Cisco Unified Communications Operating System Administration Guide, Release 9.0(1)

First Published: July 18, 2012

Last Modified: July 18, 2012

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-27113-01

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 used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses 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)

© 2013 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface — Preface ix

Purpose ix

Audience ix

Organization ix

Related documentation x

Conventions x

Obtain support xi

Security overview xi

PART I — Cisco Unified CM OS platform 1

CHAPTER 1 — Introduction 3

Overview 3

Browser requirements 4

Operating system status 4

Settings 4

Security configuration 5

Software upgrades 5

Services 6

Command Line Interface 6

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 12
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 30
Delete and regenerate certificate 31
Delete trust certificate 31
Regenerate certificate 32
Certificate regeneration if intracluster communication is enabled using EMCC 34
Upload certificate 34
Upload certificate or certificate chain 34
Upload third-party CA certificates 35

Third-party signed certificate or certificate chain 36
Generate certificate signing request 36
Download certificate signing request 37
Third-party CA certificates 37
Monitor certificate expiration 38
Certificate revocation 39
Configure Online Certificate Status Protocol 39
Troubleshoot certificate errors 39
IPsec 40
Set up IPsec policy 40
Migration characteristics 44
Manage IPsec policies 45
Bulk certificate management 46
Export certificates 46
Import certificates 47
Configure the SSO application 48

CHAPTER 7 Services 51
Ping 51
Set up remote support 52

CHAPTER 8 Software upgrades 55
Pre-upgrade tasks 56
Upgrade considerations 58
Software upgrade process overview 58
Upgrade configuration changes 59
Administration changes 59
Upgrade tasks 60
User provisioning 61
Upgrade a cluster 61
Supported upgrades 62
Presence Data Loss After Upgrade Cisco Unified Business Edition 5000 to Cisco Unified Communications Manager 63
Obtain upgrade file 63
Software upgrade procedures 63

Local source software upgrade 63
Upgrade from local source 63
Remote source upgrade 64
SFTP server support 64
Remote source software upgrade 65
Bridge upgrade 66
Post-upgrade tasks 68
Reduced permissions for Access Control Groups 69
Revert to previous version 69
Revert cluster to previous version 69
Revert node to previous version 70
Reset database replication 70
COP files, dial plans, and locales 71
COP file installation 71
Dial plan installation 71
Locale installation 71
Locale installation considerations 72
Locale files 72
Error messages 72
Supported products 74
Manage TFTP server files 74
Set up a custom log-on message 75

PART II IM and Presence service OS platform 77

CHAPTER 9 Getting started 79
Sign in to Cisco Unified IM and Presence Operating System Administration 79
Recover Administrator password 80
Create customized log-on message 81

CHAPTER 10 Settings 83
IP settings 83
Change Ethernet settings 83
Change IP publisher node address on subsequent nodes 84
Troubleshoot IP publisher node address change on subsequent node 85

NTP settings 85
Change SMTP settings 86
Change time settings 86
Correct time zone data 86

CHAPTER 11 Shutdown and restart 87
Shut down system 87
Work with disk partitions 88
Revert IM and Presence node to previous version 88
Restart current version 88

CHAPTER 12 Security 91
Browser security 91
Verify Internet Explorer security settings 91
Create login banner 91
IPsec policy management 92
Create IPsec policy 92
Enable or Disable existing IPsec policy 94
Delete IPsec policy 95

CHAPTER 13 Security certificate management 97
Certificates and certificate trust list management 97
View certificates 97
Download certificate or certificate trust list 98
Delete certificate 99
Regenerate certificate 99
Upload certificate or certificate trust list 100
Upload directory trust certificate 101
Configure certificate revocation 101
Third Party CA certificates 102
Third-party certificate process management 103
Generate certificate signing request 103
Download certificate signing request 104
Monitor certificate expiration dates 104

CHAPTER 14 Single Sign-On 107

Introduction 107

Set up Single Sign-On 107

CHAPTER 15 Software Upgrades 109

Software upgrades 109

Locale-specific upgrades 109

Locale installer 109

Locale file installation 110

Error messages 110

CHAPTER 16 Utilities 113

Ping another server 113

Set up a remote account 114

Configure remote support 114

APPENDIX A Component status in Cisco Unified Operating System 117

View cluster nodes status 117

View hardware status 118

View network status 118

View installed software 120

View system status 120

View IP preferences 121

Preface

- Purpose, page ix
- Audience, page ix
- Organization, page ix
- Related documentation, page x
- Conventions, page x
- Obtain support, page xi

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	“Unified CM 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.

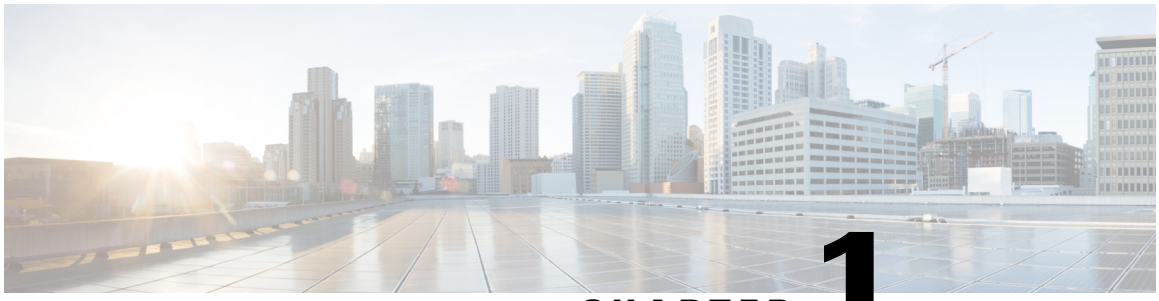
Further information regarding U.S. export regulations may be found at

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

PART I

Cisco Unified CM OS platform

- Introduction, 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

Introduction

This chapter provides information about Cisco Unified Communications Manager, from which you can perform many common system administration functions through the Cisco Unified Communications Operating System.

- Overview, page 3
- Browser requirements, page 4
- Operating system status, page 4
- Settings, page 4
- Security configuration, page 5
- Software upgrades, page 5
- Services, page 6
- Command Line Interface, page 6

Overview

Cisco Unified Communications Operating System Administration allows you to configure and manage the Cisco Unified Communications Operating System. Administration tasks include the following examples:

- 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.

The following sections describe each operating system function in more detail.

Browser requirements

You can access Cisco Unified Communications Operating System by using the following browsers:

You can access Cisco Unified Communications Operating System with this browser...	...if you use one of these operating systems
Microsoft Internet Explorer 8	• Microsoft XP SP3 • Microsoft Vista SP2 [or later service pack (SP)] • Microsoft Windows 7 with the latest SP
Mozilla Firefox 3.x	• Microsoft XP SP3 • Microsoft Vista SP2 (or the latest SP) • Microsoft Windows 7 with the latest SP • Apple Mac OS X with the latest SP
Safari 4.x	• Apple Mac OS X

Ensure the URL of the Cisco Unified Communications Operating System node (`https://node_name`) is included in the browser "Trusted Site Zone" or the "Local Intranet Site Zone" for all product features to work correctly.

Operating system status

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

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

Related Topics

Status and configuration, on page 11

Settings

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

- IP - Updates the IP addresses and Dynamic Host Configuration Protocol (DHCP) client settings that were entered when the application was installed.
- NTP Server settings - Configures the IP addresses of an external NTP server; add or delete an NTP server.
- SMTP settings - Configures the SMTP host that the operating system will use for sending e-mail 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.

Note This command does not power down the server. To power down the server, press the power button.

Related Topics

Settings, on page 19
System Restart, on page 25

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.

Related Topics

Security, on page 29

Software upgrades

The software upgrade options enable you 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 gets 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. See the *Upgrade Guide for the Cisco Unified Communications Manager* for more information.

