



Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection

Release 10.x
Revised November, 2014

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Text Part Number:

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 or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: 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. (1721R)

Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection Release 10.x
© 2014 Cisco Systems, Inc. All rights reserved.



Preface	v
Audience and Use	v
Conventions	v
Related Documentation	vi
Obtaining Documentation and Submitting a Service Request	vii
Cisco Product Security Overview	vii
Introduction	1-1
Overview	1-1
Browser Requirements	1-2
Operating System Status and Configuration	1-2
Settings	1-2
Security Configuration	1-3
Software Upgrades	1-3
Command Line Interface	1-4
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
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
Settings	4-1
IP Settings	4-1
Ethernet Settings	4-1
Ethernet IPv6 Configuration Settings	4-2
Publisher Settings	4-2

- NTP Servers 4-2
- SMTP Settings 4-3
- Time Settings 4-4

System Restart 5-1

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

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 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 6-7
 - Download a Certificate Signing Request 6-7
 - Obtaining Third-Party CA Certificates 6-8
 - Monitor Certificate Expiration Dates 6-9
- IPSEC Management 6-9
 - Set Up a New IPsec Policy 6-9
 - Managing Existing IPsec Policies 6-11

Software Upgrades 7-1

- Setting Up a Customized Log-on Message 7-1

Services 8-1

- Ping 8-1
- Remote Support 8-2



Preface

This preface contains the following sections:

- [Audience and Use, page 5](#)
- [Conventions, page 5](#)
- [Related Documentation, page 6](#)
- [Documentation References to Cisco Business Edition, page 7](#)
- [Cisco Product Security Overview, page 7](#)

Audience and Use

The *Cisco Unified Communications Operating System Administration Guide* provides information about using the Cisco Unified Communications Operating System graphical user interface (GUI).

The guide 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.

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 Communications Solutions*.

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in boldface .
<i>italic</i> font	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.

Convention	Description
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.

The *Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection* also uses the following conventions:



Note

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



Timesaver

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



Tip

Means *the information contains useful tips*.



Caution

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



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.

Related Documentation

For further information about related Cisco IP telephony applications and products, see 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

Documentation References to Cisco Business Edition

In Cisco Unity Connection 10.x documentation set, references to “Cisco Business Edition” and Cisco Business Edition apply on Business Edition 6000/7000. The references do not apply on any other Business Editions.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, 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>

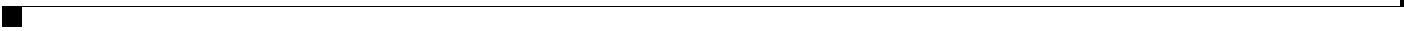
Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

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.





Introduction

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

This chapter comprises the following sections:

- [Overview, page 1-1](#)
- [Browser Requirements, page 1-2](#)
- [Operating System Status and Configuration, page 1-2](#)
- [Settings, page 1-2](#)
- [Security Configuration, page 1-3](#)
- [Software Upgrades, page 1-3](#)
- [The application provides the following operating system utilities:, page 1-3](#)
- [Command Line Interface, page 1-4](#)

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	<ul style="list-style-type: none"> • Microsoft XP service pack 3 • Microsoft Vista service pack 2 or later service pack • Microsoft Windows 7 with the latest service pack
Mozilla Firefox 3.x	<ul style="list-style-type: none"> • Microsoft XP service pack 3 • Microsoft Vista service pack 2 or later service pack • Microsoft Windows 7 with the latest service pack • Apple MAC OS X with the latest service pack
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, 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.”](#)

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 Communications Solutions*.



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 OS 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 Browse to the URL for Cisco Unity Connection Administration.

Step 2 From the **Navigation** menu in the upper, right corner of the Cisco Unity Connection 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 OS 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 created.

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.



Status and Configuration

This chapter provides information on administering the system and contains the following topics:

- [Cluster Nodes, page 3-1](#)
- [Hardware Status, page 3-2](#)
- [Network Configuration, page 3-2](#)
- [Installed Software, page 3-3](#)
- [System Status, page 3-4](#)
- [IP Preferences, page 3-5](#)

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.
Optionsosadmin-3-2	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.



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](#)
- [Ethernet IPv6 Configuration Settings, page 4-2](#)
- [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 IP settings, do the following procedure.



Caution

Do not use the procedure to change IP settings for Cisco Unity Connection.

For information on changing the IP address of a Connection server, see the “Changing the IP Addresses of Cisco Unity Connection Servers” *Upgrade Guide for Cisco Unity Connection* at http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html.

For information on changing the host name of a Unity Connection 10.x server, *Install, Upgrade, and Maintenance Guide for Cisco Unity Connection 10x* at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/install_upgrade/guide/10xcuciu_mgx.html.

