Cisco Unified Communications Operating System Administration Guide

Release 8.6(1)

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-24967-01

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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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

Cisco Unified Communications Operating System Administration Guide
© 2011 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface 5

Purpose 5

Audience 5

Organization 5

Related Documentation 6

Conventions 6

Obtaining Documentation, Obtaining Support, and Security Guidelines 7

Cisco Product Security Overview 7

CHAPTER 1 **Introduction** 1-1

Overview 1-1

Browser Requirements 1-1

Operating System Status and Configuration 1-2

Settings 1-2

Security Configuration 1-3

Software Upgrades 1-3

Services 1-3

Command Line Interface 1-4

CHAPTER 2 **Log in to Cisco Unified Communications Operating System Administration** 2-1

Logging in to Cisco Unified Communications Operating System Administration 2-1

Resetting Administrator and Security Passwords 2-2

CHAPTER 3 **Status and Configuration** 3-1

Cluster Nodes 3-1

Hardware Status 3-2

Network Configuration 3-2

Installed Software 3-3

System Status 3-4

IP Preferences 3-5

CHAPTER 4 **Settings** 4-1

IP Settings 4-1

Ethernet Settings 4-1

Ethernet IPv6 Configuration Settings 4-2

Publisher Settings 4-6

Changing IP Address on a Subsequent Cisco Unified Communications Manager Node 4-6

NTP Servers 4-7

SMTP Settings 4-8

Time Settings 4-9

CHAPTER 5 **System Restart** 5-1

Switch Versions and Restart 5-1

Restart Current Version 5-2

Shut Down the System 5-2

CHAPTER 6 **Security** 6-1

Set Internet Explorer Security Options 6-1

Manage Certificates 6-1

Display Certificates 6-2

Download a Certificate 6-2

Delete and Regenerate a Certificate 6-2

Deleting a Trust Certificate 6-3

Regenerating a Certificate 6-3

Upload a Certificate or Certificate Chain 6-5

Uploading a Certificate or Certificate Chain 6-5

Using Third-Party CA Certificates 6-6

Uploading Third-Party Signed Certificate or Certificate Chain 6-6

Generating a Certificate Signing Request 6-7

Downloading a Certificate Signing Request 6-7

Obtaining Third-Party CA Certificates 6-8

Monitor Certificate Expiration Dates 6-8

Certificate Revocation 6-9

Configure Online Certificate Status Protocol 6-9

IPsec Management 6-10

Set Up a New IPsec Policy 6-10

Migration characteristics 6-14

Manage Existing IPsec Policies 6-14

Bulk Certificate Management 6-15

Exporting Certificates 6-16
Importing Certificates 6-16

CHAPTER 7 **Software Upgrades 7-1**
Pre-Upgrade Tasks 7-2
Software Upgrade Considerations 7-3
Overview of the Software Upgrade Process 7-4
Making Configuration Changes During an Upgrade 7-5
Administration Changes 7-5
User Provisioning 7-7
Upgrading a Cluster in Parallel 7-7
Supported Upgrades 7-8
Partition Size Limitations When You Upgrade from a 5.x Release to a 7.x Release 7-8
Obtaining the Upgrade File 7-9
Software Upgrade Procedures 7-10
Upgrading from a Local Source 7-10
Upgrading Software or Installing Locales from a Local Source 7-10
Upgrading from a Remote Source 7-12
Maintaining Correct Time Zone Data 7-12
Supported SFTP Servers 7-12
Upgrading Software or Installing Locales from a Remote Source 7-13
Bridge Upgrade 7-15
Post-Upgrade Tasks 7-16
Reverting to a Previous Version 7-17
Reverting a Cluster to a Previous Version 7-17
Reverting the Publisher or Subscriber Nodes to a Previous Version 7-18
Resetting Database Replication When Reverting to an Older Product Release 7-19
Installing COP Files, Dial Plans, and Locales 7-19
COP File Installation 7-19
Dial Plan Installation 7-19
Locale Installation 7-19
Installing Locales 7-20
Cisco Unified Communications Manager Locale Files 7-20
Error Messages 7-21
Supported Cisco Unified Communications Products 7-22
Managing TFTP Server Files 7-22
Setting Up a Customized Log-on Message 7-23