Note You must do all software installations and upgrades by using the software upgrades features that are included in the Cisco Unified Communications Operating System GUI and command line interface. The system can upload and process only software that Cisco Systems approved. 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:

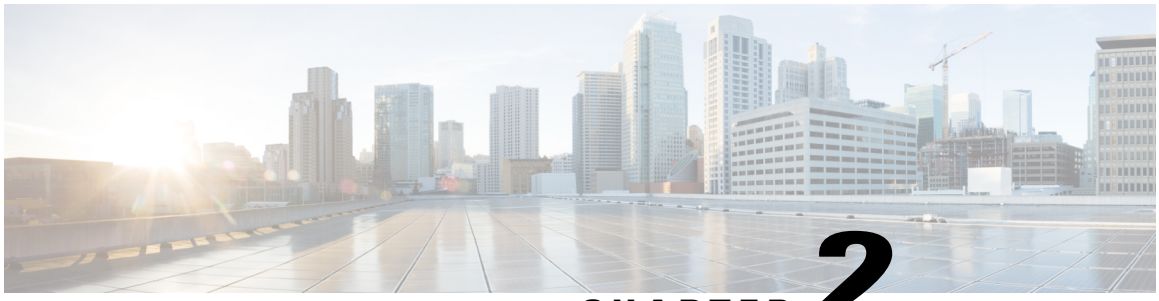
- Ping - Checks connectivity with other network devices.
- Remote Support - Sets up an account that Cisco support personnel can use to access the system. This account automatically expires after the number of days that you specify.

Related Topics

Services, on page 51

Command Line Interface

You can access a command line interface from the console or through a secure shell connection to the server. For more information, refer to 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.

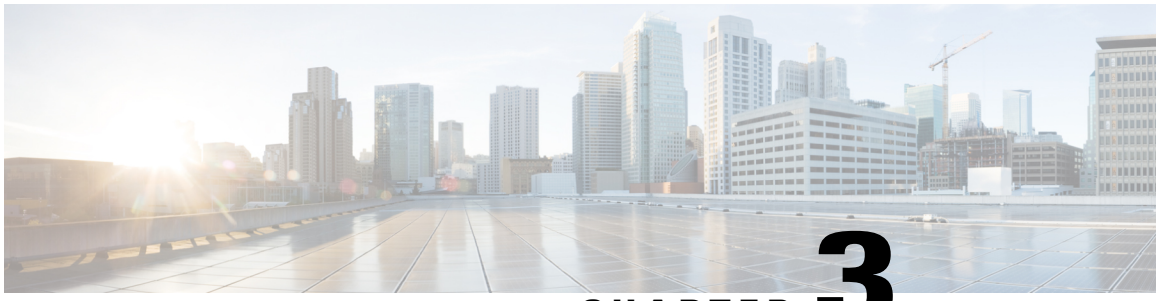
Step 6 After the system verifies that you have inserted the disk, you get prompted to enter one of the following options to continue:
a) Enter a to reset the administrator password.
b) Enter s to reset the security password.
c) Enter q to quit.

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 12
- 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
Type of Node	Indicates whether the node is a publisher node or a 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.
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.
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.

Field	Description
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.
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 Cisco MCS 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.
Platform Version	Displays the platform 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.
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.

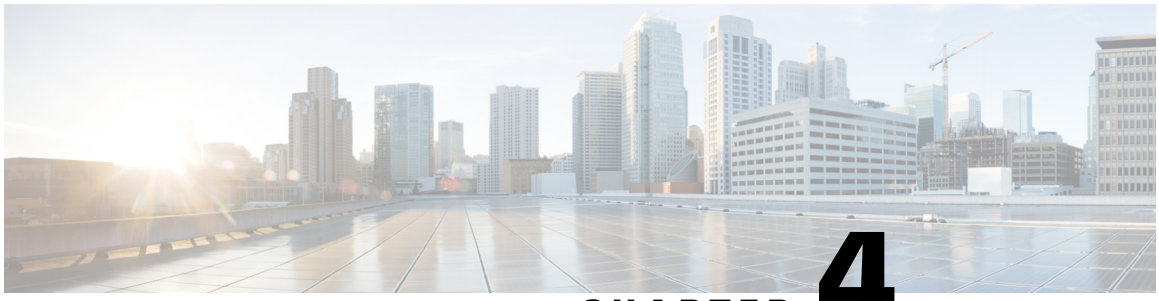
Step 3 Click **Find**.
All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

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.

Field	Description
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 subsequent nodes, to set the IP address of the publisher.

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 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 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. **Note** If you run Cisco Unified Communications Manager on a virtualized server and you change this value, you must obtain a replacement license file that is registered to the calculated license Mac based on the new value.
IP Address	Displays the IP address of the system. **Note** If you run Cisco Unified Communications Manager on a virtualized server and you change this value, you must obtain a replacement license file that is registered to the calculated license Mac based on the new value.
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 Release 8.6(1) 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 Communications 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.
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 subsequent or subscriber nodes, you can view or change the IP address of the first node or publisher for the 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 publisher IP settings, 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 publisher IP address on subsequent nodes of the cluster, not on the publisher itself.

Step 2 Enter the new publisher IP address.

Step 3 Click **Save**.

Set up IP address

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

Procedure

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

where node-name specifies the host name or IP address of the subsequent 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 publisher and click **Save**.

Step 5 Restart the subsequent node.

Set up NTP servers

Ensure that external NTP servers are stratum 5 or higher (1-9). To add, delete, or modify an external NTP server, follow this procedure:

Note You can only configure the NTP server settings on the first node or publisher.

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.

Note If you run Cisco Unified Communications Manager on a virtualized server and you change this value, you must obtain a replacement license file that is registered to the calculated license MAC based on the new value.

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**.

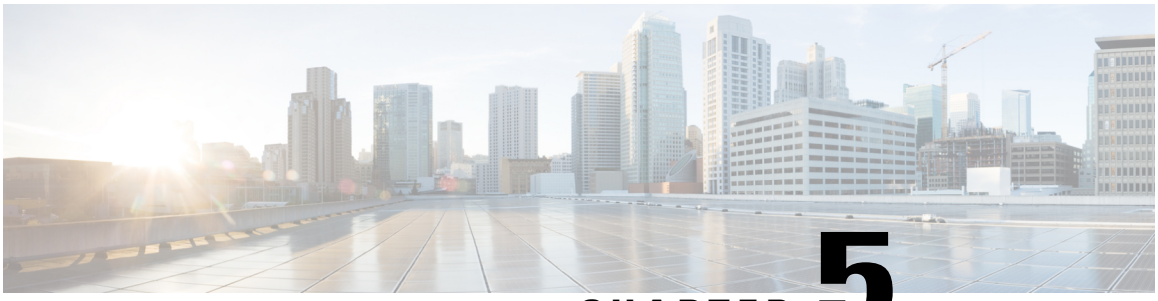
Step 2 Enter the date and time for the system.

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:

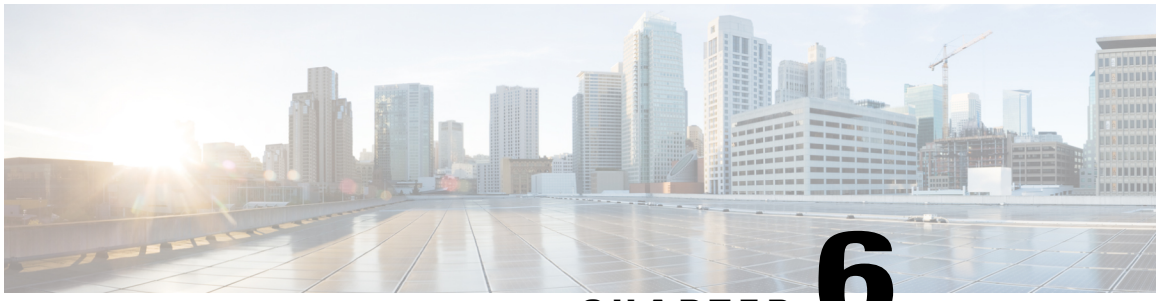
a) Shut down the system from the Cisco Unified Communications Operating System Administration window.

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 40
- Bulk certificate management, page 46
- Configure the SSO application, page 48

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.

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 and CAPF
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 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 36
Download certificate signing request, on page 37
Third-party CA certificates, on page 37
Third-party signed certificate or certificate chain, on page 36

Third-party signed certificate or certificate chain

Upload the 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 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 having only CA Certificates, choose the certificate name with the format certificate type-trust. When you upload an application certificate or Certificate chain having 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 having application certificate and CA Certificates.

When you upload a CAPF CA root certificate, it gets 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 recently generated CSR that was used to obtain signed certificate and overwrites the existing certificate including 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 of the cluster.

Note For the current release of the Cisco Unified Operating System, the Directory option no longer displays 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 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) containing both the application certificate and CA certificates. Get information about obtaining these certificates from your CA. The process varies among CAs.

Cisco Unified Communications Operating System generates CSRs in PEM encoding format. It 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:

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

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. **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 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 is a problem with the tomcat-trust certificate. A "Connection to the Server cannot be established (Unable to connect to Remote Node)" error will appear on any of the following Serviceability interface pages:

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

This procedure provides steps for you to try when attempting to resolve the certificate error. Each step is progressive and not necessarily sequential. In some cases, you will 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 the CLI, restart the Cisco Certificate Change Notification service: **utils service restart Cisco Certificate Change Notification**.

