not match

Problem The checksum value of the upgrade file does not match the checksum indicated on Cisco.com.

Solution The two checksum values must match to ensure the authenticity and integrity of the upgrade file. If the checksum values do not match, download a fresh version of the file from Cisco.com and try the upgrade again.

Database replication did not complete

Problem After an upgrade, database replication did not complete and the result of the command **utils dbreplication runtimestate** was not 2.

Solution After a successful upgrade and switch version to the new software, database replication should take place automatically. During this time core services on the subscriber nodes will not start. Database replication in large deployments can take several hours to complete. If, after several hours, the **utils dbreplication runtimestate** command shows that database replication did not complete, you need to reset the database replication. Run the following command on the publisher node: `utils dbreplication reset all`

Cisco UP Presence Engine database does not restart

Problem After you switch back to Cisco Unified Presence Release 8.6(3) or an earlier software version, the Cisco UP Presence Engine database does not restart.

Solution Ensure that you installed the required COP file, `ciscocm.cup.pe_db_install.cop`, on every node in the cluster after you switched back to Cisco Unified Presence Release 8.6(3), or earlier.

Version Errors

Selected Upgrade Is Disallowed From the Current Version

Problem During a refresh upgrade, the following error is reported: `Error encountered: The selected upgrade is disallowed from the current version.`

Solution You did not install the required COP file on the node. Download the following COP file from Cisco.com: `ciscocm.cup.refresh_upgrade_v<latest_version>.cop`. Restart the server. Install the COP file on every node in the cluster before you attempt the refresh upgrade again.

Version Does Not Match the Active or Inactive Version

Problem During an upgrade on a Cisco IM and Presence server, you cannot select the software image from the disk or remote directory. The following error is reported: `The version obtained from the name does not match the active or inactive version of the publisher.`

Solution The version matching rules have not been met. The software versions must meet the following requirements:

- The software version of the IM and Presence database publisher node (the first IM and Presence node that you upgrade) must match the first two numbers of the software version installed on the Unified

Communications Manager publisher node. The software version installed on the Unified Communications Manager publisher node may be active or inactive. For example, IM and Presence Service software version 10.0.1.10000-1 is compatible with Cisco Unified Communications Manager software version 10.0.1.30000-2.

- The software version of the IM and Presence subscriber nodes that you upgrade must match five numbers of the software version installed on the IM and Presence database publisher node.

Ensure that the first node that you upgrade is either the Unified Communications Manager publisher node or the IM and Presence database publisher node, or select a different image for the software upgrade.

Switch Version on Cisco IM and Presence Node Fails

Problem Switching the version on the Cisco IM and Presence node fails. The following error is reported: `Version mismatch. Please switch versions on the publisher and try again.`

Solution The version matching rules have not been met. The software versions must meet the following requirements:

- The software version of the IM and Presence database publisher node (the first IM and Presence node that you upgrade) must match the first two numbers of the software version installed on the Unified Communications Manager publisher node. For example, IM and Presence Service software version 10.0.1.10000-1 is compatible with Cisco Unified Communications Manager software version 10.0.1.30000-2.
- The software version of the IM and Presence subscriber nodes that you upgrade must match five numbers of the software version installed on the IM and Presence database publisher node.

To correct this error, ensure that the first node that you switch is either theUnified Communications Manager publisher node or the IM and Presence database publisher node.

Failed refresh upgrade

Problem A refresh upgrade failed.

Solution Restart the system, it should reboot to the software version that was running before you attempted the refresh upgrade. If you cannot access the system, you must use the Recovery CD to recover the node.

Cancelled or failed upgrade

If you cancel an upgrade at any stage, or if an upgrade fails, you must reboot the IM and Presence server before you attempt another upgrade.

Directory Was Located and Searched but No Valid Options or Upgrades Were Available

Problem During an IM and Presence Service upgrade, the IM and Presence Service server generates the following error message, even though the upgrade path and file are valid:

```
The directory was located and searched but no valid options or upgrades
were available. Note, a machine cannot be downgraded so option and upgrade
files for previous releases were ignored.
```

Solution The upgrade manager checks for connectivity between IM and Presence Service and Cisco Unified Communications Manager to validate the version during the upgrade. If this fails, the IM and Presence Service server generates the error message even though the upgrade path and file are valid. Use a tool, such as the Cisco Unified CM IM and Presence Administration System Troubleshooter, to check that there is connectivity between IM and Presence Service and Cisco Unified Communications Manager before proceeding with the upgrade.

Common Partition Full Upgrade Failure

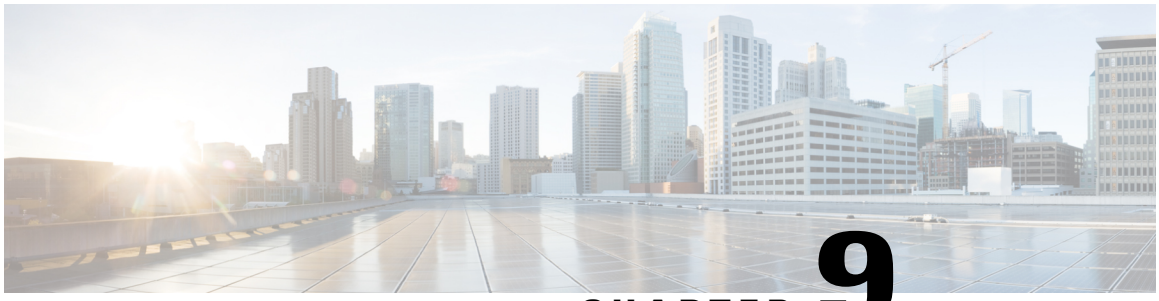
Problem The upgrade of IM and Presence Service fails with an error stating that the common partition is full.

Solution Download and apply the COP file ciscocm.free_common_cup_space_v<latest_version>.cop.sgn. This COP file cleans up the common partition and allows subsequent upgrades to proceed as normal.

PART II

IM and Presence Service OS platform

- Getting started, page 111
- Settings, page 115
- Shutdown and restart, page 119
- Security, page 123
- Security certificate management , page 129
- OpenAM Single Sign-On, page 139
- Software Upgrades, page 141
- Utilities, page 145



CHAPTER 9

Getting started

Use Microsoft Internet Explorer version 6.0 or a later release, or Mozilla Firefox version 3.0 or a later release to access the Cisco Unified IM and Presence Operating System Administration interface. Other browsers are not supported.

- Sign in to Cisco Unified IM and Presence Operating System Administration, page 111
- Recover Administrator password, page 112
- Create customized log-on message, page 113

Sign in to Cisco Unified IM and Presence Operating System Administration

Before You Begin

If you are currently signed in to Cisco Cisco Unified Communications Manager IM and Presence Administration, sign out before proceeding.

Procedure

Step 1 Select **Navigation** > **Cisco Unified IM and Presence OS Administration** from the menu in the upper, right corner of the Cisco Cisco Unified Communications Manager IM and Presence Administration window.

Step 2 Select **Go**.

Step 3 Enter your Administrator username and password.

Step 4 Select **Submit**.

You can also access Cisco Unified IM and Presence Operating System Administration directly by entering the following URL:

`http://server-name/cmplatform`

The Administrator username and password are established during installation or created using the command line interface.

Recover Administrator password

If you lose the Administrator password and cannot access the system, you can reset the Administrator password.

Before You Begin

- During this procedure, you will be required to remove and then insert a valid CD or DVD in the disk drive to prove that you have physical access to the system.

Note At any point, when requested to insert CD or DVD media, it should be mounted through vSphere client for VMWare server.

- The Administrator sign-in must start with an alphabetic character, be at least six characters long, and can contain alphanumeric characters, hyphens, and underscores.
- You will be required to remove, then insert, any valid CD or DVD media through the VMWare-vSphere client. To begin, you must remove any media from the VMWare client CD/DVD drive. You may press Control-C at any time to abort.