CHAPTER 8 **Services** 8-1

Ping 8-1

Remote Support 8-2

INDEX

Preface

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
Introduction	This chapter provides an overview of the functions that are available through the Cisco Unified Communications Operating System.
Log in to Cisco Unified Communications Operating System Administration	This chapter provides procedures for logging in to the Cisco Unified Communications Operating System and for recovering a lost Administrator password.
Status and Configuration	This chapter provides procedures for displaying operating system status and configuration settings.
Settings	This chapter provides procedures for viewing and changing the Ethernet settings, IP settings, and NTP settings.
System Restart	This chapter provides procedures for restarting and shutting down the system.

Chapter	Description
Security	This chapter provides procedures for certificate management and for IPSec management.
Software Upgrades	This chapter provides procedures for installing software upgrades and for uploading files to the TFTP server.
Services	This chapter provides procedures for using the utilities that the operating system provides, including ping and remote support.

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.
	This pointer highlights an important line of text in an example.
^	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.
< >	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.**

Obtaining Documentation, Obtaining Support, and Security Guidelines

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

Cisco Product 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

CHAPTER 1

Introduction

For Cisco Unified Communications Manager, you can perform many common system administration functions through the Cisco Unified Communications Operating System.

This chapter comprises the following sections:

- Overview
- Browser Requirements
- Operating System Status and Configuration
- Security Configuration
- Software Upgrades
- Services
- Command Line Interface

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 server 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 server (**https://***servername*) is included in the browser "Trusted Site Zone" or the "Local Intranet Site Zone" for all product features to work correctly.

Operating System Status and Configuration

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

For more information, see Chapter 3, "Status and Configuration."

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.

For more information, see Chapter 4, "Settings."

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 server.

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

For more information see Chapter 5, "System Restart."

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

For more information, see Chapter 6, "Security."

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.

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.

For more information, see Chapter 7, "Software Upgrades."

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.

For more information, see Chapter 8, "Services."

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

Log in to Cisco Unified Communications 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.

This chapter comprises the following sections:

- Logging in to Cisco Unified Communications Operating System Administration, page 2-1
- Resetting Administrator and Security Passwords, page 2-2

Logging in to Cisco Unified Communications Operating System Administration

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://*server-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.

Resetting Administrator and Security 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 server in a cluster after you change its security password. Failure to reboot the servers (nodes) causes system service problems and problems with the Cisco Unified Communications Manager Administration windows on the subscriber servers.

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:

- Username: **pwrecovery**
- 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:

- Enter **a** to reset the administrator password.
- Enter **s** to reset the security password.
- 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 and contains the following topics:

- Cluster Nodes
- Hardware Status
- Network Configuration
- Installed Software
- System Status
- IP Preferences

Cluster Nodes

To view information on 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 displays.

Step 2 For a description of the fields on the Cluster Nodes window, see Table 3-1.

Table 3-1 Cluster Nodes Field Descriptions

Field	Description
Hostname	Displays the complete hostname of the server.
IP Address	Displays the IP address of the server.
Alias	Displays the alias name of the server, when defined.
Type of Node	Indicates whether the server is a publisher node or a subscriber node.

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 Table 3-2.

Table 3-2 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.

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 Table 3-3 for descriptions of the fields on the Network Settings window.

Table 3-3 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.
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.

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 Table 3-4.

Table 3-4 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.

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 Table 3-5 for descriptions of the fields on the Platform Status window.

Table 3-5 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.

Table 3-5 System Status Field Descriptions (continued)

Field	Description
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.

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; go to Step 3.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- 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

Table 3-6 IP Preferences Field Descriptions

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

CHAPTER 4

Settings

Use the Settings options to display and change IP settings, host settings, and Network Time Protocol (NTP) settings.

This chapter contains the following sections:

- IP Settings, page 4-1
- NTP Servers, page 4-7
- SMTP Settings, page 4-8
- Time Settings, page 4-9

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.

This section contains the following topics:

- Ethernet Settings, page 4-1
- Ethernet IPv6 Configuration Settings, page 4-2
- Publisher Settings, page 4-6
- Changing IP Address on a Subsequent Cisco Unified Communications Manager Node, page 4-6

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 Table 4-1.

