



Cisco Unified Communications Operating System Administration Guide

Release 7.0(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-16419-01

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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0805R)

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

Cisco Unified Communications Operating System Administration Guide
© 2008 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface 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	1-3

CHAPTER 2

Log in to Cisco Unified Communications Operating System Administration	2-1
Logging in to Cisco Unified Communications Operating System Administration	2-1
Recovering 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
Publisher Settings	4-2
NTP Servers	4-2
SMTP Settings	4-3
Time Settings	4-3

CHAPTER 5

System Restart 5-1

- Switch Versions and Restart 5-1
- Restart Current Version 5-1
- Shut Down the System 5-2

CHAPTER 6

Security 6-1

- Set Internet Explorer Security Options 6-1
- Manage Certificates and Certificate Trust Lists 6-1
 - Display Certificates 6-2
 - Download a Certificate or CTL 6-2
 - Delete and Regenerate a Certificate 6-2
 - Deleting a Certificate 6-3
 - Regenerating a Certificate 6-3
 - Upload a Certificate or Certificate Trust List 6-4
 - Upload a Certificate 6-4
 - Upload a Certificate Trust List 6-5
 - Upload a Directory Trust Certificate 6-5
 - Using Third-Party CA Certificates 6-6
 - Generating a Certificate Signing Request 6-6
 - Download a Certificate Signing Request 6-7
 - Obtaining Third-Party CA Certificates 6-7
 - Monitor Certificate Expiration Dates 6-8
- IPSEC Management 6-8
 - Set Up a New IPsec Policy 6-8
 - Managing Existing IPsec Policies 6-10

CHAPTER 7

Software Upgrades 7-1

- Pre-Upgrade Tasks 7-1
- Software Upgrade and Installation 7-2
 - Obtaining the Upgrade File 7-3
 - Upgrading Software or Installing Locales from a Local Source 7-3
 - Upgrading Software or Installing Locales from a Remote Source 7-4
- Post-Upgrade Tasks 7-7
- Stalled Upgrades 7-7
- Reverting to a Previous Version 7-8
- Dial Plan Installation 7-8
- Locale Installation 7-9
 - Installing Locales 7-9

Cisco Unified Communications Manager Locale Files	7-9
Managing TFTP Server Files	7-10

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 Unified 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 .
<i>italic font</i>	Arguments for which you supply values are in <i>italics</i> .
[]	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 <code>screen font</code> .
boldface screen font	Information you must enter is in boldface screen font .
<i>italic screen font</i>	Arguments for which you supply values are in <i>italic screen font</i> .
	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:

- Microsoft Internet Explorer version 6.x
- Netscape Navigator version 7.1 or later

**Note**

Cisco does not support or test other browsers, such as Mozilla Firefox.

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, Certificate Trust Lists (CTL), 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 Unified 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 recovering a lost password.

This chapter comprises the following sections:

- [Logging in to Cisco Unified Communications Operating System Administration, page 2-1](#)
- [Recovering 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.

Recovering 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 recovery 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 recover 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 4-2](#)
- [SMTP Settings, page 4-3](#)
- [Time Settings, page 4-3](#)

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](#)
- [Publisher Settings, page 4-2](#)

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.

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.
IP Address	Displays the IP address of the system.
Subnet Mask	Displays the IP subnet mask address.
Default Gateway	Shows the IP address of the network gateway.

Publisher Settings

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

NTP Servers

Ensure that external NTP server is 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:

- 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 [NTP Servers](#) for more information.

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**.



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 or 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:



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**

If you press the power button on the server, the system will immediately shut down.

To shut down the system, follow this procedure:

**Caution**

This procedure causes the system to shut down.

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 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 does not power down automatically.



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 and Certificate Trust Lists](#)
- [IPSEC Management](#)

Set Internet Explorer Security Options

To download certificates from the server, ensure your Internet Explorer security settings are configured as follows:

Procedure

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

Manage Certificates and Certificate Trust Lists

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

- [Display Certificates](#)
- [Download a Certificate or CTL](#)
- [Delete and Regenerate a Certificate](#)
- [Upload a Certificate or Certificate Trust List](#)

- [Using Third-Party CA Certificates](#)

**Note**

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

Display Certificates

To display existing certificates, 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** To view details of a certificate or trust store, click its file name.
The Certificate Configuration window displays information about the certificate.
 - Step 4** To return to the Certificate List window, select **Back To Find/List** in the Related Links list; then, click **Go**.
-

Download a Certificate or CTL

To download a certificate or CTL 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 or CTL.
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 deleting and regenerating a certificate:

- [Deleting a Certificate](#)

- [Regenerating a Certificate](#)

Deleting a Certificate

To delete a trusted certificate, follow this procedure:

**Caution**

Deleting a certificate can affect your system operations. Any existing CSR for the certificate you choose from the Certificate list gets deleted from the system, and you must generate a new CSR. For more information, see the [“Generating a Certificate Signing Request” procedure on page 6-6](#).