Procedure

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

The Ethernet Settings window displays. For a description of the fields on the Ethernet Settings window, see [Table 4-1](#).

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.

Ethernet IPv6 Configuration Settings

Publisher Settings

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 using IPv6 addressing, external NTP servers must be NTP v4.

- 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 4-2](#) 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**.
- 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.
-



System Restart

This section provides procedures for using the following restart options:

- [Switch Versions and Restart, page 5-1](#)
- [Restart Current Version, page 5-1](#)
- [Shut Down the System, page 5-2](#)

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:



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 Unified Communications Solutions*.
-



Security

This chapter describes Certificate Management and IPSec Management and provides procedures for performing the following tasks:

- [Set Internet Explorer Security Options, page 6-1](#)
- [Manage Certificates and Certificate Trust Lists, page 6-1](#)
- [IPSEC Management, page 6-12](#)

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](#)
- [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 of the certificate under **Common Name**.
The **Certificate Details** window displays information about the certificate.
 - Step 4** To return to the **Certificate List** window, click **Close** on Certificate Details window.
-

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 under **Common Name**.
The **Certificate Details** window displays.
 - Step 4** Click **Download .PEM File** or **Download .DER File**.
 - 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 that 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 for Single Server and Multi-Server Certificate” procedure on page 6-7](#).

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 under **Common Name**.
The **Certificate Details** 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 Self-signed** or **Generate CSR**.
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**.



Note

After you regenerate certificates in 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 on 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 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.

Upload a Certificate or Certificate Trust List



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/Certificate chain**.
The **Upload Certificate/Certificate chain** dialog box opens.
- Step 3** Select the certificate name from the **Certificate Purpose** list.
- Step 4** Select the file to upload by doing one of the following steps:
- In the **Upload File** text box, click the **Browse** button and navigate to the file; then, click **Open**.
- Step 5** To upload the file to the server, click the **Upload File** button.
-

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

Single-server and Multi-server Certificates Overview

As the name suggests, Single-server certificate contains single FQDN which identifies the trust for that FQDN only. The single FQDN or domain is present in Subject Alternative Name (SAN) extensions. If there are multiple servers in a cluster, then the system requires the generation of an equal number of X.509 certificates, one for each server.

The system uses a multi-server certificate to identify the trust for multiple servers or domains or sub-domains. The SAN extensions of a multi-server certificate contain multiple FQDNs or domains.

**Note**

In telephony integration, multi-server SAN certificate is supported only with secure SIP integration. However, with secure SCCP integration, only single-server certificate is supported.


The following table describes the basic differences between single-server and multi-server certificates.

Table 6-2 Configuration Comparison of Certificates

Single-server certificate	Multi-server certificate
It contains a single FQDN or domain in either the CN field and/or SAN extensions.	It contains multiple FQDNs or domains present in SAN extensions.
The system uses a single certificate for each server in a cluster.	A single certificate identifies multiple servers.
The administrator regenerates the certificate and private key on each individual server in situations such as certificate expiry, private key compromise, etc.	Since this certificate covers only one public and private key pair common to all servers, it requires secure transfer of same private key to all the servers in a cluster along with the certificate. If the private key is compromised on any server, the certificate and private key needs to be regenerated for all the servers.
Generation of single server certificate can become an overhead for the administrator in a large cluster because the administrator needs to perform steps such as generate Certificate Signing Request (CSR), send CSR to CA for signing, upload signed certificate etc for each of the servers in the cluster.	There is less overhead for the administrator in managing multi-server certificates since he or she performs the steps only once on a given server, and the system distributes the associated private key and signed certificates to all the servers in the cluster.

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	Login to Cisco Unified Communications Operating System Administration window.	 <p>Note Cisco Unified Communications Operating System Administration allows the system administrator to select the distribution type, when generating a CSR for the individual certificate purposes that supports the multi-server option. The system automatically populates the CSR with the required SAN entries and displays the default SAN entries on the screen. On generating a multi-server CSR, the system automatically distributes that CSR to all the required servers in the cluster. Similarly, on upload of a multi-server CA signed certificate, the system automatically distributes that certificate to all the required servers in the cluster</p>
Step 2	Generate a CSR on the server.	See the “Generating a Certificate Signing Request for Single Server and Multi-Server Certificate” section on page 6-7.
Step 3	Download the CSR to your PC.	See the “Download a Certificate Signing Request for Single-Server Certificate and Multi-Server Certificate” section on page 6-8.
Step 4	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 6-9 for additional notes.
Step 5	Obtain the CA root certificate.	Get information about obtaining a root certificate from your CA. See “Obtaining Third-Party CA Certificates” section on page 6-9 for additional notes.
Step 6	Upload the CA root certificate to the server.	See the “Upload a Certificate” section on page 6-4.
Step 7	Upload the application certificate to the server.	See the “Upload a Certificate” section on page 6-4.
Step 8	Restart the services that are affected by the new certificate.	<p>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.</p> <p>Note If you updated the Tomcat certificate, you also must restart the Connection IMAP Server service in Cisco Unity Connection Serviceability.</p> <p>See the Cisco Unified Communications Manager <i>Serviceability Administration Guide</i> for information about restarting services.</p>

Generating a Certificate Signing Request for Single Server and Multi-Server Certificate

Procedure

Step 1 Select **Security > Certificate Management**.