Note If you enable DHCP, the Port and Gateway settings get disabled and cannot be changed.

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

Caution Changing IP address or host of a server 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.

Procedure

Table 4-1 Ethernet Configuration Fields and Descriptions

Field	Description
DHCP	Indicates whether DHCP is Enabled or Disabled.
Hostname	Displays the host name of the server. **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.

Ethernet IPv6 Configuration Settings

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

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 Table 4-2.

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.

Table 4-2 Ethernet IPv6 Configuration Fields and Descriptions

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

Publisher Settings

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 servers in a cluster, 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.

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**.

Changing IP Address on a Subsequent Cisco Unified Communications Manager Node

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://*server-name*/iptplatform

where *server-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.

NTP Servers

Ensure that external NTP servers are stratum 9 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 should be NTP v4 (version 4). If you are usingIPv6 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.

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

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**.

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. See the "NTP Servers" section on page 4-7 for more information.

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.

CHAPTER 5

System Restart

This section provides procedures for using the following restart options:

- Switch Versions and Restart
- Restart Current Version
- Shut Down the System

Switch Versions and Restart

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 (releases 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 will have to manually delete the ITL file on each Cisco Unified IP Phone in the system. For more information, see Chapter 2, "Security by Default," in 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 Version**, 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 the 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 1

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 shut down the system, click **Shutdown** or, to stop the operation, click **Cancel**.

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

Note The hardware may require several minutes to power down.

Procedure 2 (Alternative to Procedure 1)

Step 1 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 describes certificate management and IPsec management and provides procedures for performing the following tasks:

- Set Internet Explorer Security Options
- Manage Certificates
- IPsec Management
- Bulk Certificate Management

Set Internet Explorer Security Options

To download certificates from the server, 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:

- Display Certificates
- Download a Certificate
- Delete and Regenerate a Certificate

- Upload a Certificate or Certificate Chain

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

Display 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 a 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**.

Delete and Regenerate a Certificate

These sections describe how to delete and regenerate a certificate:

- Deleting a Trust Certificate

- Regenerating a Certificate

Deleting a 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 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 **Delete**.

For more information about deleting a certificate, see the caution.

Step 5 Click **OK.**

Regenerating a Certificate

To regenerate a certificate, follow this procedure:

Note For more information about regenerating certificates, see Chapter 3, "Security by Default," in the *Cisco Unified Communications Manager Security Guide*.

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

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 Choose a certificate name from the Certificate Name list. For details about certificate names, see Table 6-1.

Step 4 Click **Generate New**.

Note You must 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 you regenerate the Tomcat certificate). In addition, if you updated the certificate for Cisco Certificate Authority Proxy Function(CAPF) or Cisco Unified Communications Manager, restart the CAPF and the Cisco CallManager service. Rerun CTL client (if configured) after you regenerate the CAPF or CallManager certificates. After you regenerate the IPsec certificate, you must restart Cisco Disaster Recovery System (DRS) Local and Cisco DRF Master services.

Note After you regenerate certificates in the Cisco Unified Communications Operating System, you must perform a backup so that the latest backup contains the regenerated certificates. If your backup does not contain the regenerated certificates and you must perform restoration tasks for any reason, 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, refer to the *Disaster Recovery System Administration Guide*.

Table 6-1 Certificate Names and Descriptions

Name	Description
tomcat	This self-signed root certificate is generated during installation for the HTTPS server.
ipsec	This self-signed root certificate is generated during installation for IPsec connections with MGCP and H.323 gateways.
CallManager	This self-signed root certificate is installed automatically when you install Cisco Unified Communications Manager. This certificate provides server identification, including the server name and the Global Unique Identifier (GUID).
CAPF	The system copies this root certificate to your server or to all servers in the cluster after you complete the Cisco client configuration.
TVS	This is a self-signed root certificate.

Upload a Certificate or Certificate Chain

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*.

These sections describe how to upload a Certificate Authority (CA) root certificate and application certificate to the server:

- Uploading a Certificate or Certificate Chain
- Using Third-Party CA Certificates

Uploading a Certificate or Certificate Chain

Note You can upload the certificate or certificate chain to Certificate Trust or for a third-party signed certificate. For more information, see Using Third-Party CA Certificates.