Step 4 After waiting 30 minutes, if the previous steps have not addressed the certificate error, delete the problem tomcat-trust certificates and manually exchange them by downloading the Tomcat certificate for each node and uploading it to its peers as a tomcat-trust certificate. Following the certificate exchange, restart Cisco Certificate Change Notification service on each impacted 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.
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.

Field	Description
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
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.

Field	Description
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.
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.

Field	Description
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
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. You must have a minimum of one token that is the same among all clusters.

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 47

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 the SSO application

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

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 Manger (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 Unified CM Administration - Enables SSO for Cisco Unified CM Administration, Cisco Unified Serviceability, and Cisco Unified Reporting
- Cisco Unified CM User Options - Enables SSO for Cisco Unified CM User Options
- 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.

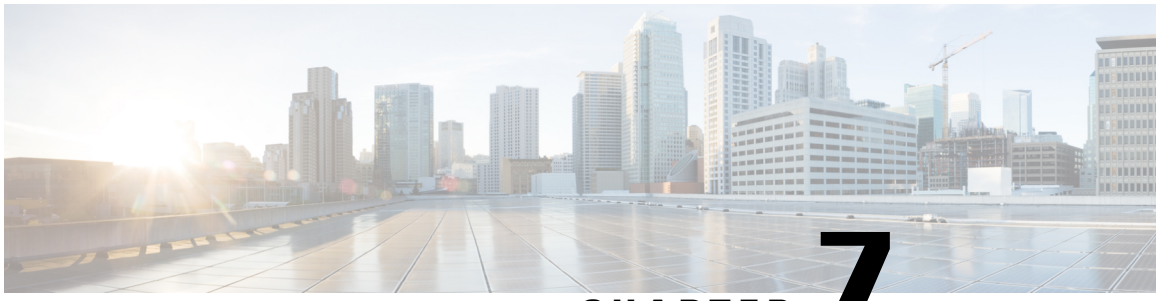
Step 3 Enter the name of the profile that is configured for this policy agent.

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.

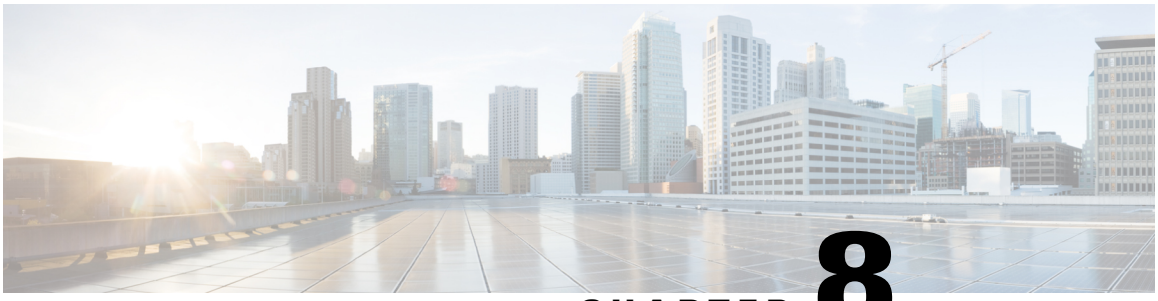
Step 4 Click **Save**.
The Remote Support Status window displays. For descriptions of fields on the Remote Support Status window, see the following table.

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

This chapter provides information about upgrading software.

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

Caution When you upgrade to Cisco Unified Communications Manager 8.6(1) the system will reboot as part of the upgrade process. Therefore, you may want to perform the upgrade during a scheduled down time for your organization to avoid service interruptions.

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).

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.

- Pre-upgrade tasks, page 56
- Upgrade considerations, page 58
- Software upgrade procedures, page 63
- Post-upgrade tasks, page 68
- Revert to previous version, page 69
- COP files, dial plans, and locales, page 71
- Manage TFTP server files, page 74
- Set up a custom log-on message, page 75

Pre-upgrade tasks

Before you begin the upgrade, perform the following tasks:

- 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, such as JTAPI, CUMA (Cisco Unified Manager Assistant), RTMT, IPCC, firewalls, and so on.

  For Cisco Unified Communications Manager, the release notes are located at

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

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

  For more information on obtaining and installing licenses, see the License File Upload chapter in the *Cisco Unified Communications Manager Administration Guide*.

Note As part of this upgrade, Enterprise License Manager is installed automatically. Following the upgrade, Enterprise License Manager can be used to provide simplified, enterprise-wide management of user-based licensing, including license fulfillment. Enterprise License Manager handles licensing fulfillment, supports allocation and reconciliation of licenses across supported products, and provides enterprise level reporting of usage and entitlement. For more information, see the *Enterprise License Manager User Guide*.

Warning You must 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 Enterprise 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.

- Before you begin the upgrade, back up your system. This is particularly important if you are upgrading software on HP7825H3 or HP7828H3 hardware as there is no option to revert to the previous version.

- If you are upgrading software on HP7825H3 or HP7828H3 hardware, ensure that you have a 16GB USB device available to migrate your data to the new system. For Cisco Unity Connection and Cisco Business Edition 5000, a 128GB external USB device is required.
- Disable 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 Be aware that, when you deactivate the Cisco Extension Mobility service, Cisco Extension Mobility users cannot log in and log out of phones that support Cisco Extension Mobility.

- Do not install Cisco Unified Communications Manager in a large Class A or Class B subnet that contains a large number of devices. When you install Cisco Unified Communications Manager in a large subnet with a large number devices in that subnet, the Address Resolution Protocol (ARP) table can fill up quickly (maximum 1024 entries, by default). When the ARP table gets full, Cisco Unified Communications Manager can have difficulty talking to endpoints and cannot add more phones.
- Before you upgrade to a later release, refer to the documentation for your currently installed COP files to identify any special considerations related to upgrading Cisco Unified Communications Manager.
- If you plan to use IPv6 with Cisco Unified Communications Manager Release 8.0(2) or later, you can provision your DNS server for IPv6 prior to upgrading to Release 8.0(2) or later. However, do not configure the DNS records for Cisco Unified Communications Manager for IPv6 until after you perform the upgrade.

Caution Configuring the DNS records for Cisco Unified Communications Manager for IPv6 prior to upgrading to Release 8.0(2) or later causes the upgrade to fail.

- Before you upgrade a cluster, execute the **utils network ipv6 ping** CLI command to verify IPv6 networking on the first node (publisher node) and subsequent nodes (subscriber nodes). If IPv6 is configured incorrectly on the subsequent nodes, load detection may take 20 minutes.
- Use the **utils dbreplication setrepltimeout** CLI command to increase the database replication timeout value when upgrading large clusters so that more subscriber nodes have sufficient time to request replication. When the timer expires, the first subscriber node, plus all other subscriber nodes that requested replication within that time period, begin a batch data replication with the 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 subscriber nodes have successfully set up replication. For more information, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.
- Before you perform the Cisco Unified Communications Manager upgrade, 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.
- Review the following related topic after you complete the pre-upgrade tasks.

Related Topics

Upgrade considerations, on page 58

Upgrade considerations

This section contains topics which should be reviewed prior to performing an upgrade.

Caution There is a known issue with upgrades from Unified CM 6.x or 7.x. Upgrades from these releases may fail with the upgrade installdb log indicating a communication or connection issue in BulkMigration. This issue is noted in CSCts34871. The workaround is to reboot the system and perform the upgrade again. See CSCts34871 in Bug Toolkit on Cisco.com for further details.

Software upgrade process overview

You cannot install upgrade software on your node while the system continues to operate.

Caution If you are upgrading your software on HP 7825H3 or HP7828H3 hardware, there is no option to revert to the previous version of Cisco Unified Communications Manager. To perform an upgrade on one of these machines you must use a 16GB USB device to facilitate data migration from the old system to the new installation. For Cisco Unity Connection and Cisco Business Edition 5000, a 128GB external USB device is required.

When you install upgrade software, there will be a temporary node outage while the Cisco Unified Communications Manager software is installed. Once you kick off the upgrade using either the command line or graphical user interface the data will be exported, and the system will be automatically rebooted at which point the node outage will begin. The duration of this outage will depend on your configuration and amount of data. During the upgrade, progress can be monitored via the console until such time that command line interface and graphical user interface access has been restored. Once restored, you can use the command line interface or graphical user interface to continue to monitor upgrade progress.