The Certificate List window displays.

Step 2 Use the find control to filter the certificate list.

Step 3 Click **Generate CSR**.

The Generate Certificate Signing Request dialog box opens.

Step 4 From the Certificate Purpose drop-down list box, select the required certificate purpose.

Step 5 From the Distribution drop-down list box, select the required distribution list item.



Note The Multi-server (SAN) option is available only when you select tomcat from the Certificate Purpose drop-down list box. Click **Generate CSR**.



Note By default, the system populates the CN field with the server FQDN (or hostname). You can modify the value, if required. For self-signed certificate, the CN is not configurable.

Step 6 For Multi-server (SAN), additional domains can be added in **Additional Domain** field.

Step 7 From the Key Length drop-down list box, select 1024 or 2048.

Step 8 From the Hash Algorithm drop-down list box, select SHA1 or SHA256.

Step 9 Click **Generate** to generate a new CSR.



Note The new CSR that is generated for a specific certificate type overwrites any existing CSR for that type. The CSR is automatically distributed to all the required servers in the cluster.

Download a Certificate Signing Request for Single-Server Certificate and Multi-Server Certificate

To download a Certificate Signing Request, follow this procedure:

Procedure

Step 1 Select **Security > Certificate Management**.

The Certificate List window displays.

Step 2 From the list, click the Common Name of the entry with type 'CSR Only' and a Distribution value matching the Common Name.



Note For multi-server SAN certificate, click the Common Name of the entry with type 'CSR Only' and a Distribution value of 'Multi-Server (SAN)'.

The CSR Details window appears.

Step 3 Click **Download CSR**.

Step 4 After the CSR download completes, click **Close**.

You need to restart the tomcat service after configuring the Multi-server SAN certificate on both Publisher and Subscriber in a cluster. See the procedure below:

Procedure

-
- Step 1** Sign in to the Unity Connection server by using an SSH application.
- Step 2** Run the following CLI command to restart the Tomcat service:
- ```
utils service restart Cisco Tomcat
```
- 