Procedure

Step 1 Sign in to the system with the following username and password:
a) Username: **pwrecovery**
b) Password: **pwreset**

Step 2 Press any key when ready.

Step 3 If you have a valid CD or DVD in the disk drive, remove it from the VMWare client CD or DVD drive now.

Step 4 Press any key to continue.
The system tests to ensure that you have removed the CD or DVD from the VMWare client drive.
Note You may press Control-C at any time to abort.

Step 5 Connect the CD or DVD drive from WMWare client and press any key when ready.

Step 6 Insert a valid CD or DVD into the VMWare client drive.

Step 7 After the system verifies that you have inserted the disk, you are prompted to enter a new Administrator password.

Step 8 Reenter the new password.

Step 9 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.
Note During the VMWare pwrecovery/pwreset, if you do not strictly follow the instruction, a few of errors may occur but they can be ignored.

If you want to set up a different Administrator password, use the CLI command **set password**. See the *Command Line Interface Reference Guide for Cisco Unified Solutions* for more information.

The system checks the new password that you enter for strength. If the password does not contain enough different characters, you are prompted to enter a new password.

Create customized log-on message

You can upload a text file that contains a customized log-on message that appears in each of the IM and Presence Service applications administrative interfaces.

Procedure

Step 1 Sign in to Cisco Unified IM and Presence Operating System Administration.

Step 2 Select **Software Upgrades** > **Customized Logon Message**.

Step 3 Select **Browse** to select the text file you want to upload.

Note Text files are the only supported format and must be smaller than 10KB.

Step 4 (Optional) Check the **Require User Acknowledgement** check box.

Step 5 Select **Upload File**.

Step 6 To revert to the default log-on message, select **Delete**.

CHAPTER 10

Settings

You can view and update the following operating system settings:

- IP—the IP addresses and Dynamic Host Configuration Protocol (DHCP) client settings that were entered when the application was installed.
- SMTP—the SMTP host that the operating system uses for sending email notifications.

This section also describes how to change time settings and correct time zone data.

- IP settings, page 115
- NTP settings, page 117
- Change SMTP settings, page 118
- Change time settings, page 118
- Correct time zone data, page 118

IP settings

Change Ethernet settings

You can determine whether Dynamic Host Configuration Protocol (DHCP) is active and locate the related Ethernet IP addresses, as well as the IP address for the network gateway.

Before You Begin

- All Ethernet settings apply only to Eth0. You cannot configure any settings for Eth1. The Maximum Transmission Unit (MTU) on Eth0 defaults to 1500.
- Changing the Ethernet settings causes an immediate system restart.

Procedure

Step 1 Sign in to Cisco Unified IM and Presence Operating System Administration.

Step 2 Select **Settings** > **IP** > **Ethernet**.

Step 3 Enter the new values in the appropriate fields to modify the Ethernet settings, and then select **Save**.

Table 18: Ethernet Settings Fields and Descriptions

Field	Description
DHCP	Indicates whether DHCP is Enabled or Disabled.
Hostname	Shows the name of the host node. **Note** You can only change the hostname after changes to these configuration settings are complete: • DNS • Cisco Unified Communications Manager Application Server List • IM and Presence Topology
IP Address	Shows the IP address of the system. **Note** Changing the IP address or host on the IM and Presence database publisher node can affect system performance.
Subnet Mask	Shows the IP subnet mask address.
Default Gateway	Shows the IP address of the network gateway.

Troubleshooting Tips

If you enable DHCP, the system disables the Port and Gateway setting and it cannot be changed.

Change publisher node IP address on subscriber nodes

If, for network configuration purposes, you changed the IP address or hostname on the IM and Presence Service database publisher node, then you will need to update the IP address of the IM and Presence Service database publisher node on IM and Presence Service subscriber nodes.

Before You Begin

Use this functionality only if you want an IM and Presence Service subscriber node to point to a different IM and Presence Service database publisher node. If this node is the IM and Presence Service database publisher node, be aware that you cannot use this window to change the IP address.

Procedure

Step 1 Sign in to Cisco Unified IM and Presence Operating System Administration.

Step 2 Select **Settings** > **IP** > **Publisher**.

Step 3 Enter the new IM and Presence Service database publisher node IP address.

Step 4 (Optional) Enter a new IM and Presence Service database publisher node name.

Related Topics

Change Ethernet settings, on page 115
Troubleshoot publisher node IP address change on subscriber node, on page 117

Troubleshoot publisher node IP address change on subscriber node

Before You Begin

If the IP address of the IM and Presence database publisher node changes while an IM and Presence subscriber node is offline, be aware that you may not be able to sign in to Cisco Cisco Unified Communications Manager IM and Presence Administration on the IM and Presence subscriber node. Complete this procedure if IM and Presence does not function properly.

Procedure

Step 1 Sign in directly to Cisco Unified IM and Presence Operating System Administration on the subsequent node by using the following URL:`http://node-name/cmplatform` where `node-name` specifies the hostname or IP address of the IM and Presence subscriber node.

Step 2 Enter your Administrator user name and password and select **Submit**.

Step 3 Select **Settings** > **IP** > **Publisher**.

Step 4 Enter the new IP address for the IM and Presence database publisher node and select **Save**.

Step 5 Restart the IM and Presence subscriber node.

Related Topics

Change publisher node IP address on subscriber nodes, on page 116

NTP settings

By design, you cannot configure or change the NTP server following a fresh installation of the IM and Presence Service.

Change SMTP settings

Before You Begin

You must configure an SMTP host if you want the system to send you email, for example, from the Certificate Expiry Monitor.

Procedure

Step 1 Sign in to Cisco Unified IM and Presence Operating System Administration.

Step 2 Select **Settings** > **SMTP**.

Step 3 Enter or modify the SMTP hostname or IP address.

Change time settings

You can manually configure the node time if NTP is currently disabled.

Before You Begin

Before you can manually configure the node time, you must delete any NTP servers that you have configured.

Procedure

Step 1 Sign in to Cisco Unified IM and Presence Operating System Administration.

Step 2 Select **Settings** > **Time**.

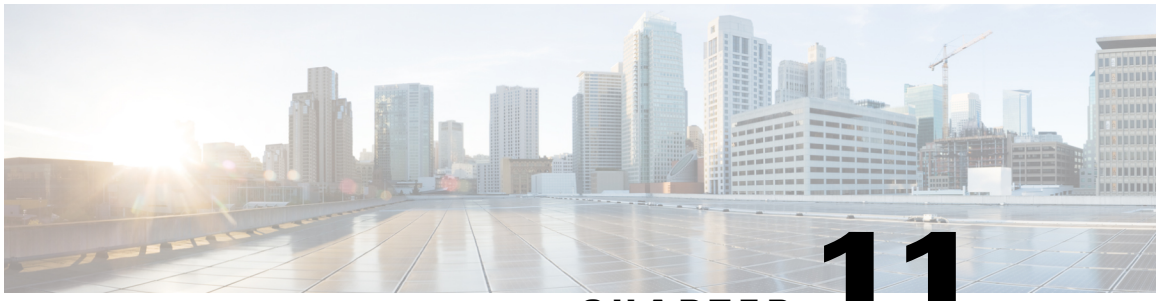
Step 3 Enter the date and time for the system.

Related Topics

Troubleshoot publisher node IP address change on subscriber node, on page 117
Correct time zone data, on page 118

Correct time zone data

The IM and Presence Service includes the latest time zone information and Cisco contacts you about major time zone events. After you install the IM and Presence Service, you can download a COP file with the latest updates. For more information on how to correctly upgrade your time zone data, see the *Release Notes for Cisco Unified Communications Manager* on Cisco.com.



CHAPTER 11

Shutdown and restart

You may need to choose from the following options to shut down or restart the system:

- Shutdown—Stops all running software and shuts down the node.
- Switch Versions—Switches the active and inactive disk partitions and restarts the system. You normally select this option after the inactive partition has been updated and you want to start running a newer software version.
- Restart—Restarts the system without switching partitions.