Note If an administrator or a phone user makes changes during the upgrade process (export of data), that data could be lost after upgrade.

When you initiate the upgrade, you can indicate to activate the partition with the new upgrade software or return to using the partition with the previous version of the software at upgrade completion. With the exception of HP 7825H3 and HP7828H3 hardware upgrades, the previous software remains in the inactive partition until the next upgrade. Your configuration information migrates automatically to the upgraded version in the active partition.

When you upgrade a cluster, start by upgrading the publisher node. You can begin upgrading subsequent nodes in parallel after the publisher node reaches a specified point in the upgrade. There will be a temporary node outage until all subscriber nodes get upgraded to the new software version. See the section *Upgrade a cluster* for more information about determining when to begin upgrading subsequent nodes.

All nodes 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 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 get lost.

Note You can only make changes to 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.

If the upgrade of a subsequent node fails after you upgrade the publisher node and switch it to the new version or fail to upgrade one of the subsequent nodes in your cluster during the upgrade cycle, you can do one of the following:

- Correct the errors that caused the upgrade failure on the subsequent node. You may want to check the network connectivity of the nodes in your cluster, reboot the subsequent node, ensure the node memory and CPU usage on the subsequent node is not too high. Upgrade the subsequent node again.
- Make sure that the active partition of the publisher node runs the newest version of software installed on the node. Perform a fresh installation on the subsequent node using the same software version as that running on the active partition of the publisher node. If you are reinstalling the subsequent node, you should delete the node from Cisco Unified Communications Manager Administration and add the node again as described in the *Cisco Unified Communications Manager Administration Guide*.

You can upgrade from a DVD (local source) or from a network location (remote source) that the node can access.

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 might get unset. 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.

Note Be sure to back up your system data before starting the software upgrade process. For more information, see the *Disaster Recovery System Administration Guide*. If you are upgrading your software on HP 7825H3 or HP7828H3 hardware, there is no option to revert to the previous version of Cisco Unified Communications Manager. If you do not back up your system data before starting the software upgrade process your data will be lost if your upgrade fails for some reason. If you chose to revert to the prior version, you will need to install the prior version and restore your data from your DRS backup.

Related Topics

Upgrade a cluster, on page 61

Upgrade configuration changes

This section describes the restrictions that apply to the configuration and provisioning changes that you can make during an upgrade.

Administration changes

The administrator must not make any configuration changes to Cisco Unified Communications Manager during an upgrade. Configuration changes include any changes that you make in Cisco Unified Communications Manager Administration, Cisco Unified Serviceability, and the User Option windows.

Any configuration changes that you make during an upgrade could get lost after the upgrade completes, and some configuration changes can cause the upgrade to fail.

If you are upgrading your system, you must complete the upgrade tasks in this section before you perform any configuration tasks.

Caution If you fail to follow these recommendations, unexpected behavior may occur; for example, ports may not initialize as expected.

Upgrade tasks

To successfully complete the upgrade, perform the upgrade tasks in the following order before you begin making configuration changes.

Note Cisco strongly recommends that you do not perform configuration tasks until the upgrade completes on all nodes in the cluster, until you have switched the nodes over to the upgraded partition, and until you have verified that database replication is functioning.

For more information, see the refresh upgrade procedure in the *Cisco Unified Communications Manager Security Guide*.

Procedure

Step 1 If you are performing a refresh upgrade from Cisco Unified Communications Manager Release 7.x, see the *Cisco Unified Communications Manager Security Guide* for more information about the upgrade procedure.

Step 2 Stop all configuration tasks; that is, do not perform configuration tasks in the various Cisco Unified Communications Manager-related GUIs or the CLI (with the exception of performing the upgrade in the Cisco Unified Communications Operating System GUI).

Step 3 Upgrade the first node in the cluster (the publisher node).

Note If performing an L2 upgrade, choose no for automatic reboot. The switch version will occur in step 4.

Note If performing an refresh upgrade, choose to run new version at the completion of the upgrade. Step 4 is not required.

Step 4 Upgrade the subsequent nodes in the cluster (the subscriber nodes).

Note If performing an L2 upgrade, choose no for automatic reboot. The switch version will occur in step 5.

Note If performing an refresh upgrade, choose to run new version at the completion of the upgrade. Step 5 is not required.

Step 5 Switch over the first node to the upgraded partition.

Step 6 Switch over subsequent nodes to the upgraded partition.

Note You can switch the subsequent 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 and the subsequent nodes. You can check database replication status by using one of the following methods:

- In Cisco Unified Reporting, access the Unified CM 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.
- 1 - Replication setup script fired from this node.
- 2 - Good replication.
- 3 - Bad replication.
- 4 - Replication setup did not succeed.

Before you proceed, ensure that you have a good database replication status. For more information about using the Real Time Monitoring Tool, see the *Cisco Unified Real Time Monitoring Tool Administration Guide*.

Step 8 When all other upgrade tasks are complete, you can perform any needed configuration tasks as required.

User provisioning

For upgrades from Cisco Unified Communications Manager Release 8.x, changes that are made to the following user-facing features get preserved after the upgrade completes:

- Call Forward All (CFA)
- Message Waiting Indication (MWI)
- Privacy Enable/Disable
- Do Not Disturb Enable/Disable (DND)
- Extension Mobility Login (EM)
- Hunt Group Logout
- Device Mobility
- CTI CAPF status for end users and application users
- Credential hacking and authentication
- Recording enabling
- Single Number Reach enabling

Upgrade a cluster

When you upgrade a cluster, begin upgrading the publisher node first. You can begin upgrading subsequent nodes after the publisher node has finished upgrading. There will be a temporary server outage until all subscriber nodes get upgraded to the new software version.

During the upgrade of the publisher node, you can view the installation log, install_log_<date+time>.log, by using the Software Installation/Upgrade window in Cisco Unified Communications Operating System Administration or the command line interface (CLI). You can also use the CLI to search for the relevant information in the install log by following this procedure:

Procedure

Step 1 List the install logs; for example:

```
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
```