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 or CTL.
The Certificate Configuration window displays.
- Step 4** Click **Delete**.
-

Regenerating a Certificate

To regenerate a certificate, follow this procedure:

**Caution**

Regenerating a certificate can affect your system operations.

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 a description of the certificate names that display, see [Table 6-1](#).
- Step 4** Click **Generate New**.
-

Table 6-1 Certificate Names and Descriptions

Name	Description
tomcat	This self-signed root certificate gets generated during installation for the HTTPS server.
ipsec	This self-signed root certificate gets generated during installation for IPsec connections with MGCP and H.323 gateways.
CallManager	This self-signed root certificate automatically installs 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 CTL client configuration.

Upload a Certificate or Certificate Trust List



Caution

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



Note

The system does not distribute trust certificates to other cluster nodes automatically. If you need to have the same certificate on more than one node, you must upload the certificate to each node individually.

These sections describe how to upload a CA root certificate, application certificate, or CTL file to the server:

- [Upload a Certificate](#)
- [Upload a Certificate Trust List](#)
- [Upload a Directory Trust Certificate](#)

Upload a Certificate

Procedure

-
- Step 1** Navigate to **Security > Certificate Management**.
The Certificate List window displays.
- Step 2** Click **Upload Certificate**.
The Upload Certificate dialog box opens.

- Step 3** Select the certificate name from the **Certificate Name** list.
- Step 4** If you are uploading an application certificate that was issued by a third-party CA, enter the name of the CA root certificate in the **Root Certificate** text box. If you are uploading a CA root certificate, leave this text box empty.
- Step 5** 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**.
- Step 6** To upload the file to the server, click the **Upload File** button.
-

Upload a Certificate Trust List

Procedure

- Step 1** Navigate to **Security > Certificate Management**.
The Certificate List window displays.
- Step 2** Click **Upload Certificate**.
The Upload Certificate Trust List dialog box opens.
- Step 3** Select the certificate name from the **Certificate Name** list.
- Step 4** If you are uploading an application certificate that was issued by a third-party CA, enter the name of the CA root certificate in the **Root Certificate** text box. If you are uploading a CA root certificate, leave this text box empty.
- Step 5** 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**.
- Step 6** To upload the file to the server, click the **Upload File** button.
-

Upload a Directory Trust Certificate

Procedure

- Step 1** Navigate to **Security > Certificate Management**.
The Certificate List window displays.
- Step 2** Click **Upload Certificate**.
The Upload Certificate Trust List dialog box opens.
- Step 3** Select **directory-trust** from the **Certificate Name** list.
- Step 4** Enter the file to upload in the **Upload File** field.
- Step 5** To upload the file, click the **Upload File** button.
- Step 6** Log into Cisco Unified Serviceability.

- Step 7** Navigate to **Tools > Control Center - Feature Services**.
- Step 8** Restart the service **Cisco Dirsync**.
- Step 9** Log in to the Cisco Unified Communications Operating System CLI as an administrator.
- Step 10** To restart the Tomcat service, enter the command **utils service restart Cisco Tomcat**.
- Step 11** After the services have been restarted, you can add the directory agreement for SSL.

Using Third-Party CA Certificates

Cisco Unified Communications Operating System supports certificates that a third-party Certificate Authority (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 6-6.
Step 2	Download the CSR to your PC.	See the “Download a Certificate Signing Request” section on page 6-7.
Step 3	Use the CSR to obtain an application certificate from a CA.	Get information about obtaining application certificates from your CA. See “Obtaining Third-Party CA Certificates” section on page 6-7 for additional notes.
Step 4	Obtain the CA root certificate.	Get information about obtaining a root certificate from your CA. See “Obtaining Third-Party CA Certificates” section on page 6-7 for additional notes.
Step 5	Upload the CA root certificate to the server.	See the “Upload a Certificate” section on page 6-4.
Step 6	Upload the application certificate to the server.	See the “Upload a Certificate” section on page 6-4.
Step 7	If you updated the certificate for CAPF or Cisco Unified Communications Manager, generate a new CTL file.	See the <i>Cisco Unified Communications Manager Security Guide</i> .
Step 8	Restart the services that are affected by the new certificate.	For all certificate types, restart the corresponding service (for example, restart the Tomcat service if you updated the Tomcat certificate). In addition, if you updated the certificate for CAPF or Cisco Unified Communications Manager, restart the TFTP service. See the <i>Cisco Unified Communications Manager Serviceability Administration Guide</i> for information about restarting services.