Note To power down the node, press the **power** button. Note, however, that this action may lead to file system corruption and is not recommended.

- Shut down system, page 119
- Work with Disk Partitions, page 120

Shut down system

Procedure

Step 1 Sign in to Cisco Unified IM and Presence Operating System Administration.

Step 2 Select **Settings** > **Version**.

Step 3 Perform one of the following actions:

a) Select **Shutdown** to halt all processes and shut down the system.

b) Select **Cancel** to stop the operation.
The hardware does not power down automatically. If you press the power button on the server, the system will immediately shut down.

What to Do Next

Work with Disk Partitions, on page 120

Work with Disk Partitions

Revert IM and Presence node to previous version

When you are upgrading to a newer software version and when you need to fall back to an earlier software version, you can shut down the system that is running on the active disk partition and then automatically restart the system using the software version on the inactive partition. The software version running on both the active and inactive partitions is indicated.

Caution This procedure causes the system to restart and become temporarily out of service.

Before You Begin

Upgrade the database on the active partition. The database on the inactive partition does not get updated. If you make changes to the database after an upgrade, you must repeat those changes after switching the partition.

Procedure

Step 1 Sign in to Cisco Unified IM and Presence Operating System Administration.

Step 2 Select **Settings** > **Version**.

Step 3 Perform one of the following actions:

a) Select **Switch Versions** to switch versions and restart the system.

- The system restarts, and the partition that is currently inactive becomes active.
- After you verify that you want to restart the system, the system restarts, which might take up to 15 minutes.

b) Select **Cancel** to stop the operation.

Related Topics

Software Upgrades, on page 141

Restart current version

You can restart the system on the current partition without switching versions.

Caution This procedure causes the system to restart and become temporarily out of service.

Before You Begin

Shut down the system on which the active version is running.

Procedure

Step 1 Sign in to Cisco Unified IM and Presence Operating System Administration.

Step 2 Select **Settings** > **Version**.

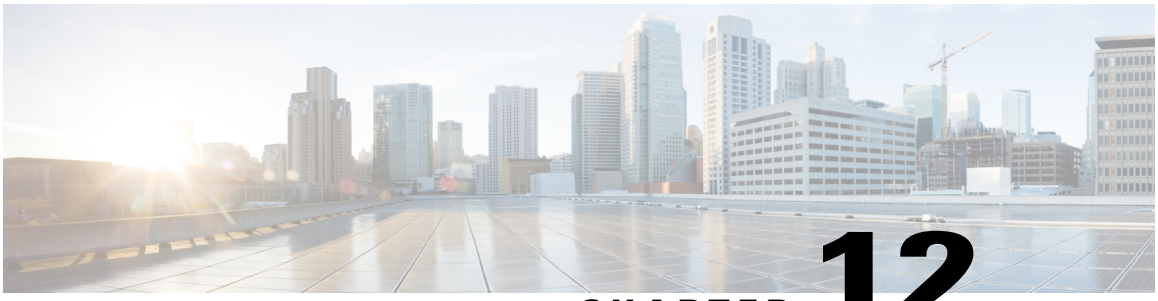
Step 3 Perform one of the following actions:

a) Select **Restart** to restart the system.
The system restarts on the current partition without switching versions.

b) Select **Cancel** to stop the operation.

Related Topics

Shut down system, on page 119



CHAPTER 12

Security

- Browser security, page 123
- IPsec policy management, page 124

Browser security

Verify Internet Explorer Security Settings

To download certificates from the node, you must ensure that your Internet Explorer security settings are configured correctly.

Procedure

Step 1 Start Internet Explorer.

Step 2 Select **Tools** > **Internet Options**.

Step 3 Select the **Advanced** tab.

Step 4 Scroll down to the Security section on the Advanced tab.

Step 5 If necessary, clear **Do not save encrypted pages to disk**.

Step 6 Select **OK**.

Create login banner

From Cisco Unified Presence Release 8.6(4), you can create a banner that users acknowledge as part of their login to any IM and Presence interface. You must create a .txt file using any text editor, include important notifications that you want users to be made aware of, and upload it to Cisco Unified IM and Presence Operating System Administration. This banner will then appear on all IM and Presence Service interfaces notifying users of important information before they login, including legal warnings and obligations. The following interfaces will display this banner before and after a user logs in:

- Cisco Cisco Unified Communications Manager IM and Presence Administration

- Cisco Unified IM and Presence Operating System Administration
- Cisco Unified IM and Presence Serviceability
- Cisco Unified IM and Presence Reporting
- IM and Presence Disaster Recovery System

Procedure

Step 1 Create a .txt file with the contents you want to display in the banner.
Step 2 Sign in to Cisco Unified IM and Presence Operating System Administration.
Step 3 Select **Software Upgrades** > **Customized Logon Message**.
Step 4 Select **Browse and locate the .txt file**.
Step 5 Select **Upload File**.
Step 6 The banner will appear before and after login on most IM and Presence interfaces.

IPsec policy management

Note IPsec is not automatically established between nodes in a cluster during installation of the IM and Presence Service.

Create IPsec policy

You can set up a new IPsec policy. Do not, however, attempt to create IPsec policies during an IM and Presence node upgrade.

Caution IPsec, especially with encryption, will affect the performance of your system.

Before You Begin

To access the Security menu items, you must sign in again to Cisco Unified IM and Presence Operating System Administration using your Administrator password.

Procedure

Step 1 Sign in to Cisco Unified IM and Presence Operating System Administration.
Step 2 Select**Security** > **IPSEC Configuration**.
Step 3 Select **Add New**.
Step 4 Enter the new values in the appropriate fields.

Field	Description
Policy Group Name	Specifies the group name to which the IPsec policy belongs.
Policy Name	Specifies the name of the IPsec policy.
Authentication Method	Specifies the authentication method, for example, Certificate.
Preshared Key	Specifies the preshared key if you selected Pre-shared Key in the Authentication Method field.
Peer Type	Specifies whether the peer is the same type or different.
Certificate Name	Specifies the name of the certificate used for authentication.
Destination Address	Specifies the IP address or FQDN of the destination.
Destination Port	Specifies the port number at the destination.
Source Address	Specifies the IP address or FQDN of the source.
Source Port	Specifies the port number at the source.
Mode	Specifies Tunnel or Transport mode.
Remote Port	Specifies the port number to use at the destination.
Protocol	Specifies the specific protocol, or Any: • TCP • UDP • Any
Encryption Algorithm	From the list box, select the encryption algorithm. Choices include • DES • 3DES
Hash Algorithm	Specifies the hash algorithm: • SHA1—Hash algorithm that is used in phase one IKE negotiation • MD5—Hash algorithm that is used in phase one IKE negotiation

Field	Description
ESP Algorithm	From the list box, select the ESP algorithm. Choices include • NULL_ENC • DES • 3DES • BLOWFISH • RIJNDAEL
Phase One Life Time	Specifies the lifetime for phase one IKE negotiation, in seconds.
Phase One DH	From the list box, select the phase one DH value. Choices include 2, 1, 5, 14, 16, 17, and 18.
Phase Two Life Time	Specifies the lifetime for phase two IKE negotiation, in seconds.
Phase Two DH	From the list box, select the phase two DH value. Choices include 2, 1, 5, 14, 16, 17, and 18.
Enable Policy	Check to enable the IPsec policy.

What to Do Next

Enable or Disable existing IPsec policy, on page 126

Enable or Disable existing IPsec policy

You can enable or disable an existing IPsec policy. Do not, however, attempt to create, enable or disable IPsec policies during an IM and Presence node upgrade.

Caution IPsec, especially with encryption, will affect the performance of your system.

Before You Begin

Complete the steps to create an IPsec policy.

Procedure

Step 1 Sign in to Cisco Unified IM and Presence Operating System Administration.