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:

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

Using Third-Party CA Certificates

Cisco Unified Communications Operating System supports certificates that a third-party CA issues with PKCS#10 Certificate Signing Request (CSR). The following table provides an overview of this process, with references to additional documentation:

	Task	For More Information
Step 1	Generate a CSR on the server.	See the "Generating a Certificate Signing Request" section on page 6-7.
Step 2	Download the CSR to your PC.	See the "Downloading a Certificate Signing Request" section on page 6-7.

	Task	For More Information
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 application certificates from your CA. See "Obtaining Third-Party CA Certificates" section on page 6-8 for additional notes.
Step 4	Obtain the CA certificate or certificate chain.	Get information about obtaining a root certificate from your CA. See "Obtaining Third-Party CA Certificates" section on page 6-8 for additional notes.
Step 5	Upload third-party certificate.	See "Uploading Third-Party Signed Certificate or Certificate Chain" section on page 6-6
Step 6	If you updated the certificate for CAPF or Cisco Unified Communications Manager, generate a new CTL (Certificate Trust List) file.	See the Chapter 4, "Configuring the Cisco CTL Client" in 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.

Uploading 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.

Generating a 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 Select the certificate name from the Certificate Name list.

Step 4 Click **Generate CSR**.

Note Generating CSR overwrites any existing CSR.

Downloading a 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**.

Obtaining 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 Dates

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 Table 6-2 for a description of the Certificate Monitor Expiration fields.

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

Table 6-2 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.

Certificate Revocation

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

Configure Online Certificate Status Protocol

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.

IPsec Management

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

- Set Up a New IPsec Policy
- Manage Existing IPsec Policies

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

Set Up a New 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.

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 Table 6-3.

Step 4 To set up the new IPsec policy, click **Save**.

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

Table 6-3 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. 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.
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

Table 6-3 IPSEC Policy and Association Field Descriptions (continued)

Field	Description
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.
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.

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

Table 6-4 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.

Table 6-4 IPSEC Policy and Association Field Descriptions (continued)

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

Table 6-4 IPSEC Policy and Association Field Descriptions (continued)

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.

Migration characteristics

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

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

Exporting 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. For a description of the fields on this window, see Table 6-5.

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
- All

Step 6 Click **Export**.

The system exports and stores the certificates you chose on the central SFTP server.

Importing 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.

Table 6-5 Bulk Certificate Management Field Descriptions

Field	Description
IP Address	Enter the IP address of the common server 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 server.

Table 6-5 Bulk Certificate Management Field Descriptions (continued)

Field	Description
Password	Enter the appropriate password.
Directory	Enter a directory on the server where you want to save the certificates. Example: /users/cisco

CHAPTER 7

Software Upgrades

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, 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.

This chapter contains the following sections:

- Pre-Upgrade Tasks, page 7-2
- Software Upgrade Considerations, page 7-3
- Software Upgrade Procedures, page 7-10
- Post-Upgrade Tasks, page 7-16
- Reverting to a Previous Version, page 7-17
- Installing COP Files, Dial Plans, and Locales, page 7-19
- Managing TFTP Server Files, page 7-22
- Setting Up a Customized Log-on Message, page 7-23

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*.

- 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 key available to migrate your data to the new system.

- 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.

Caution Failure to deactivate the Cisco Extension Mobility service could cause the upgrade to fail.

- 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.

Note If you have the Nokia s60 COP file installed, you must install any newer version of it before you upgrade 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 server) and subsequent nodes (subscriber servers). If IPv6 is configured incorrectly on the subsequent nodes, load detection may take 20 minutes.
- 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.
- After you complete the pre-upgrade tasks, review with the "Software Upgrade Considerations" section on page 7-3.

Software Upgrade Considerations

This section contains the following topics:

- Overview of the Software Upgrade Process, page 7-4
- Making Configuration Changes During an Upgrade, page 7-5
- Upgrading a Cluster in Parallel, page 7-7
- Supported Upgrades, page 7-8
- Obtaining the Upgrade File, page 7-9
- Supported SFTP Servers, page 7-12

Overview of the Software Upgrade Process

With this version of Cisco Unified Communications Manager, you cannot install upgrade software on your server 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 key to migrate the data from the old system to the new installation.