Generating a Certificate Signing Request

To generate a Certificate Signing Request (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.



Note For the current release of the Cisco Unified Operating System, the Directory option is no longer available in the list of Certificate Names. However, you can still upload a Directory Trust certificate from a previous release, which is required for the DirSync service to work in Secure mode.

- Step 4** Click **Generate CSR**.
-

Download 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. Get information about obtaining these certificates from your CA. The process varies among CAs.

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 that are listed on the final page of the CSR generation process.

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

Monitor Certificate Expiration Dates

The system can automatically send you an e-mail 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	Select 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.

IPSEC Management

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

- [Set Up a New IPsec Policy](#)
- [Managing Existing IPsec Policies](#)



Note

IPsec does not automatically get 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 get 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 on the IPSEC Policy Configuration window. For a description of the fields on this window, see [Table 6-3](#).
- Step 4** To set up the new IPSec policy, click **Save**.

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.
Preshared Key	Specifies the preshared key if you selected Pre-shared Key in the Authentication Name field.
Peer Type	Specifies whether the peer is the same type or different.
Destination Address	Specifies the IP address or FQDN of the destination.
Destination Port	Specifies the port number at the destination.
Source Address	Specifies the IP address or FQDN of the source.
Source Port	Specifies the port number at the source.
Mode	Specifies Tunnel or Transport mode.
Remote Port	Specifies the port number to use at the destination.
Protocol	Specifies the specific protocol, or Any: <ul style="list-style-type: none"> • TCP • UDP • Any
Encryption Algorithm	From the drop-down list, choose the encryption algorithm. Choices include <ul style="list-style-type: none"> • DES • 3DES

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

Field	Description
Hash Algorithm	Specifies the hash algorithm <ul style="list-style-type: none"> • SHA1—Hash algorithm that is used in phase 1 IKE negotiation • MD5—Hash algorithm that is used in phase 1 IKE negotiation
ESP Algorithm	From the drop-down list, choose the ESP algorithm. Choices include <ul style="list-style-type: none"> • NULL_ENC • DES • 3DES • BLOWFISH • RIJNDAEL
Phase One Life Time	Specifies the lifetime for phase One, IKE negotiation, in seconds.
Phase One DH	From the drop-down list, choose the phase One DH value. Choices include: 2, 1, 5, 14, 16, 17, and 18.
Phase Two Life Time	Specifies the lifetime for phase Two, IKE negotiation, in seconds.
Phase Two DH	From the drop-down list, choose the phase Two DH value. Choices include: 2, 1, 5, 14, 16, 17, and 18.
Enable Policy	Check the check box to enable the policy.

Managing 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 will get lost, do not modify or create IPsec policies during an upgrade.



Caution

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



Caution

Any changes that you make to the existing IPsec policies can impact your normal system operations.

Procedure

Step 1 Navigate to **Security > IPSEC Configuration**.



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

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, use the **Enable Policy** check box.
- c. Click **Save**.

Step 3 To delete one or more policies, follow these steps:

- a. Select the check box next to the policies that you want to delete.
You can click **Select All** to select all policies or **Clear All** to clear all the check boxes.
 - b. Click **Delete Selected**.
-



CHAPTER 7

Software Upgrades

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

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

This chapter contains the following sections:

- [Pre-Upgrade Tasks, page 7-1](#)
- [Software Upgrade and Installation, page 7-2](#)
- [Post-Upgrade Tasks, page 7-7](#)
- [Stalled Upgrades, page 7-7](#)
- [Reverting to a Previous Version, page 7-8](#)
- [Dial Plan Installation, page 7-8](#)
- [Locale Installation, page 7-9](#)
- [Managing TFTP Server Files, page 7-10](#)

Pre-Upgrade Tasks

Before you begin the upgrade, perform the following tasks:

- Read the release notes for the new release and be sure you understand the new features and how the upgrade interacts with the other products associated with your system, such as JTAPI, IPMA, RTMT, IPCC, firewalls, and so on.