Step 2 Perform one of the following actions in the IPSEC Policy Configuration frame:

a) Check **Enable Policy** to enable the policy.

b) Uncheck **Enable Policy** to disable the policy.

Related Topics

Create IPsec policy, on page 124

Delete IPsec policy

You can delete one or more IPsec policies. Do not, however, attempt to delete IPsec policies during an IM and Presence node upgrade.

Caution IPsec, especially with encryption, will affect the performance of your system.

Before You Begin

To access the Security menu items, you must sign in again to Cisco Unified IM and Presence Operating System Administration using your Administrator password.

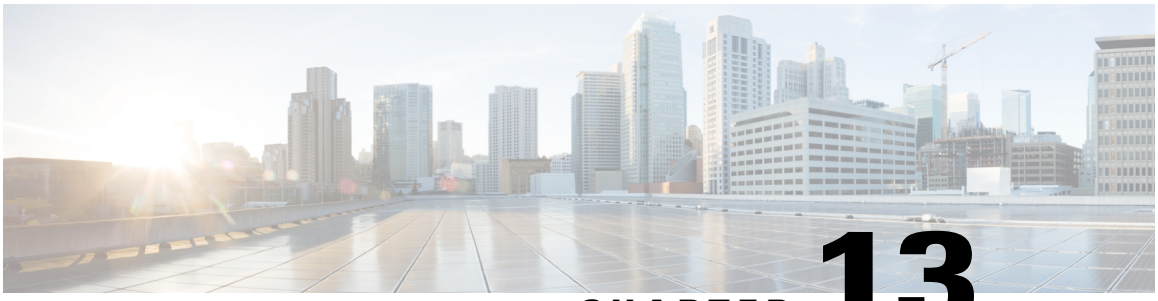
Procedure

Step 1 Sign in to Cisco Unified IM and Presence Operating System Administration.

Step 2 Select **Security** > **IPSEC Configuration**.

Step 3 Select the policy or policies that you want to delete.

Step 4 Select **Delete**.



CHAPTER 13

Security certificate management

The operating system security options enable you to manage security certificates in these two ways:

- Certificate Management—Manages certificates, Certificate Trust Lists (CTL), and Certificate Signing Requests (CSR). You can display, upload, download, delete, and regenerate certificates.
- Certificate Monitor—Allows you to monitor the expiration dates of the certificates on the node.

- Certificates and certificate trust list management, page 129
- Third Party CA certificates, page 135

Certificates and certificate trust list management

View Certificates

Before You Begin

To access the Security menu items, you must sign in again to Cisco Unified IM and Presence Operating System Administration using your Administrator password.

Procedure

Step 1 Sign in to Cisco Unified IM and Presence Operating System Administration.

Step 2 Select **Security** > **Certificate Management**.

Step 3 Perform one of the following actions:

If you want to:	Action
Filter the certificate list	Enter your search criteria, and use the **Find** controls as follows: • To filter or search records, perform one of the following actions: ◦ From the first list box, select a search parameter. ◦ From the second list box, select a search pattern. ◦ Specify the appropriate search text, if applicable. • Select **Find**.
View details of a certificate or trust store	Select the .PEM or .DER file name of the certificate.
Return to the Certificate List window	• Select **Back To Find/List** in the Related Links list. • Select **Go**.

Download certificate or certificate trust list

Before You Begin

To access the Security menu items, you must sign in again to Cisco Unified IM and Presence Operating System Administration using your Administrator password.

Procedure

Step 1 Sign in to Cisco Unified IM and Presence Operating System Administration.

Step 2 Select **Security** > **Certificate Management**.

Step 3 If required, use the Find controls to filter the certificate list as follows:

a) To filter or search records, perform one of the following actions:

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

b) Select **Find**.

Step 4 Select the file name of the certificate or CTL.

Step 5 Select **Download**.

Delete certificate

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

Caution Deleting a certificate can affect your system operations. If there is an existing CSR for the certificate you select from the Certificate list, it is deleted from the system and you must generate a new CSR.

Before You Begin

To access the Security menu items, you must sign in again to Cisco Unified IM and Presence Operating System Administration using your Administrator password.

Procedure

Step 1 Sign in to Cisco Unified IM and Presence Operating System Administration.

Step 2 Select **Security** > **Certificate Management**.

Step 3 If required, use the Find controls to filter the certificate list as follows:

a) To filter or search records, perform one of the following actions:

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

b) Select **Find**.

Step 4 Select the file name of the certificate or CTL.

Step 5 Select **Delete**.

Related Topics

Generate certificate signing request, on page 137

Regenerate certificate

A certificate of type “cert” is the only type of certificate that you can regenerate.

Caution Regenerating a certificate can affect your system operations.

Before You Begin

To access the Security menu items, you must sign in again to Cisco Unified IM and Presence Operating System Administration using your Administrator password.

Procedure

Step 1 Sign in to Cisco Unified IM and Presence Operating System Administration.

Step 2 Select **Security** > **Certificate Management**.

Step 3 Select **Generate New**.

Step 4 Select a certificate name from the Certificate Name list.

Table 19: Certificate Names and Descriptions

Name	Description
tomcat	This self-signed root certificate is generated during the installation of the IM and Presence Service node for the Cisco Tomcat service. **Note** If you want to regenerate a Cisco Unified Communications Manager certificate, you need to regenerate the certificate on the Cisco Unified Communications Manager node. You can not regenerate Cisco Unified Communications Manager certificates from an IM and Presence node. **Note** If you upload or regenerate a Tomcat certificate in an IM and Presence Service cluster, you must restart the Cisco Tomcat service using the OS Administration CLI command: `utils service restart Cisco Tomcat`
ipsec	This self-signed root certificate is generated during the installation of the IM and Presence Service node and is required for secure IPsec server connections.
cup	This self-signed root certificate is generated during the installation of the IM and Presence node. **Note** If this security certificate is regenerated restart the following services: • Cisco SIP Proxy service • Cisco Presence Engine service

Name	Description
cup-xmpp	This self-signed root certificate is generated during the installation of the IM and Presence node. **Note** If this security certificate is regenerated restart the Cisco XCP Router service.
cup-xmpp-s2s	This self-signed root certificate is generated during the installation of the IM and Presence node. **Note** The trust certificates for cup-xmpp-s2s are stored in cup-xmpp-trust along with the general XMPP trust certificates. **Note** If this security certificate is regenerated restart the Cisco XCP Router service.

Step 5 Select **Generate CSR** .

Upload certificate or certificate trust list

Caution Uploading a new certificate or certificate trust list (CTL) file can affect your system operations.

Before You Begin

- The system does not automatically distribute non-trust single server certificates such as tomcat, cup, cup-xmpp, cup-xmpp-s2s, and ipsec to other nodes on the cluster. Multi-Server SAN based certificates, including their signing certificates, are automatically distributed to other nodes on the cluster and only need to be uploaded to one IM and Presence Service node per cluster.
- The Cisco Intercluster Sync Agent service automatically distributes trust certificates such as tomcat-trust, cup-trust, cup-xmpp-trust, and ipsec-trust to other nodes on the cluster and to any configured IM and Presence Service Intercluster peers. This process can take up to 30 minutes to complete. A manual upload of trust certificates to other nodes can be performed if required.
- To access the Security menu items, you must sign out and sign back in to Cisco Unified IM and Presence Operating System Administration using your Administrator password.

Procedure

Step 1 Sign in to Cisco Unified IM and Presence Operating System Administration.
Step 2 Select **Security** > **Certificate Management**.
Step 3 Select **Upload Certificate** .
Step 4 Select the name of the certificate or CTL from the **Certificate Name** drop-down list.
Step 5 Select the file to upload by completing the following actions:

a) Enter the path to the file in the **Upload File** text box.
b) Select **Browse** and navigate to the file.
c) Select **Open**.

Step 6 Select **Upload File** to upload the file to the node.

Step 7 Restart the services that are affected by the new certificate.

Configure Certificate Revocation

You can use the OCSP to obtain the revocation status of the certificate. To configure OCSP, follow this procedure.