When you install 8.6 upgrade software, there will be a temporary server outage while the CUCM 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 server outage will begin. The duration of this outage will depend on your configuration and amount of data.

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 the upgrade is complete, you can choose to activate the partition with the new upgrade software or return to using the partition with the previous version of the software. 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, you start by upgrading the first node. You can begin upgrading subsequent nodes in parallel after the first node reaches a specified point in the upgrade, as described in the "Upgrading a Cluster in Parallel" section on page 7-7.

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

If 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 first 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 server 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 first node runs the newest version of software installed on the server. Perform a fresh installation on the subsequent node using the same software version as that running on the active partition of the first node. If you are reinstalling the subsequent node, you should delete the server from Cisco Unified Communications Manager Administration and add the server 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 Cisco Unified Communications Manager server 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.

Making Configuration Changes During an Upgrade

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 servers in the cluster, until you have switched the servers over to the upgraded partition, and until you have verified that database replication is functioning.

Procedure

Step 1 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 2 Upgrade the first node in the cluster (the publisher node).

Step 3 Upgrade the subsequent nodes in the cluster (the subscriber nodes).

Step 4 Switch over the first node to the upgraded partition.

Step 5 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 6 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 Cisco Unified Real Time Monitoring Tool Administration Guide*.

Step 7 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

Upgrading a Cluster in Parallel

When you upgrade a cluster that is running a supported version of Cisco Unified Communications Manager 8.x to Cisco Unified Communications Manager 8.6, begin upgrading the first node first. You can begin upgrading subsequent nodes in parallel after the first node reaches a specified point in the upgrade.

During the upgrade of the first node, 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 begin the upgrade of the subsequent nodes after the following information displays in the log:

PRODUCT_TARGET is <product target id>

PRODUCT_NAME is <product name>

PRODUCT_VERSION is <product version to which you are upgrading, such as 8.6>

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:

```
file search install install_log_2008-10-14.09.31.06.log PRODUCT_VERSION

Searching path: /var/log/install/install_log_2008-10-14.09.31.06.log
Searching file: /var/log/install/install_log_2008-10-14.09.31.06.log
10/14/2008 09:52:14 upgrade_os.sh|PRODUCT_VERSION is 7.1.0.39000-97|<LVL::Info>

Search completed
```

Step 3 When the **file search** command finds the PRODUCT_VERSION string in the install log, you can start the upgrade of the subsequent nodes.

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

When you are ready to activate the new version, you must activate the new software on the first node before activating it on all other nodes.

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

Obtaining the Upgrade File

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

For more information, see the “Installation and Upgrade Information” section of the applicable Cisco Unified Communications Manager release notes at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_release_notes_list.html

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 and contains the following topics:

- Upgrading from a Local Source, page 7-10
- Upgrading from a Remote Source, page 7-12
- Bridge Upgrade, page 7-15

Upgrading from a 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 key to migrate the data from the old system to the new installation.

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 key to migrate the data from the old system to the new installation.

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 **Reboot 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 reboot 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.

Upgrading from a Remote Source

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 key to migrate the data from the old system to the new installation.

Supported SFTP Servers

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.

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

Step 2 Log in to Cisco Unified Communications Operating System Administration.

Step 3 Navigate to **Software Upgrades > Install/Upgrade**.

The Software Installation/Upgrade window displays.

Step 4 From the **Source** list, choose **Remote Filesystem**.

Step 5 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

- Begin the path with a forward slash (/) and use forward slashes throughout the path.
- 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 6 In the **Server** field, enter the server name or IP address.

Step 7 In the **User Name** field, enter your user name on the remote server.

Step 8 In the **User Password** field, enter your password on the remote server.

Step 9 Select the transfer protocol from the **Transfer Protocol** field.

Step 10 To use the Email Notification feature, enter your Email Destination and SMTP Server in the fields provided.

Step 11 To continue the upgrade process, click **Next**.

Step 12 Choose the upgrade version that you want to install and click **Next**.

Step 13 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:

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

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

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

Step 14 If you want to install the upgrade and automatically reboot to the upgraded partition, choose **Reboot to upgraded partition**. The system restarts and runs the upgraded software.