## 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.

For all certificate types except CAPF, 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, 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 Key Usage:
Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication, IPSec End System
```

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, not the root CA.

You upload CA root certificates and application certificates by using the same Upload Certificate dialog box. When you upload a CA root certificate, choose the certificate name with the format *certificate type-trust*. When you upload an application certificate, choose the certificate name that only includes the certificate type. For example, choose **tomcat-trust** when you upload a Tomcat CA root certificate; choose **tomcat** when you upload a Tomcat application certificate.

## 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 6-3](#) for a description of the **Certificate Monitor Expiration** fields.
- Step 3** To save your changes, click **Save**.
- 

**Table 6-3** 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.<br><br><b>Note</b> For the system to send notifications, you must configure an SMTP host. |

## Certificate Revocation

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 Management**.  
The **Certificate List** window displays.
- Step 2** Check the Enable OCSP check box in the Online Certificate Status Protocol Configuration area.
- Step 3** Choose Use OCSP URI from Certificate if the certificate is configured with OCSP URI and that to be used to contact OCSP Responder.
- Step 4** Choose Use configured OCSP URI if external or configured URI is used to contact OCSP Responder. Enter the URI of the OCSP Responder, where certificate revocation status is verified, in the OCSP Configured URI field.
- Step 5** Check the check box for Enable Revocation Check to perform the revocation check.



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

- Step 6** Enter the Check Every value to check the periodicity of the certificate revocation status.
- Click Hours or Days to check the revocation status hourly or daily.
- Step 7** Click Save.



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



**Note** The Certificate revocation status check is performed only during upload of a Certificate or Certificate chain and the appropriate alarm will be raised if a certificate is revoked. The Cisco Certificate Expiry Monitor service must be restarted to ensure certificate revocation. Navigate to Cisco Unified Serviceability > Tool > Control Center - Network Services and restart the Cisco Certificate Expiry Monitor service.

## Generating IPSEC Certificate

To generate or regenerate the ipsec certificate on standalone or cluster, follow this procedure::

### Procedure

- 
- Step 1** Navigate to **Security > Certificate Management**.  
The **Certificate List** window displays.
- Step 2** Click Generate Self-signed > or > Generate CSR.
- Step 3** Select ipsec from the Certificate Purpose drop-down list.
- Step 4** Click Generate.
- After generating the certificate, ipsec and ipsec trust will be updated with the certificate for standalone or publisher server.

- Step 5** In case of subscriber server, follow Step 1 to Step 4 for generating ipsec certificate. After generating, download the ipsec certificate from subscriber server.
- Step 6** Navigate to Security > Certificate Management on subscriber server.
- Step 7** Click Upload Certificate/Certificate Chain.  
The Upload Certificate Trust List dialog box opens.
- Step 8** Select the ipsec-trust from the Certificate Purpose drop-down list.
- Step 9** Browse the certificate and click Upload.
- Step 10** After uploading the ipsec certificate to subscriber server, restart the below services first on publisher server and then subscriber server.
- Cisco DRF Master
  - Cisco DRF Local

## 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 6-4](#).



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

**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.                                                                                                                                                                                                                                                                                                                                                                                       |
| Authentication Method | Specifies the authentication method.                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Preshared Key         | Specifies the preshared key if you selected Pre-shared Key in the Authentication Name field.<br><br><b>Note</b> Pre-shared 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 pre-shared IPsec keys, so they are compatible with current versions of Cisco Unified Communications Manager. |
| 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 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"> <li>• TCP</li> <li>• UDP</li> <li>• Any</li> </ul>                                                                                                                                                                                                                                                                                                                                                        |
| Encryption Algorithm  | From the drop-down list, choose the encryption algorithm. Choices include <ul style="list-style-type: none"> <li>• DES</li> <li>• 3DES</li> </ul>                                                                                                                                                                                                                                                                                                                                     |
| Hash Algorithm        | Specifies the hash algorithm <ul style="list-style-type: none"> <li>• SHA1—Hash algorithm that is used in phase 1 IKE negotiation</li> <li>• MD5—Hash algorithm that is used in phase 1 IKE negotiation</li> </ul>                                                                                                                                                                                                                                                                    |

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

| Field               | Description                                                                                                                                                                                            |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ESP Algorithm       | From the drop-down list, choose the ESP algorithm. Choices include <ul style="list-style-type: none"> <li>• NULL_ENC</li> <li>• DES</li> <li>• 3DES</li> <li>• BLOWFISH</li> <li>• RIJNDAEL</li> </ul> |
| 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, 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: 2, 1, and 5.                                                                                                                  |
| 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. Check 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**.
-





## Software Upgrades

---

### Setting Up a Customized Log-on Message

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.

---





## 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.                                   |





---

## C

### certificates

- deleting [6-2](#)
- displaying [6-2](#)
- downloading [6-2](#)
- downloading a signing request [6-7](#)
- expiration monitor fields (table) [6-9](#)
- managing [6-1](#)
- monitoring expiration dates [6-9](#)
- regenerating [6-2](#)
- uploading [6-4](#)

### Certificate Trust List

*See* CTL

### cluster nodes

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

### CTL

- managing [6-1](#)
- uploading [6-4](#)

---

## E

Ethernet settings [4-1](#)

---

## H

### hardware, status

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

---

## I

### installed software

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

### IPSec

- changing policy [6-11](#)
- displaying policy [6-11](#)
- management [6-9](#)
- policy fields (table) [6-10](#)
- setting up new policy [6-9](#)

---

## L

### logging in

- overview [2-1](#)

---

## N

### network status

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

### nodes, cluster

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

NTP server settings [4-2](#)

---

## O

### operating system

- hardware status
  - fields (table) [3-2](#)
  - procedure [3-2](#)
- introduction [1-1](#)

logging in [2-1](#)  
 network status fields (table) [3-3](#)  
 restart [5-1](#)

---

## P

ping [8-1](#)  
 publisher settings [4-2](#)

---

## R

remote support  
   setting up [8-2](#)  
   status fields (table) [8-2](#)  
 restart  
   current version [5-1](#)

---

## S

services  
   ping [8-1](#)  
   remote support  
     overview [8-2](#)  
     setting up [8-2](#)  
 settings  
   Ethernet  
     fields (table) [4-2](#)  
     procedure [4-1](#)  
   IP [4-1](#)  
   NTP servers [4-2](#)  
   publisher [4-2](#)  
   SMTP [4-3](#)  
   time [4-4](#)  
 shutdown, operating system [5-2](#)  
 SMTP settings [4-3](#)  
 software  
   installed  
     fields (table) [3-4](#)

  procedure [3-3](#)  
 status  
   hardware  
     fields (table) [3-2](#)  
     procedure [3-2](#)  
   network  
     fields (table) [3-3](#)  
   system  
     fields (table) [3-4](#)  
     procedure [3-4](#)  
 system  
   shutdown [5-2](#)  
   status  
     fields (table) [3-4](#)  
     procedure [3-4](#)

---

## T

time settings [4-4](#)

---

## V

version, restart [5-1](#)