Before You Begin

You must upload the Online Certificate Status Protocol (OCSP) Responder certificate to tomcat-trust before enabling OCSP.

Procedure

Step 1 Navigate to **Security** > **Certificate Revocation**
The Certificate Revocation window displays.

Step 2 Check the **Enable OCSP** check box in the **Online Certificate Status Protocol Configuration** area.

Step 3 Choose one of the following options:

Option	Description
Use OCSP URI from Certificate	Choose this option if the certificate is configured with OCSP URI and is to be used to contact OCSP Responder. To verify that there is an OCSP URI in the certificate, complete the following steps: **1** Select **Security** > **Certificate Management**. **2** Search for the certificate using the Find filters. **3** Select the .PEM file or .DER file link for the certificate. **4** In the **Certificate Configuration** window, ensure that there is an entry for Extension:AuthorityInfoAccessSyntax and that it has an accessLocation URL.
Use configured OCSP URI	Choose this option if external or configured URI is used to contact OCSP Responder. Enter the URI of the OCSP Responder, where certificate revocation status is verified, in the OCSP Configured URI field.

Step 4 Select **Save**.
The certificate revocation status check is performed only during upload of a certificate or certificate chain. The appropriate alarm will be raised if a certificate is revoked.

Troubleshoot certificate errors

If you encounter an error when attempting to access Cisco Unified Communications Manager services from an IM and Presence node or IM and Presence services from a Cisco Unified Communications Manager node, there is a problem with the tomcat-trust certificate. The error message "Connection to the Server cannot be established (unable to connect to Remote Node)" will appear the following Serviceability interface pages:

- Service Activation
- Control Center - Feature Services
- Control Center - Network Services

This procedure provides steps 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 the Cisco Unified IM and Presence OS Administration interface, 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 Select the certificate to obtain information about the certificate and verify that the content matches the contents of the same 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 have not addressed the certificate error and an IM and Presence tomcat-trust certificate is present, delete the certificate. After you delete the certificate, you must manually exchange it by downloading the Tomcat certificate for each node, and uploading it to its peers as a tomcat-trust certificate. After the certificate exchange is complete, restart Cisco Tomcat on each impacted server: **utils service restart Cisco Tomcat**.

Third Party CA certificates

Cisco Unified Operating System supports certificates that a third-party Certificate Authority (CA) issues with PKCS # 10 Certificate Signing Request (CSR).

To use an application certificate that a third-party CA issues, you must obtain both the signed application certificate and the CA root certificate from the CA. Get information about obtaining these certificates from your CA. The process varies among CAs.

IM and Presence Service Certificate Signing Requests (CSRs) include extensions that you must include in your request for an application certificate from the CA. If your CA does not support the ExtensionRequest

mechanism, you must enable the X.509 extensions that are listed in the generated CSR file. For information on how to view the extensions in the generated CSR file, see View Certificates.

Cisco verified third-party certificates that were obtained from Microsoft, Keon, and Verisign CAs. Certificates from other CAs might work but have not been verified.

Cisco Unified Operating System generates certificates in DER and PEM encoding formats and generates CSRs in PEM encoding format. It accepts certificates in PEM and DER encoding formats.

Public Certificate Authorities (CA) typically require Certificate Signing Requests (CSRs) to conform to specific formats. For example, a public CA might only accept CSRs that:

- Are Base64-encoded
- Do not contain certain characters, such as @&!, in the Organization, OU, or other fields.
- Use specific bit lengths in the server's public key

Likewise, if you submit CSRs from multiple nodes, public CAs might require that the information is consistent in all CSRs.

To prevent issues with your CSRs, you should review the format requirements from the public CA to which you plan to submit the CSRs. You should then ensure that the information you enter when configuring your server conforms to the format that the public CA requires.

Third-party certificate process management

This procedure provides an overview of the third-party certificate process, with references to each step in sequence:

	Task	For More Information
Step 1	Generate a CSR on the node.	See Generate certificate signing request, on page 137.
Step 2	Download the CSR to your PC.	See Download certificate signing request, on page 137.
Step 3	Use the CSR to obtain an application certificate from a CA.	Get information about obtaining application certificates from your CA.
Step 4	Obtain the CA root certificate.	Get information about obtaining a root certificate from your CA.
Step 5	Upload the CA root certificate to the node.	See Upload certificate or certificate trust list, on page 133.
Step 6	Upload the application certificate to the node.	See Upload certificate or certificate trust list, on page 133.
Step 7	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 certificate). For information about restarting services, see the *Cisco Unified Serviceability Administration Guide*.

Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager describes in detail how to upload the following types of CA signed certificates to an IM and Presence Service deployment:

- tomcat certificate
- cup-xmpp certificate
- cup-xmpp-s2s certificate

Generate certificate signing request

Before You Begin

- To access the Security menu items, you must sign in again to Cisco Unified IM and Presence Operating System Administration using your Administrator password.
- For the current release of the Cisco Unified IM and Presence Operating System, the Directory option is no longer available in the list of Certificate Names. However, you can still upload a Directory Trust certificate from a previous release, which is required for the DirSync service to work in Secure mode.

Procedure

Step 1 Sign in to Cisco Unified IM and Presence Operating System Administration.
Step 2 Select **Security** > **Certificate Management**.
Step 3 Select **Generate CSR**.
Step 4 Select the certificate name from the **Certificate Name** list.
Step 5 Select **Generate CSR** .

Related Topics

Upload directory trust certificate

Download certificate signing request

Before You Begin

To access the Security menu items, you must sign in again to Cisco Unified IM and Presence Operating System Administration using your Administrator password.

Procedure

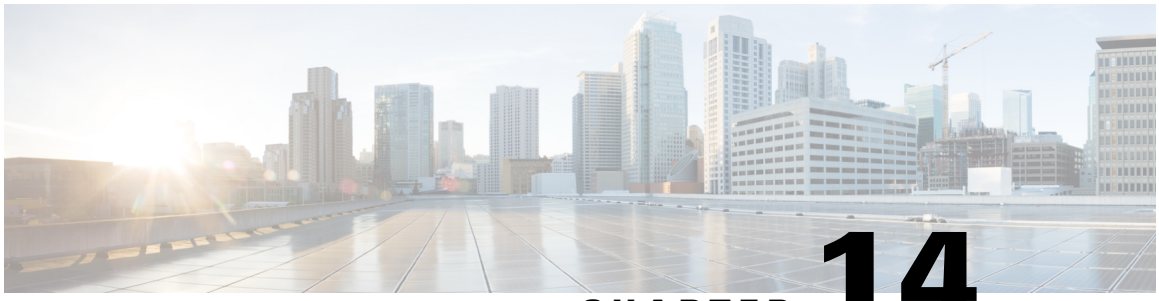
Step 1 Sign in to Cisco Unified IM and Presence Operating System Administration.
Step 2 Select **Security** > **Certificate Management**.
Step 3 Select **Download CSR**.
Step 4 Select the certificate name from the **Certificate Name** list.
Step 5 Select **Download CSR**.

Monitor certificate expiration dates

The system can automatically send you an email when a certificate is close to its expiration date.

Procedure

Step 1 Sign in to Cisco Unified IM and Presence Operating System Administration.
Step 2 Select **Security** > **Certificate Monitor** to view the current Certificate Expiration Monitor configuration.
Step 3 In the **Notification Start Time** field, enter the number of days before the certificate expires that you want to be notified.
Step 4 In the **Notification Frequency** field, enter the frequency for notification, either in hours or days.
Step 5 Check the **Enable E-mail Notification** check box to enable email notification.
Step 6 In the **E-mail IDs** field, enter the email address to which you want notifications sent.
Note For the system to send notifications, you must configure an SMTP host.
Step 7 Select **Save**.