Step 15 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 reboot 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 server that supports the newest release of Cisco Unified Communications Manager.

Servers that are no longer supported, but are permitted to function as bridge upgrade servers, 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.

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) server. 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) servers. 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 Unifed 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 server. You must obtain and install a new license on this server. 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 Step 4. 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 server, 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 in Step 4. You will be prompted for the "old" security password that you noted in Step 4. For further details, refer to the *Disaster Recovery System Administration Guide*.

Step 8 On your new supported first node server, 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:

- 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.

Reverting to a Previous Version

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

This section contains the following topics:

- Reverting a Cluster to a Previous Version, page 7-17
- Reverting the Publisher or Subscriber Nodes to a Previous Version, page 7-18
- Resetting Database Replication When Reverting to an Older Product Release, page 7-19

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 key to migrate the data from the old system to the new installation.

Reverting a Cluster to a Previous Version

Note If you downgrade a cluster to a nonsecure previous release of Cisco Unified Communications Manager (releases 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 will have to manually delete the ITL file on each Cisco Unified IP Phone in the system. For more information, see Chapter 2, “Security by Default,” in the *Cisco Unified Communications Manager Security Guide*.

To revert a cluster to a previous version, follow these major steps:

	Task	For Additional Information
Step 1	Revert the publisher node.	"Reverting the Publisher or Subscriber Nodes to a Previous Version" section on page 7-18.
Step 2	Revert all backup subscriber nodes.	"Reverting the Publisher or Subscriber Nodes to a Previous Version" section on page 7-18
Step 3	Revert all primary subscriber nodes.	"Reverting the Publisher or Subscriber Nodes to a Previous Version" section on page 7-18
Step 4	If you are reverting to an older product release, reset database replication within the cluster.	"Resetting Database Replication When Reverting to an Older Product Release" section on page 7-19

Reverting the Publisher or Subscriber Nodes to a Previous Version

Procedure

Step 1 Open Cisco Unified Communications Operating System Administration directly by entering the following URL:

https://*server-name***/cmplatform**

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

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, you can follow these steps:

a. Log in to Open 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 by entering the following URL and entering your user name and password:

https://*server-name***/ccmadmin**

f. Verify that you can log in and that your configuration data exists.

Resetting Database Replication When Reverting to an Older Product Release

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.

Installing COP Files, Dial Plans, and Locales

This section contains the following topics:

- COP File Installation, page 7-19
- Dial Plan Installation, page 7-19
- Locale Installation, page 7-19

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 COP file on every server in a cluster.
- After you install a COP file, you must restart the server.

Note You must restart Cisco Unified Communications Manager to ensure that configuration changes that are made during the COP file installation get written into the database. Cisco recommends that you perform this restart during an off-peak period.

Dial Plan Installation

You can install dial plan files from either a local or a remote source by using the same process that is described earlier in this chapter for installing software upgrades. See the "Software Upgrade Procedures" section on page 7-10 for more information about this process.

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.

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.

Changes do not take effect until you reboot every server in the cluster. Cisco strongly recommends that you do not reboot the servers until you have installed all locales on all servers in the cluster. Minimize call-processing interruptions by rebooting the servers after regular business hours.

Installing Locales

You can install locale files from either a local or a remote source by using the same process that is described earlier in this chapter for installing software upgrades. See the "Software Upgrade Procedures" section on page 7-10 for more information about this process.

Note To activate the newly installed locales, you must restart the server.

See the "Cisco Unified Communications Manager Locale Files" section on page 7-20 for information on the Cisco Unified Communications Manager locale files that you must install. You can install more than one locale before you restart the server.