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

http://cisco.com/en/US/products/ps7273/prod_release_notes_list.html

For Cisco Unity Connection, the release notes are located at

http://cisco.com/en/US/products/ps6509/prod_release_notes_list.html

- Ensure that you have the necessary license files for the new release. For more information, see the *Cisco Unified Communications Manager Administration Guide*.

- Before you begin the upgrade, back up your system. For more information, see the *Disaster Recovery System Administration Guide*.
- 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 will not be able to log in and log out of phones that support Cisco Extension Mobility.

**Caution**

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

After you complete the pre-upgrade tasks, continue with the [“Software Upgrade and Installation” section on page 7-2](#).

Software Upgrade and Installation

You can install upgrade software on your server while the system continues to operate. Two partitions exist on your system: an active, bootable partition and an inactive, bootable partition. The system boots up and operates entirely on the partition that is marked as the active partition.

**Note**

If you have users logging in and logging out of Cisco Extension Mobility, this could cause the upgrade to fail. Before starting the upgrade, you must disable the Cisco Extension Mobility service. For more information, see the [“Pre-Upgrade Tasks” section on page 7-1](#).

When you install upgrade software, you install the software on the inactive partition. The system continues to function normally while you are installing the software. When you are ready, you activate the inactive partition and reboot the system with the new upgrade software. The current active partition will then get identified as the inactive partition when the system restarts. The current software remains in the inactive partition until the next upgrade. Your configuration information migrates automatically to the upgraded version in the active partition.

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

You can install a patch or upgrade version from a DVD (local source) or from a network location (remote source) that the Cisco Unified Communications Manager Business Edition server can access.

**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*.

This section contains the following topics:

- [Obtaining the Upgrade File, page 7-3](#)
- [Upgrading Software or Installing Locales from a Local Source, page 7-3](#)
- [Upgrading Software or Installing Locales from a Remote Source, page 7-4](#)

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 Business Edition release notes at http://www.cisco.com/en/US/products/ps7273/prod_release_notes_list.html.

**Note**

Do not rename the patch file before you install it because the system will not recognize it as a valid file.

**Note**

Do not unzip or untar the file. If you do, the system may not be able to read the upgrade files.

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.

Upgrading Software or Installing Locales from a Local Source

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

Procedure

-
- Step 1** If you are upgrading Cisco Unified Communications Manager Business Edition, skip to [Step 2](#). If you are adding a Cisco Unity Connection locale, stop the Connection Conversation Manager and Connection Mixer services:
- a. Start Cisco Unity Connection Serviceability.
 - b. Navigate to **Tools > Control Center - Feature Services**.
 - c. Under Critical Services, in the Connection Conversation Manager row, click **Stop**.
 - d. Wait for the service to stop.
 - e. Also under Critical Services, in the Connection Mixer row, click **Stop**.
 - f. Wait for the service to stop.
- Step 2** Insert the new DVD into the disc drive on the local server that is to be upgraded.
- Step 3** Log into Cisco Unified Communications Operating System Administration by entering its URL in a browser:
- `http://server-name/cmplatform`**
- where *server-name* is the name or IP address of the server.
- Step 4** Navigate to **Software Upgrades > Install/Upgrade**.

The Software Installation/Upgrade window displays.

Step 5 Choose **DVD/CD** from the **Source** list.

Step 6 Enter the path to the patch file on the CD or DVD in the Directory field.

If the file is in the root directory, or if you created an ISO image DVD, enter a slash (/) in the Directory field.

Step 7 To continue the upgrade process, click **Next**.

Step 8 Choose the upgrade version that you want to install and click **Next**.

Step 9 In the next window, monitor the progress of the download.

Step 10 If you are upgrading Cisco Unified Communications Manager Business Edition, skip to [Step 11](#).

If you are installing Cisco Unity Connection locales and want to install another locale, click **Install Another**, and return to [Step 4](#).

If you do not want to install another locale, restart the Connection Conversation Manager and Connection Mixer services:

- a. Start Cisco Unity Connection Serviceability.
- b. Navigate to **Tools > Control Center - Feature Services**.
- c. Under Critical Services, in the Connection Conversation Manager row, click **Start**.
- d. Wait for the service to start.
- e. Also under Critical Services, in the Connection Mixer row, click **Start**.
- f. Wait for the service to start.
- g. Skip the rest of the procedure.