CHAPTER 14

OpenAM Single Sign-On

- OpenAM Single Sign-On, page 139

OpenAM Single Sign-On

Introduction

There are two types of Single Sign-On (SSO): OpenAM SSO and Security Assertion Markup Language (SAML) SSO. The Cisco Unified IM and Presence Operating System interface is used to configure OpenAM SSO only. For information about SAML SSO, see the *Features and Services Guide for Cisco Unified Communications Manager*.

The OpenAM SSO feature allows end users to log in to Windows and use the following IM and Presence applications without being required to sign in again:

- Cisco Unified CM IM and Presence Administration
- Cisco Unified IM and Presence Serviceability
- Cisco Unified IM and Presence Reporting
- IM and Presence Disaster Recovery System
- Real-Time Monitoring Tool (RTMT) Administration
- Cisco Unified IM and Presence Operating System Administration
- Cisco Client Profile Agent

Set up OpenAM Single Sign-On

To configure OpenAM SSO, select **Cisco Unified IM and Presence OS Administration > Security > Single Sign On**.

The SSO feature is divided into three components:

- Status
- Server Settings

- Select Applications

Status

A warning message displays indicating that the change in SSO settings causes Tomcat to restart.

The following error messages may display when enabling the SSO feature:

- Invalid Open Access Manager (OpenAM) server URL - This error message displays when you give an invalid OpenAM server URL.
- Invalid profile credentials - This error message displays when you give a wrong profile name or wrong profile password or both.
- Security trust error - This error message displays when the OpenAM certificate has not been imported.

Note If you get any of the above error messages while enabling SSO, the status changes to the related error.

Server Settings

The node settings are editable only when SSO is disabled for all applications.

Select Applications

You can enable or disable SSO on any of the following applications:

- Cisco Cisco Unified Communications Manager IM and Presence Administration - Enables SSO for Cisco Cisco Unified Communications Manager IM and Presence Administration, Cisco Unified IM and Presence Serviceability, and Cisco Unified IM and Presence Reporting
- Cisco Unified IM and Presence Operating System Administration - Enables SSO for Cisco Unified IM and Presence Operating System Administration and IM and Presence Disaster Recovery System
- Real-Time Monitoring Tool - Enables the web application for the Real-Time Monitoring Tool
- Cisco Client Profile Agent - Enables SSO for the Cisco Client Profile Agent service. This option is only available to customers using Common Access Card (CAC) sign-on.

Procedure

Step 1 Enter the URL of the Open Access Manager (OpenAM) server.

Example:
```
https://opensso.sample.com:443/opensso
```

Step 2 Enter the relative path where the policy agent should be deployed. The relative path must be alphanumeric.

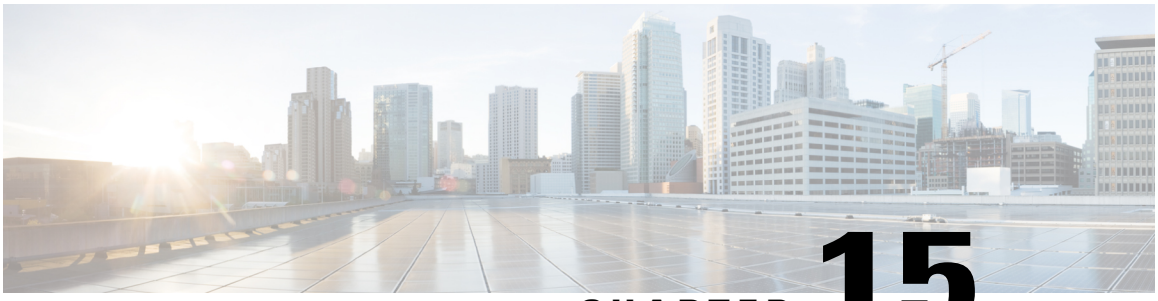
Step 3 Enter the name of the profile that is configured for this policy agent.

Step 4 Enter the password of the profile name.

Step 5 Enter the login module instance name that is configured for Windows Desktop SSO.

Step 6 Click **Save.**

Step 7 In the **Confirmation** dialog box, click **OK** to restart Tomcat.



CHAPTER 15

Software Upgrades

- Software upgrades, page 141
- Locale-specific upgrades , page 141

Software upgrades

You can perform software upgrades by using the Software Upgrades menu options, or using the Command Line Interface. The system can only upload and process software that Cisco approves.

You can access the upgrade file during the installation process from either a local DVD or from a remote FTP or SFTP server.

For detailed information about planning and performing a software upgrade, see the IM and Presence Service information in the *Upgrade Guide for Cisco Unified Communications Manager*.

Locale-specific upgrades

Locale installer

Cisco provides locale-specific versions of the IM and Presence Locale Installer on www.cisco.com. Installed by the system administrator, the locale installer allows the user to view/receive the chosen translated text or tones, if applicable, when a user works with supported interfaces.

User locale files provide translated text and voice prompts, if available, for phone displays, user applications, and user web pages in the locale that the user selects. User-only locale installers exist on the web.

When installing IM and Presence locales, you must install the user local files which contain language information for a specific language and country and use the following convention:

ps-locale-*language-country-version*.cop

Locale file installation

Note Before you install a locale for a country on IM and Presence, you must first install the Cisco Unified Communications Manager locale file for the same country on the Cisco Unified Communications Manager cluster.

You can install more than one locale file on each node in the cluster. You must restart each node in the cluster after installation to activate the new locales. For more information about installing locales, see *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.

Error Messages

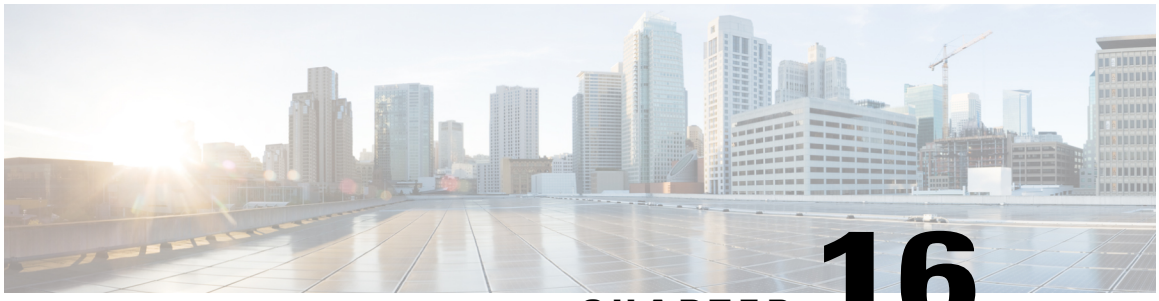
See the following table for a description of the messages that can occur during Locale Installer activation. If an error occurs, you can view the messages in the installation log.

Table 20: Locale Installer Messages and Descriptions

Message	Description
[LOCALE] File not found: <language>_<country>_user_locale.csv, the user locale has not been added to the database.	This error occurs when the system cannot locate the CSV file, which contains user locale information to add to the database, which indicates an error with the build process.
[LOCALE] File not found: <country>_network_locale.csv, the network locale has not been added to the database.	This error occurs when the system cannot locate the CSV file, which contains network locale information to add to the database This indicates an error with the build process.
[LOCALE] CSV file installer installdb is not present or not executable	You must ensure that an application called *installdb* is present. It reads information that a CSV file contains and applies it correctly to the target database. If this application is not found, it did not get installed with the Cisco Unified Communications application (very unlikely), has been deleted (more likely), or the node does not have a Cisco Unified Communications application, such as Cisco Unified Communications Manager or IM and Presence Service, installed (most likely). Installation of the locale will terminate because locales will not work without the correct records in the database.