Step 2 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
```

What to Do Next

After the publisher node has been upgraded, you can start to upgrade the subsequent nodes. When you are ready to activate the new version, you must activate the new software on the publisher node before activating it on all other nodes.

Caution If you attempt to upgrade the subsequent nodes in parallel with the publisher node, do not choose the Reboot to upgraded partition on either publisher node or subsequent nodes while configuring the upgrade options. If selected, the publisher node may complete its upgrade and reboot while the subsequent nodes are upgrading, which causes the upgrade of the subsequent nodes to fail.

Supported upgrades

For information about supported upgrades, see the Release Notes for your product release and the Cisco Unified Communications Manager Compatibility Matrix at the following URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_device_support_tables_list.html

Presence Data Loss After Upgrade Cisco Unified Business Edition 5000 to Cisco Unified Communications Manager

There is no upgrade path in VMware to upgrade from Cisco Unified Business Edition 5000 to Cisco Unified Communications Manager. A fresh installation is needed. After you perform the fresh installation, IM and Presence Service re-synchronizes data with the new Cisco Unified Communications Manager. The Syncagent uses the primary key (pkid) as a comparison field for the synchronization. When the Cisco Unified Communications Manager is re-installed, all the pkid on Cisco Unified Communications Manager are changed. As such, any existing data on IM and Presence Service is cleaned up and the Syncagent deletes the old data. Be sure to backup your data before performing this procedure.

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.

Software upgrade procedures

This section provides procedures for upgrading from either a local or a remote source.

Local source software upgrade

Upgrade from local source

To upgrade the software from local DVD, follow this procedure:

Procedure

Step 1 If you are upgrading software on HP7825H3 or HP7828H3 hardware insert the 16GB USB device to facilitate data migration from the old system to the new installation. For Cisco Unity Connection and Cisco Business Edition 5000, a 128GB external USB device is required.

Caution If you are upgrading your software on HP7825H3 or HP7828H3 hardware, there is no option to revert to the previous version of Cisco Unified Communications Manager. To perform an upgrade on one of these machines you must use a 16GB USB device to facilitate data migration from the old system to the new installation. For Cisco Unity Connection and Cisco Business Edition 5000, a 128GB external USB device is required.

Step 2 If you do not have a Cisco-provided upgrade disk, create an upgrade disk by burning the upgrade file that you downloaded onto a DVD as an ISO image.

Note Just copying the .iso file to the DVD will not work. Most commercial disk burning applications can create ISO image disks.

Step 3 Insert the new DVD into the disc drive on the local server that is to be upgraded.

Step 4 Log in to Cisco Unified Communications Operating System Administration.

Step 5 Navigate to **Software Upgrades** > **Install/Upgrade**.
The Software Installation/Upgrade window displays.

Step 6 From the **Source** list, choose **DVD**.

Step 7 Enter a slash (/) in the Directory field.

Step 8 To use the Email Notification feature, enter your Email Destination and SMTP Server in the fields provided.

Step 9 To continue the upgrade process, click **Next**.

Step 10 Choose the upgrade version that you want to install and click **Next**.

Step 11 In the next window, monitor the progress of the download.

Step 12 If you want to run the upgraded software at the completion of the upgrade process and automatically reboot to the upgraded partition, choose **Switch to new version after upgrade**. The system restarts and is running the upgraded software.

Step 13 If you want to install the upgrade and then manually switch to the upgraded partition at a later time, do the following steps:

a) Choose **Do not switch to new version after upgrade**.
b) Click **Next**.
The Upgrade Status window displays the Upgrade log.
c) When the installation completes, click **Finish**.
d) To restart the system and activate the upgrade, choose **Settings** > **Version**; then, click **Switch Version**.
The system restarts running the upgraded software.

Remote source upgrade

Caution If you are upgrading your software on HP7825H3 or HP7828H3 hardware, there is no option to revert to the previous version of Cisco Unified Communications Manager. To perform an upgrade on one of these machines you must use a 16GB USB device to facilitate data migration from the old system to the new installation. For Cisco Unity Connection and Cisco Business Edition 5000, a 128GB external USB device is required.

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.

Remote source software upgrade

To upgrade the software from a network location or remote server, use the following procedure.

Note Do not use the browser controls, such as Refresh/Reload, while you are accessing Cisco Unified Communications Operating System Administration. Instead, use the navigation controls that are provided by the interface.

Procedure

Step 1 If you are upgrading software on HP7825H3 or HP7828H3 hardware insert the 16GB USB device to facilitate data migration from the old system to the new installation. For Cisco Unity Connection and Cisco Business Edition 5000, a 128GB external USB device is required.

Step 2 Put the upgrade file on an FTP or SFTP server that the server that you are upgrading can access.

Step 3 Log in to Cisco Unified Communications Operating System Administration.

Step 4 Navigate to **Software Upgrades** > **Install/Upgrade**.
The Software Installation/Upgrade window displays.

Step 5 From the **Source** list, choose **Remote Filesystem**.

Step 6 In the **Directory** field, enter the path to the directory that contains the patch file on the remote system.
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. 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, remember that you are connecting to an FTP or SFTP server, so use the appropriate syntax, including

a) Begin the path with a forward slash (/) and use forward slashes throughout the path.

b) The path must start from the FTP or SFTP root directory on the server, so you cannot enter a Windows absolute path, which starts with a drive letter (for example, C:).

Step 7 In the **Server** field, enter the server name or IP address.

Step 8 In the **User Name** field, enter your user name on the remote server.

Step 9 In the **User Password** field, enter your password on the remote server.

Step 10 Select the transfer protocol from the **Transfer Protocol** field.

Step 11 To use the Email Notification feature, enter your Email Destination and SMTP Server in the fields provided.

Step 12 To continue the upgrade process, click **Next**.

Step 13 Choose the upgrade version that you want to install and click **Next**.

Step 14 In the next window, monitor the progress of the download.

Note If you lose your connection with the server or close your browser during the upgrade process, you may see the following message when you try to access the Software Upgrades menu again:

Note Warning: Another session is installing software, click Assume Control to take over the installation.

Note If you are sure you want to take over the session, click **Assume Control**.

Note If Assume Control does not display, you can also monitor the upgrade with the Real Time Monitoring Tool.

Step 15 If you want to install the upgrade and automatically reboot to the upgraded partition, choose **Switch to new version after upgrade**. The system restarts and runs the upgraded software.

Step 16 If you want to install the upgrade and then manually reboot to the upgraded partition at a later time, complete the following steps:

a) Choose **Do not switch to new version after upgrade**.

b) Click **Next**.
The Upgrade Status window displays the Upgrade log.

c) When the installation completes, click **Finish**.

d) To restart the system and activate the upgrade, choose **Settings** > **Version**; then, click **Switch Version**.
The system restarts and is running the upgraded software.

Bridge upgrade

The bridge upgrade provides a migration path for customers who want to migrate from discontinued Cisco Unified Communications Manager server to a node that supports the newest release of Cisco Unified Communications Manager.

Servers that are no longer supported, but are permitted to function as bridge upgrade nodes, can upgrade and boot but will not allow Cisco Unified Communications Manager to function.