Step 11 If you want to install the upgrade and automatically reboot to the upgraded partition, choose **Reboot to upgraded partition**. The system restarts running the upgraded software.

Step 12 If you want to install the upgrade and then manually reboot 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 Software or Installing Locales from a Remote Source

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 accessing Cisco Unified Operating System Administration. Instead, use the navigation controls provided by the interface.

Procedure

-
- Step 1** Put the upgrade file on an FTP or SFTP server that the server you are upgrading can access.
- Step 2** If you are upgrading Cisco Unified Communications Manager Business Edition, skip to [Step 3](#).
If you are adding a Cisco Unity Connection locale, stop the Connection Conversation Manager and Connection Mixer services:
- Start Cisco Unity Connection Serviceability.
 - Navigate to **Tools > Control Center - Feature Services**.
 - Under Critical Services, in the Connection Conversation Manager row, click **Stop**.
 - Wait for the service to stop.
 - Also under Critical Services, in the Connection Mixer row, click **Stop**.
 - Wait for the service to stop.
- Step 3** Log into Cisco Unified Communications Operating System Administration by entering its URL in a browser:
http://server-name/cmplatform
where *server-name* is the name or IP address of the server.
- Step 4** Navigate to **Software Upgrades > Install/Upgrade**.
The Software Installation/Upgrade window displays.
- Step 5** Choose **Remote Filesystem** from the **Source** list.
- Step 6** Enter the path to the directory that contains the patch file on the remote system in the **Directory** field.
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 7** In the **Server** field, enter the server name or IP address.
- Step 8** In the **User Name** field, enter your user name on the remote server.
- Step 9** In the **User Password** field, enter your password on the remote server.
- Step 10** Select the transfer protocol from the **Transfer Protocol** field.
- Step 11** To 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 are installing upgrade software, skip to [Step 15](#).

If you are installing Cisco Unity Connection locales and want to install another locale, click **Install Another**, and return to [Step 4](#).

If you do not want to install another locale, restart the Connection Conversation Manager and Connection Mixer services:

- a. Start Cisco Unity Connection Serviceability.
- b. Navigate to **Tools > Control Center - Feature Services**.
- c. Under Critical Services, in the Connection Conversation Manager row, click **Start**.
- d. Wait for the service to start.
- e. Also under Critical Services, in the Connection Mixer row, click **Start**.
- f. Wait for the service to start.
- g. Skip the rest of the procedure.

Step 15 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 16 If you want to install the upgrade and then manually reboot 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.

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 will not be able to 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.

Stalled Upgrades

During the installation of upgrade software, the upgrade may seem to stall. The upgrade log stops displaying new log messages. When the upgrade stalls, you must cancel the upgrade, disable I/O throttling, and restart the upgrade procedure. When you successfully complete the upgrade, you do not need to reenable I/O throttling.

To disable I/O throttling, enter the CLI command **utils iothrottle disable**.

To display the status of I/O throttling, enter the CLI command **utils iothrottle status**.

To enable I/O throttling, enter the CLI command **utils iothrottle enable**. By default, iothrottle remains enabled.

If the system does not respond to the cancellation, you must reboot the server, disable I/O throttling, and restart the upgrade process procedure.

Reverting to a Previous Version

After upgrading, you can revert to the software version that was running before the upgrade, by restarting your system and switching to the software version on the inactive partition.

Procedure

- Step 1** Open Cisco Unified Communications Operating System Administration directly by entering the following URL:
- `https://server-name/cmplatform`**
- where *server-name* is the host name or IP address of the Cisco Unified Communications Manager Business Edition server.
- Step 2** Enter your Administrator username 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:
- Log into Open Cisco Unified Communications Operating System Administration again.
 - Choose **Settings>Version**.
 - The Version Settings window displays.
 - Verify that the correct product version is now running on the active partition.
 - Verify that all activated services are running.
 - Log into Cisco Unified Communications Manager Administration by entering the following URL and entering your user name and password:
- `https://server-name/ccmadmin`**
- Verify that you can log in and that your configuration data exists.
-

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 and Installation” section on page 7-2](#) 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.