Message	Description
[LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maDialogs_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maMessages_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maGlobalUI_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/LocaleMasterVersion.txt.Checksum.	These errors could occur when the system fails to create a checksum file, which an absent Java executable, `/usr/local/thirdparty/java/j2sdk/jre/bin/java`, `an absent or damaged Java archive file, /usr/local/cm/jar/cmutil.jar`, or an absent or damaged Java class, `com.cisco.ccm.util.Zipper`, causes. Even if these errors occur, the locale will continue to work correctly, with the exception of Cisco Unified Communications Manager Assistant, which can not detect a change in localized Cisco Unified Communications Manager Assistant files.
[LOCALE] Could not find /usr/local/cm/application_locale/cmservices/ipma/LocaleMasterVersion.txt in order to update Unified CM Assistant locale information.	This error occurs when the system does not find the file in the correct location, which is most likely due to an error in the build process.
[LOCALE] Addition of <locale-installer-file-name> to the database has failed!	This error occurs because the collective result of any failure that occurs when a locale is being installed causes it; it indicates a terminal condition.
[LOCALE] Could not locate <locale-installer-file-name>	The system will not migrate this locale during an upgrade. The downloaded locale installer file no longer resides in the download location. The platform may have moved or deleted it. This is noncritical error indicates that after the Cisco Unified Communications application has been upgraded, you need to either reapply the locale installer or download and apply a new locale installer.
[LOCALE] Could not copy <locale-installer-file-name> to migratory path. This locale will not be migrated during an upgrade!	You cannot copy the downloaded locale installer file to the migration path. This noncritical error indicates that after the Cisco Unified Communications application has been upgraded, you need to either reapply the locale installer or download and apply a new locale installer.
[LOCALE] DRS unregistration failed	The locale installer could not deregister from the Disaster Recovery System. A backup or restore record will not include the locale installer. Record the installation log and contact Cisco TAC.

Message	Description
[LOCALE] Backup failed!	The Disaster Recovery System could not create a tarball from the downloaded locale installer files. Re-apply the local installer before attempting to back up. **Note** Manually reinstalling locales after a system restore achieves the same goal.
[LOCALE] No COP files found in restored tarball!	Corruption of backup files may prevent successful extraction of locale installer files. **Note** Manual reapplication of the locale installer will restore the locale fully.
[LOCALE] Failed to successfully reinstall COP files!	Corruption of backup files may damage locale installer files. **Note** Manual reapplication of the locale installer will restore the locale fully.
[LOCALE] Failed to build script to reinstall COP files!	The platform could not dynamically create the script used to reinstall locales. **Note** Manual reapplication of the locale installer will restore the locale fully. Record the installation log and contact TAC.



CHAPTER 16

Utilities

The Cisco Unified IM and Presence Operating System application provides the following 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.

- Ping another node, page 145
- Set up a remote account, page 146

Ping another node

You can ping another node in the network and view the resulting statistics.

Procedure

Step 1 Sign in to Cisco Unified IM and Presence Operating System Administration.
Step 2 Select **Services** > **Ping**.
Step 3 Enter the IP address or network name for the system that you want to ping.
Step 4 Enter the ping interval in seconds.
Step 5 Enter the packet size.
Step 6 Select a ping iteration value to set the number of times that you want to ping the system.
Step 7 Select whether you want to validate IPsec. If you do, check **Validate IPSec.**
Step 8 Select **Ping**.

Troubleshooting Tips

When you specify multiple pings, the ping command does not display the ping date and time in real time. Be aware that the Ping command displays the data after the number of pings that you specified completes.

Set up a remote account

In the **Remote Account Support** window, you can set up a remote account, for a specified period of time, that Cisco support personnel can use to access your system.

The remote support process works like this:

Procedure

Step 1 You set up a remote support account. This account includes a configurable time limit on how long Cisco personnel can access it.

Step 2 When you set up the remote support account, a pass phrase is generated.

Step 3 You call Cisco support personnel and provides the remote support account name and pass phrase.

Step 4 Cisco support personnel enter the pass phrase into a decoder program that generates a password.

Step 5 Cisco support personnel sign into the remote support account on your system by using the decoded password. When the account time limit expires, Cisco support personnel can no longer access your remote support account.

Configure remote support

Procedure

Step 1 Sign in to Cisco Unified IM and Presence Operating System Administration.

Step 2 Select **Services** > **Remote Support**.

Step 3 If no remote support account is configured, select **Add**.

Step 4 Complete the fields in the **Remote Access Configuration Status** window, as described in the table below.

Table 21: Remote Access Configuration Fields and Descriptions

Field	Description
Account name	Enter an account name for the remote account. Ensure the account name comprises at least six characters in all lowercase, alphabetic characters
Expiration	Enter the account life duration in days.

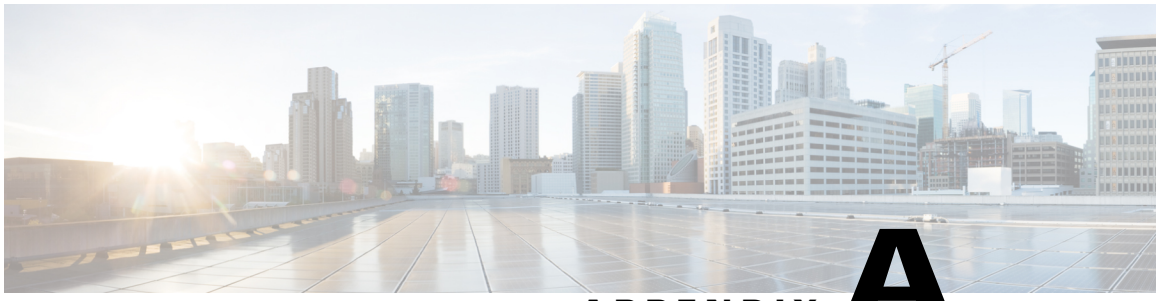
Step 5 Select **Save**.

Step 6 Review these system-generated parameters:

Field	Description
Passphrase	Displays the generated pass phrase.

Field	Description
Decode version	Indicates the version of the decoder in use.

Step 7 Contact your Cisco personnel to access the remote support system using the generated pass phrase.



APPENDIX A

Component status in Cisco Unified Operating System

- View Cluster Nodes Status, page 149
- View Hardware Status, page 150
- View Network Status, page 151
- View Installed Software, page 152
- View System Status, page 152
- View IP Preferences, page 153

View Cluster Nodes Status

Procedure

Step 1 Sign in to Cisco Unified IM and Presence Operating System Administration.

Step 2 Select **Show** > **Cluster**.

Step 3 Review the fields in the Cluster window.

Table 22: Cluster Nodes Field Descriptions

Field	Description
Hostname	The complete hostname of the node.
IP Address	The IP address of the node.
Alias	The alias name of the node, when defined.
Type of Node	Indicates whether the server is an IM and Presence database publisher node or an IM and Presence subscriber node.

View Hardware Status

Procedure

Step 1 Sign in to Cisco Unified IM and Presence Operating System Administration.

Step 2 Select **Show** > **Hardware**.

Step 3 Review the fields in the **Hardware Status** window, as described in the table below.

Table 23: Hardware Status Field Descriptions

Field	Description
Platform Type	The model identity of the platform node.
Serial Number	The serial number of the platform node.
Virtual Hardware	Indicates if the virtual hardware is configured.
Virtual Support	Indicates if the virtual hardware is supported.
Processor Speed	Processor speed (measured in MHz) in the platform node.
CPU Type	The type of processor in the platform node.
Memory	The total amount of memory in MBytes.
Object ID	Used by SNMP to identify an object.
OS Version	The version of the platform operating system.
RAID Details	Status of the RAID controller and logical drive if the machine is RAID enabled.

View Network Status

Before You Begin

The network status information that displays depends on whether Network Fault Tolerance is enabled. When Network Fault Tolerance is enabled, Ethernet port 1 automatically takes over network communications if Ethernet port 0 fails. If Network Fault Tolerance is enabled, network status information displays for the network ports Ethernet 0, Ethernet 1, and Bond 0. If Network Fault Tolerance is not enabled, status information displays only for Ethernet 0.

Procedure

Step 1 Sign in to Cisco Unified IM and Presence Operating System Administration.

Step 2 Select **Show** > **Network**.