When you attempt to upgrade your Cisco Unified Communications Manager version on a discontinued server model, Cisco Unified Communications Manager inserts a message into the upgrade log. The upgrade log is displayed on the web browser when the upgrade is initiated through the Cisco Unified Communications Operating System Administration window, or you can view it through CLI if you used CLI to perform the upgrade. This message notes that you can only use the new version to obtain a DRS backup. The warning message in the log is followed by a delay that allows you to cancel the upgrade if you do not want to do a bridge upgrade.

When the system boots the new Cisco Unified Communications Manager version, a warning appears on the console that tells you that the only thing you can do with the new Cisco Unified Communications Manager version is to perform a DRS backup ("This hardware has limited functionality. Backup and Restore is the only supported functionality."). Because of the restricted visibility of the console, the warning displays during both CLI and GUI sessions.

Note During a bridge upgrade, if the only upgrade is to the publisher (rather than to all nodes in the cluster) all subscribers must be offline.

Use the following procedure to perform a bridge upgrade:

Procedure

Step 1 Perform an upgrade to the new Cisco Unified Communications Manager version on your discontinued first node (publisher node). Refer to the preceding sections in this chapter that describe the kind of upgrade you want to do. Observe the warning on the console that tells you that the only thing you can do with the new Cisco Unified Communications Manager version is to perform a DRS backup ("This hardware has limited functionality. Backup and Restore is the only supported functionality.").

Step 2 Perform an upgrade to the new Cisco Unified Communications Manager version on your subsequent node (subscriber nodes). Refer to the preceding sections in this chapter that describe the kind of upgrade you want to do.

Step 3 Verify database synchronization between all nodes. You can use the CLI commands utils dbreplication runtime state and utils dbreplication status. For more information, refer to the Command Line Interface Reference Guide for Cisco Unified Communications Solutions.

Step 4 Using the new Cisco Unified Communications Manager version on your discontinued first node server, perform a DRS backup. The DRS backups are encrypted using the cluster security password provided at install time. You must remember this security password as the "old" password, because you may be prompted to enter this "old" password at the time of restore. Refer to the Disaster Recovery System Administration Guide.

Step 5 Disconnect your discontinued server from the network.

Step 6 Install the new Cisco Unified Communications Manager version on your new supported first node. You must obtain and install a new license on this node. Refer to the guide Installing Cisco Unified Communications Manager. You will be prompted to enter a "new" security password, a password that is different from the "old" password you noted in the previous step. The guide Installing Cisco Unified Communications Manager describes the requirements of a "new" security password that Cisco Unified Communications Manager will accept. You must remember this "new" security password.

Step 7 Using the new Cisco Unified Communications Manager version on your new supported first node, perform the Disaster Recovery System Administration Guide procedure "Restoring the First Node only (Rebuilding the Publisher Alone)". First, select only select the first node for restore. You can only select the subsequent nodes for restore after the completion of first node restore. Use the discontinued server's backup file that you created previously. You will be prompted for the "old" security password that you noted previously. For further details, refer to the *Disaster Recovery System Administration Guide*.

Step 8 On your new supported first node, reactivate all services that used to be active on your discontinued first node server before the bridge upgrade. Refer to the *Administration Guide for Cisco Unity Connection Serviceability*.

Step 9 Verify database synchronization between all nodes. You can use the CLI commands **utils dbreplication runtime state** and **utils dbreplication status**. For more information, refer to the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*.

Post-upgrade tasks

After the upgrade, perform the following tasks:

- 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.

- 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.

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

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 Communications Manager 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.

Revert 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.

Caution If you are upgrading your software on HP7825H3 or HP7828H3 hardware, there is no option to revert to the previous version of Cisco Unified Communications Manager. To perform an upgrade on one of these machines you must use a 16GB USB device to facilitate data migration from the old system to the new installation. For Cisco Unity Connection and Cisco Business Edition 5000, a 128GB external USB device is required.

Revert cluster to previous version

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*.

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

Procedure

Step 1 Revert the publisher node.

Step 2 Revert all backup subscriber nodes.

Step 3 Revert all primary subscriber nodes.

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

Related Topics

Revert node to previous version, on page 70
Reset database replication, on page 70

Revert node to previous version

Procedure

Step 1 Open Cisco Unified Communications Operating System Administration directly by entering the following URL:
https://node-name/**cmplatform**

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

Step 2 Enter your Administrator user name and password.

Step 3 Choose **Settings** > **Version**.
The Version Settings window displays.

Step 4 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 5 To verify that the version switch was successful, follow these steps:

a) Log in to Cisco Unified Communications Operating System Administration again.
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 Communications Manager Administration.
f) Verify that you can log in and that your configuration data exists.

Reset database replication

If you revert 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.

COP files, dial plans, and locales

This section contains information about COP files, dial plans, and locales.

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.

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 Communications Manager Administration and then navigate to **Call Routing** > **Dial Plan Installer** to complete installing the dial plans.

Locale installation

Cisco provides locale-specific versions of the Cisco Unified Communications Manager 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.

Tip Since the primary language spoken in Belgium is Dutch, you can download the Dutch (Netherlands) locale file, for example, cm-locale-nl_NL- 8.5.1.2100-1.cop.sgn (Cisco Unified Communications Locale Installer 8.5.1.21000-1 Dutch (Netherlands)). Secondary languages commonly spoken in Belgium are French and German.

User Locales

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 chooses. User-only locale installers exist on the web.

Network Locales

Network locale files provide country-specific phone tones and gateway tones, if available. Network-only locale installers exist on the web.

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

Note The Cisco Media Convergence Server (MCS) or Cisco-approved, customer-provided server 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.

Locale installation considerations

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 nodes, 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. To activate the new locale, you must restart each node in the cluster after installation.

You can install locale 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 a remote source.

Locale files

When you install locales on a node, install the following files:

- User Locale files - These files contain language information for a specific language and country and use the following convention:

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

- Combined Network Locale file - Contains country-specific files for all countries 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)

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 14: 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.
[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.

Message	Description
[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`

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 Communications Manager 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.