Cisco Unified Communications Manager Locale Files

When you are installing Cisco Unified Communications Manager locales, you must install the following files:

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

  cm-locale-*language-country-version*.cop

- 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

Error Messages

See Table 7-1 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 7-1 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 server does not have Cisco Unified Communications Manager installed (most likely). Installation of the locale will terminate because locales will not work without the correct records that are held in the database.
[LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maDialogs_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maMessages_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maGlobalUI_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/LocaleMasterVersion.txt.Checksum.	These errors could occur when the system fails to create a checksum file; causes can include an absent Java executable, /usr/local/thirdparty/java/j2sdk/jre/bin/java, an absent or damaged Java archive file, /usr/local/cm/jar/cmutil.jar, or an absent or damaged Java class, com.cisco.ccm.util.Zipper. Even if these errors occur, the locale will continue to work correctly, with the exception of Cisco Unified Communications Manager Assistant, which cannot detect a change in localized Cisco Unified Communications Manager Assistant files.
[LOCALE] Could not find /usr/local/cm/application_locale/cmservices/ipma/LocaleMasterVersion.txt in order to update Unified CM Assistant locale information.	This error occurs when the file does not get found in the correct location, which is most likely due to an error in the build process.
[LOCALE] Addition of <RPM-file-name> to the Cisco Unified Communications Manager database has failed!	This error occurs because of the collective result of any failure that occurs when a locale is being installed; it indicates a terminal condition.

Supported Cisco Unified Communications 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

Managing 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 servers, 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*.

Setting Up a Customized 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.

CHAPTER 8

Services

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

This chapter contains the following sections:

- Ping, page 8-1
- Remote Support, page 8-2

Ping

The Ping Utility window enables you to ping another server 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.

Remote Support

From the Remote Account Support 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 Table 8-1.

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.

Table 8-1 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.

INDEX

A

administrator password 2

B

browser requirements 1

C

Certificate Trust List
  See CTL
certificates
  deleting 2
  displaying 2
  downloading 2
  downloading a signing request 7
  expiration monitor fields (table) 9
  managing 1
  monitoring expiration dates 9
  regenerating 2, 3
  uploading 4
CLI
cluster nodes
  fields (table) 1
  procedure 1
Command Line Interface
  See CLI
configuration
  operating system 2, 1
CTL
  downloading 2
  managing 1
  uploading 4

D

dial plan installation 24

E

error messages
  descriptions (table) 25
Ethernet settings 1

H

hardware, status
  fields (table) 2
  procedure 2

I

install/upgrade, menu 3
installed software
  fields (table) 4
  procedure 3
installing
  dial plan 24
  locales 24, 25
Internet Explorer
  set security options 1
IPSec
  changing policy 11
  displaying policy 11
  management 9

policy fields (table) 10
setting up new policy 9

L

locales
files 25
installation 24
installer
error messages (table) 25
installing 25
logging in
overview 1
procedure 1

M

menu
install/upgrade 3
security 3
settings 2
show 2
messages, error

N

network status
fields (table) 3
nodes, cluster
fields (table) 1
procedure 1
NTP server settings 7

O

operating system
administrator password 2
browser requirements 1
configuration 2, 1
hardware status
fields (table) 2
procedure 2
introduction 1
logging in 1
network status fields (table) 3
overview 1
restart 2
security 3
services 3
settings 2, 1
software upgrades 3
status 2, 1

P

password, recovering 2
ping 1
publisher settings 6

R

remote support
setting up 2
status fields (table) 2
restart
current version 2
system 1

S

security
configuration 3
menu 3
overview 1
set IE options 1

services
overview 1
ping 3, 1
remote support 3
overview 2
setting up 2
settings
Ethernet
fields (table) 2
procedure 1
IP 1
menu 2
NTP servers 7
overview 1
publisher 6
SMTP 8
time 9
show, menu 2
shutdown, operating system 2
SMTP settings 8
software
installed
fields (table) 4
procedure 3
upgrades 3
bridge upgrade 19
from local source 15
from remote source 16
overview 1
status
hardware
fields (table) 2
procedure 2
network
fields (table) 3
operating system 2, 1
system
fields (table) 4
procedure 4
supported products 26
system
restart 1
shutdown 2
status
fields (table) 4
procedure 4

T

TFTP server, installing files 27
throttling check box in upgrade window 12
time settings 9
V
version, restart 2
A
administrator password 2
B
browser requirements 1
C
certificates
deleting 2
displaying 2
downloading 2
downloading a signing request 7
expiration monitor fields (table) 9
monitoring expiration dates 8
regenerating 2, 3
uploading 4
CLI
cluster nodes
fields (table) 1
procedure 1
Command Line Interface
See CLI
configuration
operating system 2, 1
CTL
downloading 2