Cisco Unity Connection Locales

Cisco Unity Connection locales (languages) provide country-specific system prompts, graphical user interface, and text-to-speech functionality. For information on downloading Cisco Unity Connection locales, see the “Installation and Upgrade Information” section of the applicable Cisco Unified Communications Manager Business Edition release notes at http://www.cisco.com/en/US/products/ps7273/prod_release_notes_list.html.



Caution

Do not install more than five Cisco Unity Connection locales.

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 and Installation](#)” section on page 7-2 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 7-9 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 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

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 Unified Solutions*.



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 configurable time limit on how long Cisco personnel can access it.
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 be at least six-characters long and 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 [2-2](#)

B

browser requirements [1-1](#)

C

certificates

deleting [6-2](#)

displaying [6-2](#)

downloading [6-2](#)

downloading a signing request [6-7](#)

expiration monitor fields (table) [6-8](#)

managing [6-1](#)

monitoring expiration dates [6-8](#)

regenerating [6-2, 6-3](#)

uploading [6-4](#)

Certificate Trust List

See CTL

CLI

cluster nodes

fields (table) [3-1](#)

procedure [3-1](#)

Command Line Interface

See CLI

configuration

operating system [1-2, 3-1](#)

CTL

downloading [6-2](#)

managing [6-1](#)

uploading [6-4](#)

D

dial plan installation [7-8](#)

E

Ethernet settings [4-1](#)

H

hardware, status

fields (table) [3-2](#)

procedure [3-2](#)

I

install/upgrade, menu [1-3](#)

installed software

fields (table) [3-4](#)

procedure [3-3](#)

installing

dial plan [7-8](#)

locales [7-9](#)

Internet Explorer

set security options [6-1](#)

IPSec

changing policy [6-10](#)

displaying policy [6-10](#)

management [6-8](#)

policy fields (table) [6-9](#)

setting up new policy [6-8](#)

L

locales

- files [7-9](#)
- installation [7-9](#)
- installing [7-9](#)

logging in

- overview [2-1](#)
- procedure [2-1](#)

M

menu

- install/upgrade [1-3](#)
- security [1-3](#)
- settings [1-2](#)
- show [1-2](#)

N

network status

- fields (table) [3-3](#)

nodes, cluster

- fields (table) [3-1](#)
- procedure [3-1](#)

NTP server settings [4-2](#)**O**

operating system

- administrator password [2-2](#)
- browser requirements [1-1](#)
- configuration [1-2, 3-1](#)
- hardware status
 - fields (table) [3-2](#)
 - procedure [3-2](#)
- introduction [1-1](#)
- logging in [2-1](#)

network status fields (table) [3-3](#)

- overview [1-1](#)
- restart [5-1](#)
- security [1-3](#)
- services [1-3](#)
- settings [1-2, 4-1](#)
- software upgrades [1-3](#)
- status [1-2, 3-1](#)

Ppassword, recovering [2-2](#)ping [8-1](#)publisher settings [4-2](#)**R**

remote support

- setting up [8-2](#)
- status fields (table) [8-2](#)

restart

- current version [5-1](#)
- system [5-1](#)

S

security

- configuration [1-3](#)
- menu [1-3](#)
- overview [6-1](#)
- set IE options [6-1](#)

services

- overview [8-1](#)
- ping [1-3, 8-1](#)
- remote support [1-3](#)
 - overview [8-2](#)
 - setting up [8-2](#)

settings

- Ethernet
 - fields (table) [4-2](#)
 - procedure [4-1](#)
- IP [4-1](#)
- menu [1-2](#)
- NTP servers [4-2](#)
- overview [4-1](#)
- publisher [4-2](#)
- SMTP [4-3](#)
- time [4-3](#)
- show, menu [1-2](#)
- shutdown, operating system [5-2](#)
- SMTP settings [4-3](#)
- software
 - installation [7-2](#)
 - installed
 - fields (table) [3-4](#)
 - procedure [3-3](#)
 - upgrades [1-3](#)
 - overview [7-1](#)
 - procedure [7-2](#)
- status
 - hardware
 - fields (table) [3-2](#)
 - procedure [3-2](#)
 - network
 - fields (table) [3-3](#)
 - operating system [1-2, 3-1](#)
 - system
 - fields (table) [3-4](#)
 - procedure [3-4](#)
- system
 - restart [5-1](#)
 - shutdown [5-2](#)
 - status
 - fields (table) [3-4](#)
 - procedure [3-4](#)

T

- TFTP server, installing files [7-10](#)
- time settings [4-3](#)

V

- version, restart [5-1](#)