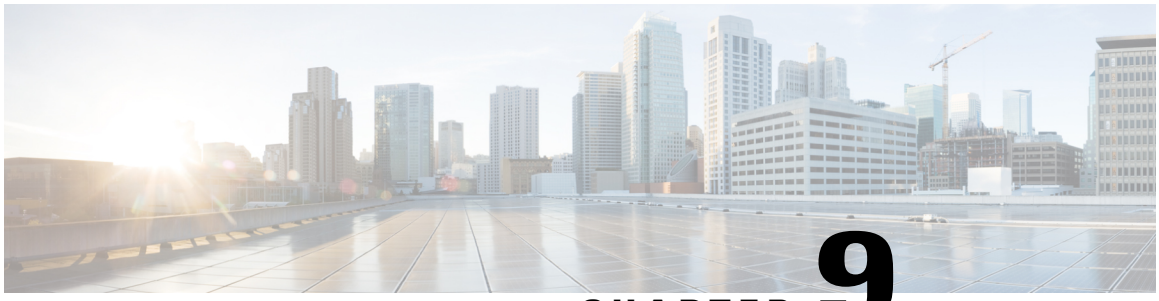
The system displays the customized log-on message.

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.

PART II

IM and Presence service OS platform

- Getting started, page 79
- Settings, page 83
- Shutdown and restart, page 87
- Security, page 91
- Security certificate management , page 97
- Single Sign-On, page 107
- Software Upgrades, page 109
- Utilities, page 113



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 79
- Recover Administrator password, page 80
- Create customized log-on message, page 81

Sign in to Cisco Unified IM and Presence Operating System Administration

Before You Begin

If you are currently signed in to Cisco Unified CM 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 Unified CM 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.

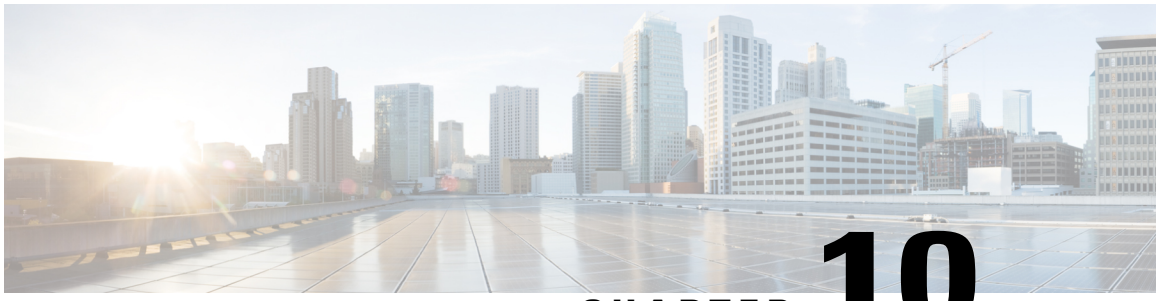
Step 2 Select **Software Upgrades** > **Customized Logon Message**.

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 Select **Upload File**.

Step 5 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 83
- NTP settings, page 85
- Change SMTP settings, page 86
- Change time settings, page 86
- Correct time zone data, page 86

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.

Table 15: Ethernet Settings Fields and Descriptions

Field	Description
DHCP	Indicates whether DHCP is Enabled or Disabled.
Hostname	Shows the name of the host server. **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 publisher server 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 IP publisher node address on subsequent nodes

If, for network configuration purposes, you changed the IP address or hostname on the IM and Presence publisher node, then you will need to update the IP address of the publisher node on subsequent nodes in IM and Presence.

Before You Begin

Use this functionality only if you want a subsequent node in IM and Presence to point to a different IM and Presence publisher node. If this node **is** the IM and Presence 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 Publisher IP address.

Step 4 (Optional) Following a fresh installation of IM and Presence, you can change the IP address of the Cisco Unified Communications Manager publisher server. Select **System** > **CUCM Publisher** in Cisco Unified CM IM and Presence Administration.

Related Topics

Change Ethernet settings, on page 83
Troubleshoot IP publisher node address change on subsequent node, on page 85

Troubleshoot IP publisher node address change on subsequent node

Before You Begin

If the IP address of the IM and Presence publisher node changes while a subsequent node is offline, be aware that you may not be able to sign in to Cisco Unified CM IM and Presence Administration on the subsequent 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://server-name/cmplatform` where `server-name` specifies the hostname or IP address of the subsequent 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 publisher server and select **Save**.

Step 5 Restart the subsequent node.

Related Topics

Change IP publisher node address on subsequent nodes, on page 84

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 server time if NTP is currently disabled.

Before You Begin

Before you can manually configure the server 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**.

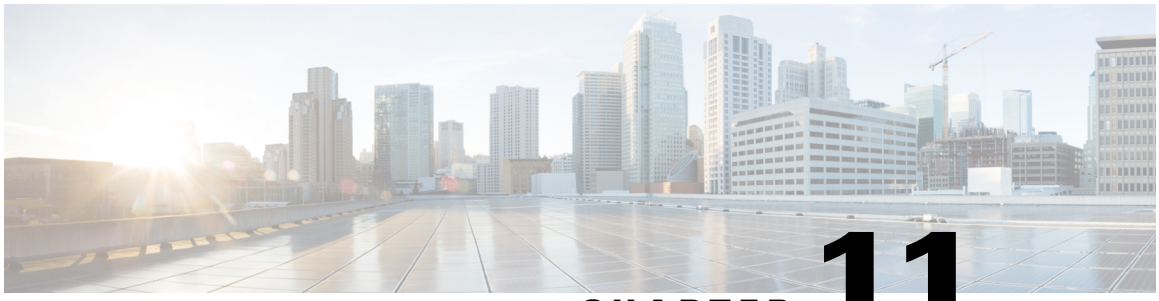
Step 3 Enter the date and time for the system.

Related Topics

Troubleshoot IP publisher node address change on subsequent node, on page 85
Correct time zone data, on page 86

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 server.
- 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 server, press the **power** button. Note, however, that this action may lead to file system corruption and is not recommended.

- Shut down system, page 87
- Work with disk partitions, page 88

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 88

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 109

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**.

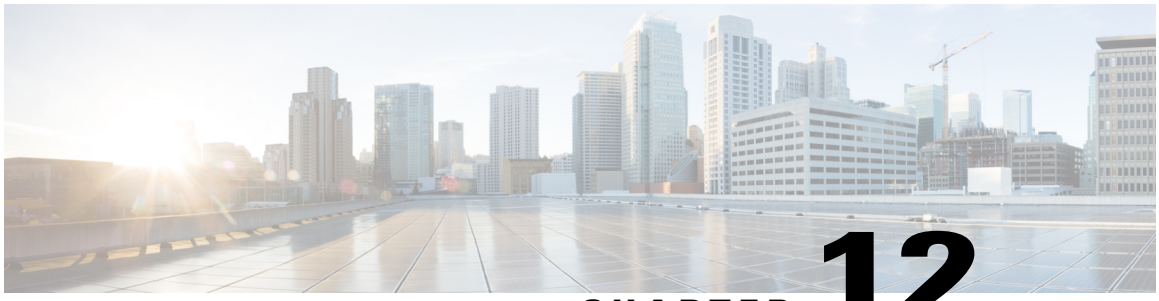
Step 3 Perform one of the following actions:

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 87



CHAPTER 12

Security

- Browser security, page 91
- IPsec policy management, page 92

Browser security

Verify Internet Explorer security settings

To download certificates from the server, 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 Unified CM 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
- Cisco Unified CM IM and Presence User Options

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 server 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

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 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 94

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 server 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 92

Delete IPsec policy

You can delete one or more IPsec policies. Do not, however, attempt to delete IPsec policies during an IM and Presence server 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.

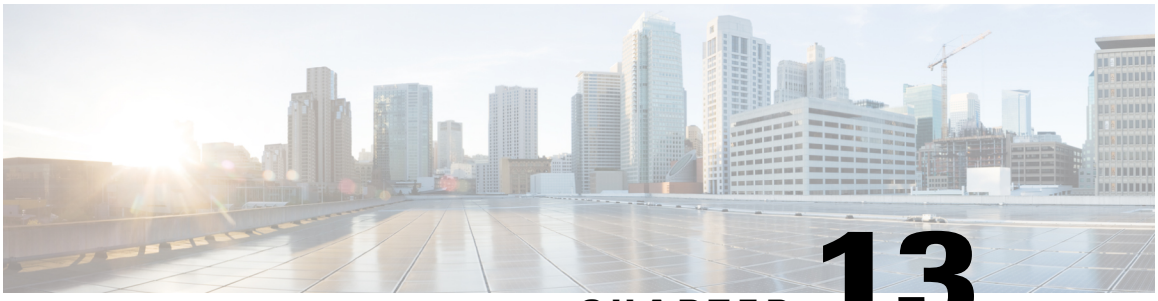
Procedure

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 server.

- Certificates and certificate trust list management, page 97
- Third Party CA certificates, page 102

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 • 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 103

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 16: Certificate Names and Descriptions

Name	Description
tomcat	This self-signed root certificate is generated during the installation of the HTTPS server.
ipsec	This self-signed root certificate is generated during the installation of secure IPsec server connections.
cup	This self-signed root certificate is generated during the installation of the IM and Presence server.
cup-xmpp	This self-signed root certificate is generated during the installation of the IM and Presence server.
cup-xmpp-s2s	This self-signed root certificate is generated during the installation of the IM and Presence server. **Note** The trust certificates for cup-xmpp-s2s are stored in cup-xmpp-trust along with the general XMPP trust certificates.

Step 5 Select **Generate New**.

Step 6 Restart the Tomcat web server after you upload or regenerate a Tomcat certificate in an IM and Presence cluster.

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 distribute trust certificates to other cluster nodes automatically. If you need to have the same certificate on more than one node, you must upload the certificate to each node individually.

- 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** list.
Step 5 Select the file to upload by completing one or of 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 server.
Step 7 Restart the services that are affected by the new certificate.

Upload directory trust certificate

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 **directory-trust** from the **Certificate Name** list.
Step 5 Enter the file to upload in the **Upload File** field.
Step 6 Select **Upload File**.
Step 7 Sign into Cisco Unified IM and Presence Serviceability.
Step 8 Select **Tools** > **Control Center - Feature Services**.
Step 9 Restart the service **Cisco Dirsync**.
Step 10 Sign in to the Cisco Unified IM and Presence Operating System Administration CLI as an administrator.
Step 11 Enter the command `utils service restart Cisco Tomcat` to restart the Tomcat service.
Step 12 After the services have been restarted, you can add the directory agreement for SSL.

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.

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.

CAPF and IM and Presence 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 final window of the CSR generation process.

Cisco Unified Operating System generates certificates in DER and PEM encoding formats and generates CSRs in PEM encoding format. It accepts certificates in DER and DER encoding formats.

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.

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 server.	See Generate certificate signing request, on page 103.
Step 2	Download the CSR to your PC.	See Download certificate signing request, on page 104.
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 server.	See Upload certificate or certificate trust list, on page 100.
Step 6	Upload the application certificate to the server.	See Upload certificate or certificate trust list, on page 100.
Step 7	If you updated the certificate for CAPF or IM and Presence, generate a new CTL file.	See Upload certificate or certificate trust list, on page 100.
Step 8	Restart the services that are affected by the new certificate.	For all certificate types, restart the corresponding service (for example, restart the Tomcat service if you updated the Tomcat certificate). For information about restarting services, see the *Cisco Unified Serviceability Administration Guide*.