Step 3 Review the fields in the **Network Configuration** window, as described in the table below.

Table 24: Network Settings Field Descriptions

Field	Description
DHCP	Indicates whether DHCP is enabled for Ethernet port 0.
Status	Indicates whether the port is Up or Down for Ethernet ports 0 and 1.
IP Address	The IP address of Ethernet port 0 (and Ethernet port 1 if Network Fault Tolerance (NFT) is enabled).
IP Mask	The IP mask of Ethernet port 0 (and Ethernet port 1 if NFT is enabled).
Link Detected	Indicates whether an active link exists.
Queue Length	The length of the queue.
MTU	The maximum transmission unit.
MAC Address	The hardware address of the port.
License MAC	The license MAC for this deployment of IM and Presence Service.
Receive Statistics	Information about received bytes and packets.
Transmit Statistics	Information about transmitted bytes and packets.
Primary DNS	The IP address of the primary domain name node.
Secondary DNS	The IP address of the secondary domain name node.

Field	Description
Domain	The domain of the node.
Gateway	The IP address of the network gateway on Ethernet port 0.

View Installed Software

You can view the software versions and installed software options.

Procedure

Step 1 Sign in to Cisco Unified IM and Presence Operating System Administration.

Step 2 Select **Show** > **Software**.

Step 3 Review the fields in the **Software Packages** window described in the table below.

Table 25: Software Packages Field Descriptions

Field	Description
Partition Versions	The software version that is running on the active and inactive partitions.
Active Version Installed Software Options	The versions of installed software options, including locales and dial plans, that are installed on the active version.
Inactive Version Installed Software Options	The versions of installed software options, including locales and dial plans, that are installed on the inactive version.

View System Status

Procedure

Step 1 Sign in to Cisco Unified IM and Presence Operating System Administration.

Step 2 Select **Show** > **System**.

Step 3 Review the fields in the **System Status** window, as described in the table below.

Table 26: Platform Status Field Descriptions

Field	Description
Host Name	The name of the Cisco MCS host where Cisco Unified Operating System is installed.
Date	The date and time based on the continent and region that were specified during operating system installation.
Time Zone	The time zone that was chosen during installation.
Locale	The language that was chosen during the operating system installation.
Product Version	The product version that is currently installed and running.
Platform Version	The platform version.
Unified OS Version	The operating system version.
License MAC	The license MAC for this deployment of IM and Presence Service.
Uptime	The system uptime information.
CPU	The percentage of CPU capacity that is idle, the percentage that is running system processes, and the percentage that is running user processes.
Memory	Information about memory usage, including the amount of total memory, free memory, and used memory in KBytes.
Disk	Displays the amount of total, free, and used disk space on the active and inactive disks. Disk logging displays the amount of total, free, and disk space that is used for disk logging.

View IP Preferences

Procedure

Step 1 Sign in to Cisco Unified IM and Presence Operating System Administration.

Step 2 Select **Show** > **IP Preferences**.

Step 3 To filter or search records, perform one of the following actions:

a) From the first list box, select a search parameter.

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

Step 4 Select **Find**.

Step 5 Review the fields in the **System Status** window.

Table 27: IP Preference Field Descriptions

Field	Description
Application	The name of the application.
Protocol	The type of protocol that this application will use, for example, TCP or UDP.
Port Number	The port number that is configured for this application.
Type	The type of transport that this application will use: • Public • Private • Translated
Translated Port	The translated port number that is configured for this application.
Status	Indicates whether the application is enabled or disabled.
Description	The description of the application.

INDEX

A

administrator password 8, 112

C

Certificate Trust List, See CTL
certificates 30, 32, 33, 35, 38, 39, 129, 130, 131, 133, 137, 138
  deleting 32
  displaying 30, 129
  downloading 30, 130
  downloading a signing request 38, 137
  expiration monitor fields 39
  expiration monitor fields (table) 138
  managing 129
  monitoring expiration dates 39, 138
  regenerating 32, 33, 131
  uploading 35, 133
CLI 5
cluster nodes 11, 149
  fields 11
  fields (table) 149
  procedure 11, 149
Command Line Interface 5
  See also CLI
configuration 3, 11, 149
  operating system 3, 11, 149
CTL 30, 129, 130, 133
  downloading 30, 130
  managing 129
  uploading 133

D

dial plan installation 98

E

error messages 95, 142
  descriptions 95
  descriptions (table) 142
Ethernet settings 19

H

hardware 12, 150
  fields 12
  fields (table) 150
  procedure 12, 150
  status 12, 150

I

install/upgrade 4, 141
  menu 4, 141
installed software 14, 152
  fields (table) 14, 152
  procedure 14, 152
installing 91, 98, 141, 142
  dial plan 98
  locales 91, 141, 142
Internet Explorer 29, 123
  set security options 29, 123
IPSec 41, 47, 124, 126
  changing policy 47, 126
  displaying policy 47, 126
  management 41, 124
  policy fields 41
  policy fields (table) 124
  setting up new policy 41, 124

L

locales 91, 95, 141, 142
  files 141
  installation 91, 141
  installer 95, 142
    error messages 95
    error messages (table) 142
  installing 142
logging in 7, 111
  overview 7, 111
  procedure 7, 111

M

menu 3, 4, 141
  install/upgrade 4, 141
  security 4
  settings 4
  show 3
messages 95, 142
  error 95, 142

N

network status 13, 151
  fields (table) 13, 151
  procedure 151
nodes 11, 149
  cluster 11, 149
  fields 11
  fields (table) 149
  procedure 11, 149
NTP server settings 22

O

operating system 3, 4, 5, 7, 8, 11, 12, 13, 19, 26, 111, 112, 115, 120, 141, 149, 150, 151
  administrator password 8, 112
  configuration 3, 11, 149
  hardware status 12, 150
    fields 12
    fields (table) 150
    procedure 12, 150
  introduction 3
  logging in 7, 111
  network status fields (table) 13, 151
  overview 3
  restart 26, 120
operating system *(continued)*
  security 4
  services 5
  settings 4, 19, 115
  software upgrades 4, 141
  status 3, 11, 149

P

password 8, 112
  recovering 8, 112
ping 51, 145
publisher settings 21, 116

R

remote support 52, 146
  setting up 52, 146
  status fields 52
  status fields (table) 146
restart 25, 26, 119, 120
  current version 26, 120
  system 25, 119

S

security 4, 29, 123, 129
  configuration 4
  menu 4
  overview 29, 123, 129
  set IE options 29, 123
services 5, 51, 52, 145, 146
  overview 51, 145
  ping 5, 51, 145
  remote support 5, 52, 146
    overview 52, 146
    setting up 52, 146
settings 4, 19, 21, 22, 23, 115, 116, 117, 118
  Ethernet 19, 115
    fields 19
    fields (table) 115
    procedure 19
  IP 19
  menu 4
  NTP servers 22
  overview 19, 115
  publisher 21, 116
  SMTP 23, 117, 118
  time 23, 118

show 3
menu 3
shutdown 26, 119
operating system 26, 119
SMTP settings 23, 117, 118
software 4, 14, 55, 83, 141, 152
installed 14, 152
fields (table) 14, 152
procedure 14, 152
upgrades 4, 55, 83, 141
from remote source 83
overview 55, 141
status 3, 11, 12, 13, 15, 149, 150, 151, 152, 153
hardware 12, 150
fields 12
fields (table) 150
procedure 12, 150
network 13, 151
fields (table) 13, 151
procedure 151
operating system 3, 11, 149
system 15, 152, 153
fields 15
fields (table) 152, 153
status *(continued)*
system *(continued)*
procedure 15, 152, 153
supported products 96
system 15, 25, 26, 119, 152, 153
restart 25, 119
shutdown 26, 119
status 15, 152, 153
fields 15
fields (table) 152, 153
procedure 15, 152, 153

T

TFTP server 98
installing files 98
time settings 23, 118

V

version 26, 120
restart 26, 120