E
error messages
descriptions (table) 5
Ethernet settings 1
H
hardware, status
fields (table) 2
procedure 2
I
install/upgrade, menu 3
installed software
fields (table) 4
procedure 3
Internet Explorer
set security options 1
IPSec
changing policy 15
displaying policy 15
management 10
policy fields (table) 11, 13
setting up new policy 10
L
locales
installer
error messages (table) 5
logging in
overview 1
procedure 1
M
menu
install/upgrade 3
security 3
settings 2
show 2
messages, error
N
network status
fields (table) 3
nodes, cluster
fields (table) 1
procedure 1
NTP server settings 4
O
operating system
administrator password 2
browser requirements 1
configuration 2, 1
hardware status
fields (table) 2
procedure 2
introduction 1
logging in 1
network status fields (table) 3
overview 1
restart 2
security 3
services 3
settings 2, 1
software upgrades 3
status 2, 1
P
password, recovering 2
ping 1
publisher settings 3
R
remote support
setting up 2
status fields (table) 2
restart
current version 2
system 1
S
security
configuration 3
menu 3
overview 1
set IE options 1

services
overview 1
ping 3, 1
remote support 3
overview 2
setting up 2
settings
Ethernet
fields (table) 2
procedure 1
IP 1
menu 2
NTP servers 4
overview 1
publisher 3
SMTP 5
time 7
show, menu 2
shutdown, operating system 2
SMTP settings 5
software
installed
fields (table) 4
procedure 3
upgrades 3
from local source 3
from remote source 3
overview 1
status
hardware
fields (table) 2
procedure 2
network
fields (table) 3
operating system 2, 1
system
fields (table) 4
procedure 4
supported products 6
system
restart 1
shutdown 2
status
fields (table) 4
procedure 4
T
time settings 7
V
version, restart 2
A
administrator password 2
B
browser requirements 1
C
certificates
deleting 2
displaying 2
downloading 2
downloading a signing request 7
expiration monitor fields (table) 9
monitoring expiration dates 8
regenerating 2, 3
uploading 5
CLI
cluster nodes
fields (table) 1
procedure 1
Command Line Interface
See CLI
configuration
operating system 2, 1
CTL
downloading 2
D
dial plan installation 19
E
error messages
descriptions (table) 21
Ethernet settings 1
H
hardware, status
fields (table) 2
procedure 2
I
install/upgrade, menu 3
installed software

fields (table) 4
procedure 3
installing
dial plan 19
locales 19, 20
Internet Explorer
set security options 1
IPSec
changing policy 14
displaying policy 14
management 10
policy fields (table) 11, 13
setting up new policy 10
L
locales
files 20
installation 19
installer
error messages (table) 21
installing 20
logging in
overview 1
procedure 1
M
menu
install/upgrade 3
security 3
settings 2
show 2
messages, error
N
network status
fields (table) 3
nodes, cluster
fields (table) 1
procedure 1
NTP server settings 7
O
operating system
administrator password 2
browser requirements 1
configuration 2, 1
hardware status
fields (table) 2
procedure 2
introduction 1
logging in 1
network status fields (table) 3
overview 1
restart 2
security 3
services 3
settings 2, 1
software upgrades 3
status 2, 1
P
password, recovering 2
ping 1
publisher settings 6
R
remote support
setting up 2
status fields (table) 2
restart
current version 2
system 1
S
security
configuration 3
menu 3
overview 1
set IE options 1
services
overview 1
ping 3, 1
remote support 3
overview 2
setting up 2
settings
Ethernet
fields (table) 2
procedure 1
IP 1
menu 2
NTP servers 7
overview 1
publisher 6
SMTP 8
time 9
show, menu 2
shutdown, operating system 2
SMTP settings 8
software
installed
fields (table) 4
procedure 3

upgrades 3
bridge upgrade 15
from local source 10
from remote source 12, 13
overview 1
status
hardware
fields (table) 2
procedure 2
network
fields (table) 3
operating system 2, 1
system
fields (table) 4
procedure 4
supported products 22
system
restart 1
shutdown 2
status
fields (table) 4
procedure 4
T
TFTP server, installing files 22
time settings 9
V
version, restart 2