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, on page 101

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**.

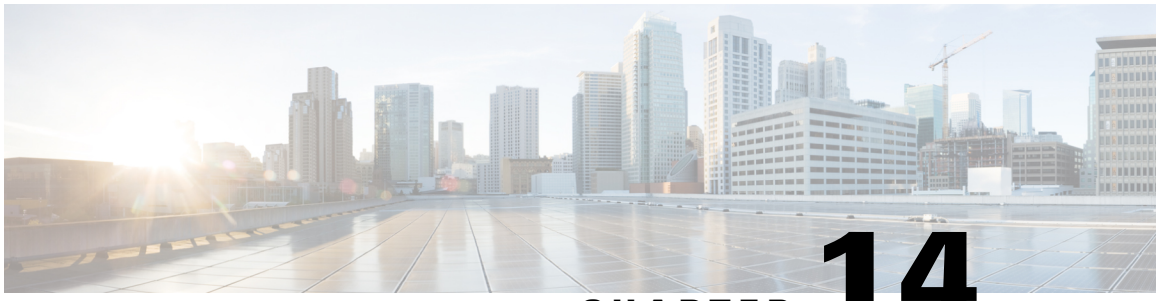
Monitor certificate expiration dates

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.



CHAPTER 14

Single Sign-On

- Introduction, page 107
- Set up Single Sign-On, page 107

Introduction

The Single Sign-On (SSO) feature allows end users to log in to Windows, then use the following IM and Presence applications without having to sign on again:

- Cisco Unified CM IM and Presence User Options
- 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

Set up Single Sign-On

To configure Single Sign-On (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 server 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 Unified CM IM and Presence Administration - Enables SSO for Cisco Unified CM IM and Presence Administration, Cisco Unified IM and Presence Serviceability, and Cisco Unified IM and Presence Reporting
- Cisco Unified CM IM and Presence User Options - Enables SSO for End User Options
- 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

Procedure

Step 1 Enter the following URL of the Open Access Manager (OpenAM) server:
`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.

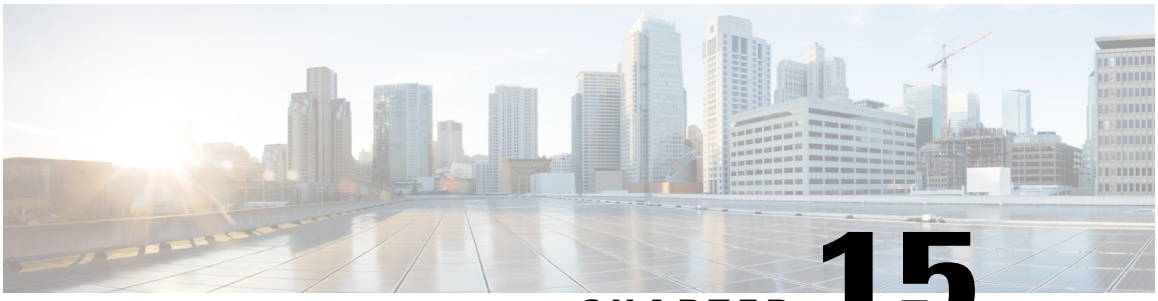
Step 5 Enter the login module instance name that is configured for Windows Desktop SSO.

Step 6 Click **Save.**

Step 7 In the **Confirmation** dialog box, click **OK** to restart Tomcat.

What to Do Next

Enable the SSO feature on the IM and Presence server by entering the `utils sso enable` command on the Command Line Interface. For more information, see the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.



CHAPTER 15

Software Upgrades

- Software upgrades, page 109
- Locale-specific upgrades , page 109

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 server in the cluster after installation to activate the new locales. For more information about installing locales, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.

Error messages

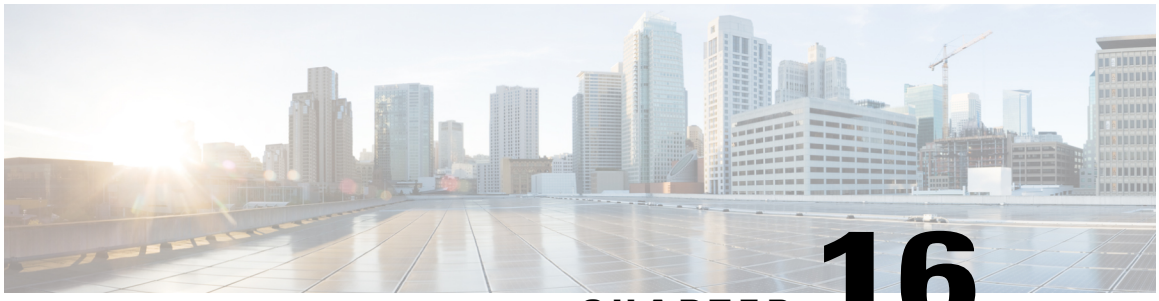
See the following table for a description of the messages that can occur during Locale Installer activation. If an error occurs, you can view the messages in the installation log.

Table 17: 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 server does not have a Cisco Unified Communications application, such as Cisco Unified Communications Manager or IM and Presence, 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 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] DRS registration failed	The locale installer could not register with 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] 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.
[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 server, page 113
- Set up a remote account, page 114

Ping another server

You can ping another server 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 Enter the ping count, that is, 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 18: 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.

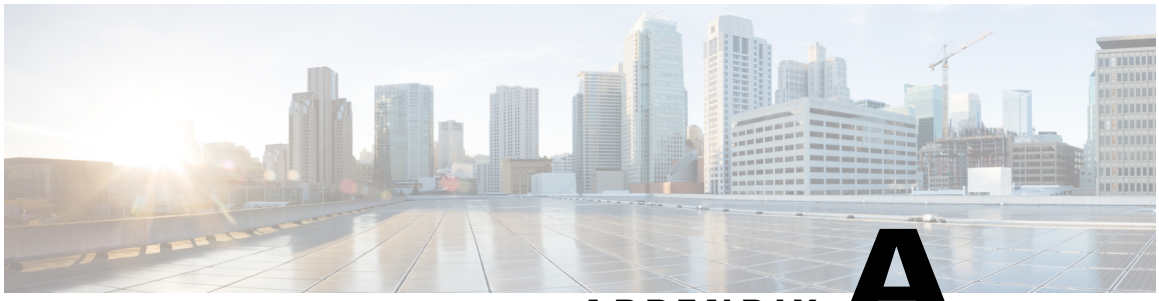
Step 5 Select **Save**.

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 117
- View hardware status, page 118
- View network status, page 118
- View installed software, page 120
- View system status, page 120
- View IP preferences, page 121

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 19: Cluster Nodes Field Descriptions

Field	Description
Hostname	The complete hostname of the server.
IP Address	The IP address of the server.
Alias	The alias name of the server, when defined.
Type of Node	Indicates whether the server is a publisher node or a 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 20: Hardware Status Field Descriptions

Field	Description
Platform Type	The model identity of the platform server.
Serial Number	The serial number of the platform server.
Processor Speed	Processor speed (measured in MHz) in the platform server.
CPU Type	The type of processor in the platform server.
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 21: 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.
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 server.
Secondary DNS	The IP address of the secondary domain name server.
Domain	The domain of the server.
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 22: 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 23: Platform Status Field Descriptions

Field	Description
Host Name	The name of the Cisco MCS host where Cisco Unified Operating System is installed.
Date/Time	The date and time based on the continent and region that were specified during operating system installation.

Field	Description
Time Zone	The time zone that was chosen during installation.
Locale	The language that was chosen during operating system installation.
Product Version	The operating system version.
Platform Version	The platform version.

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 24: 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.

Field	Description
Status	Indicates whether the application is enabled or disabled.
Description	The description of the application.

INDEX

A

administrator password 8, 80

B

browser requirements 4

C

Certificate Trust List, See CTL
certificates 30, 31, 32, 34, 37, 38, 97, 98, 99, 100, 104
  deleting 31
  displaying 30, 97
  downloading 30, 98
  downloading a signing request 37, 104
  expiration monitor fields 38
  expiration monitor fields (table) 104
  managing 97
  monitoring expiration dates 38, 104
  regenerating 31, 32, 99
  uploading 34, 100
CLI 6
cluster nodes 11, 117
  fields 11
  fields (table) 117
  procedure 11, 117
Command Line Interface 6
  See also CLI
configuration 4, 11, 117
  operating system 4, 11, 117
CTL 30, 97, 98, 100
  downloading 30, 98
  managing 97
  uploading 100

D

dial plan installation 71

E

error messages 72, 110
  descriptions 72
  descriptions (table) 110
Ethernet settings 19

H

hardware 12, 118
  fields 12
  fields (table) 118
  procedure 12, 118
  status 12, 118

I

install/upgrade 5, 109
  menu 5, 109
installed software 14, 120
  fields (table) 14, 120
  procedure 14, 120
installing 71, 109, 110
  dial plan 71
  locales 71, 109, 110
Internet Explorer 29, 91
  set security options 29, 91
IPSec 40, 45, 92, 94
  changing policy 45, 94
  displaying policy 45, 94
  management 40, 92
  policy fields 40
  policy fields (table) 92
  setting up new policy 40, 92

L

locales 71, 72, 109, 110
files 72, 109
installation 71, 109
installer 72, 110
error messages 72
error messages (table) 110
installing 110
logging in 7, 79
overview 7, 79
procedure 7, 79

M

menu 4, 5, 109
install/upgrade 5, 109
security 5
settings 4
show 4
messages 72, 110
error 72, 110

N

network status 12, 118
fields (table) 12, 118
procedure 118
nodes 11, 117
cluster 11, 117
fields 11
fields (table) 117
procedure 11, 117
NTP server settings 22

O

operating system 3, 4, 5, 6, 7, 8, 11, 12, 19, 26, 79, 80, 83, 88, 109, 117, 118
administrator password 8, 80
browser requirements 4
configuration 4, 11, 117
hardware status 12, 118
fields 12
fields (table) 118
procedure 12, 118
introduction 3
logging in 7, 79
network status fields (table) 12, 118
overview 3
operating system *(continued)*
restart 26, 88
security 5
services 6
settings 4, 19, 83
software upgrades 5, 109
status 4, 11, 117

P

password 8, 80
recovering 8, 80
ping 51, 113
publisher settings 21, 84

R

remote support 52, 114
setting up 52, 114
status fields 52
status fields (table) 114
restart 25, 26, 87, 88
current version 26, 88
system 25, 87

S

security 5, 29, 91, 97
configuration 5
menu 5
overview 29, 91, 97
set IE options 29, 91
services 6, 51, 52, 113, 114
overview 51, 113
ping 6, 51, 113
remote support 6, 52, 114
overview 52, 114
setting up 52, 114
settings 4, 19, 21, 22, 23, 83, 84, 85, 86
Ethernet 19, 83
fields 19
fields (table) 83
procedure 19
IP 19
menu 4
NTP servers 22
overview 19, 83
publisher 21, 84
SMTP 23, 85, 86
time 23, 86

show 4
menu 4
shutdown 26, 87
operating system 26, 87
SMTP settings 23, 85, 86
software 5, 14, 55, 63, 64, 65, 66, 109, 120
installed 14, 120
fields (table) 14, 120
procedure 14, 120
upgrades 5, 55, 63, 64, 65, 66, 109
bridge upgrade 66
from local source 63
from remote source 64, 65
overview 55, 109
status 4, 11, 12, 15, 117, 118, 120, 121
hardware 12, 118
fields 12
fields (table) 118
procedure 12, 118
network 12, 118
fields (table) 12, 118
procedure 118
operating system 4, 11, 117
system 15, 120, 121
fields 15
status *(continued)*
system *(continued)*
fields (table) 120, 121
procedure 15, 120, 121
supported products 74
system 15, 25, 26, 87, 120, 121
restart 25, 87
shutdown 26, 87
status 15, 120, 121
fields 15
fields (table) 120, 121
procedure 15, 120, 121

T

TFTP server 74
installing files 74
time settings 23, 86

V

version 26, 88
restart 26, 88