Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection

Release 9.x
Published May 2012

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

Text Part Number:

Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection

CONTENTS

Preface

This preface contains the following sections:

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 Unifed Communications Solutions*.

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

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 `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
	This pointer highlights an important line of text in an example.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords, are in angle brackets.

Notes use the following conventions:

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

Timesavers use the following conventions:

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

Tips use the following conventions:

Tip Means *the information contains useful tips.*

Cautions use the following conventions:

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

Warnings use the following conventions:

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

Related Documentation

For descriptions and URLs of Cisco Unity Connection documentation on Cisco.com, see the *Documentation Guide for Cisco Unity Connection Release 9.x*. The document is shipped with Cisco Unity Connection and is available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/roadmap/9xcucdg.html.

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

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.

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

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

- Check software and hardware status.
- Check and update IP addresses.
- Ping other network devices.
- Manage NTP servers.
- Upgrade system software and options.
- Manage server security, including IPSec and certificates
- Manage remote support accounts
- Restart the system.

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

Browser Requirements

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

You can access Cisco Unified Communications Operating System with this browser...	...if you use one of these operating systems
Microsoft Internet Explorer 8	• Microsoft XP service pack 3 • Microsoft Vista service pack 2 or later service pack • Microsoft Windows 7 with the latest service pack
Mozilla Firefox 3.x	• 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 Unifed Communications Solutions*.

CHAPTER 2

Log in to Cisco Unified Communications Operating System Administration

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

This chapter comprises the following sections:

Logging in to Cisco Unified Communications Operating System Administration

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 Administrator and Security Passwords

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

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

Caution The security password on all nodes in a cluster must match. Change the security password on all machines, or the cluster nodes will not communicate.

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

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

Procedure

Step 1 Log in to the system with the following username and password:

- Username: **pwrecovery**
- Password: **pwreset**

The Welcome to platform password reset window displays.

Step 2 Press any key to continue.

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

Step 4 Press any key to continue.

The system tests to ensure that you have removed the CD or DVD from the disk drive.

Step 5 Insert a valid CD or DVD into the disk drive.

Note For this test, you must use a data CD, not a music CD.

The system tests to ensure that you have inserted the disk.

Step 6 After the system verifies that you have inserted the disk, you get prompted to enter one of the following options to continue:

- Enter **a** to reset the administrator password.
- Enter **s** to reset the security password.
- Enter **q** to quit.

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

Step 8 Reenter the new password.

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

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

CHAPTER 3

Status and Configuration

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

Cluster Nodes

To view information on the nodes in the cluster, follow this procedure:

Procedure

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

The Cluster Nodes window displays.

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

Table 3-1 Cluster Nodes Field Descriptions

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

Hardware Status

To view the hardware status, follow this procedure:

Procedure

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

The Hardware status window displays.

Step 2 For descriptions of the fields on the Hardware Status window, see Table 3-2.

Table 3-2 Hardware Status Field Descriptions

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

Network Configuration

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

To view the network status, follow this procedure:

Procedure

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

The Network Settings window displays.

Step 2 See Table 3-3 for descriptions of the fields on the Network Settings window.

Table 3-3 Network Configuration Field Descriptions

Field	Description
Ethernet Details	
DHCP	Indicates whether DHCP is enabled for Ethernet port 0.
Status	Indicates whether the port is Up or Down for Ethernet ports 0 and 1.
IP Address	Shows the IP address of Ethernet port 0 [and Ethernet port 1 if Network Fault Tolerance (NFT) is enabled].
IP Mask	Shows the IP mask of Ethernet port 0 (and Ethernet port 1 if NFT is enabled).
Link Detected	Indicates whether an active link exists.
Queue Length	Displays the length of the queue.
MTU	Displays the maximum transmission unit.
MAC Address	Displays the hardware address of the port.
Receive Statistics (RX)	Displays information on received bytes, packets, and errors, as well as dropped and overrun statistics.
Transmit Statistics (TX)	Displays information on transmitted bytes, packets, and errors, as well as dropped, carrier, and collision statistics.
DNS Details	
Primary	Displays the IP address of the primary domain name server.
Secondary	Displays the IP address of the secondary domain name server.
Options	Displays the configured DNS options.
Domain	Displays the domain of the server.
Gateway	Displays the IP address of the network gateway on Ethernet port 0.

Installed Software

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

Procedure

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

The Software Packages window displays.

Step 2 For a description of the fields on the Software Packages window, see Table 3-4.

Table 3-4 Software Packages Field Descriptions

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

System Status

To view the system status, follow this procedure:

Procedure

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

The System Status window displays.

Step 2 See Table 3-5 for descriptions of the fields on the Platform Status window.

Table 3-5 System Status Field Descriptions

Field	Description
Host Name	Displays the name of the Cisco MCS host where Cisco Unified Communications Operating System is installed.
Date	Displays the date and time based on the continent and region that were specified during operating system installation.
Time Zone	Displays the time zone that was chosen during installation.
Locale	Displays the language that was chosen during operating system installation.
Product Version	Displays the operating system version.
Platform Version	Displays the platform version.
Uptime	Displays system uptime information.
CPU	Displays the percentage of CPU capacity that is idle, the percentage that is running system processes, and the percentage that is running user processes.

Table 3-5 System Status Field Descriptions (continued)

Field	Description
Memory	Displays information about memory usage, including the amount of total memory, free memory, and used memory in KBytes.
Disk/active	Displays the amount of total, free, and used disk space on the active disk.
Disk/inactive	Displays the amount of total, free, and used disk space on the inactive disk.
Disk/logging	Displays the amount of total, free, and disk space that is used for disk logging.

IP Preferences

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

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

To access the IP Preferences window, follow this procedure.

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, choose **Show > IP Preferences**.

The IP Preferences window displays. Records from an active (prior) query may also display in the window.

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- Specify the appropriate search text, if applicable.

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

Step 3 Click **Find**.

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

For a description of the IP Preferences fields, see

Table 3-6 IP Preferences Field Descriptions

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

CHAPTER 4

Settings

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

This chapter contains the following sections:

IP Settings

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

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" chapter in the applicable *Reconfiguration and 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 Connection server, see the "Renaming Cisco Unity Connection Servers" chapter in the applicable *Reconfiguration and Upgrade Guide for* Cisco Unity Connection at http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.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

Note The settings detailed below are applicable to Cisco Unity Connection release 9.0. IPv6 is not supported in earlier versions of Cisco Unity Connection.

The Ethernet IPv6 Configuration Settings page allows you to enable IPv6, and to determine a method for obtaining the IP addresses.

To view or change the IPv6 settings, follow this procedure:

Procedure

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

Step 2 To modify the ethernet IPv6 settings, enter the new values in the applicable fields. For a description of the fields on the Ethernet IPv6 Configuration Settings window, see Table 4-2.

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

Table 4-2 Ethernet IPv6 Configuration Fields and Descriptions

Field	Description
Enable IPv6	Check this check box to enable IPv6.
Address Source	Select one of the following: • Router Advertisement—Select this option if your network router is configured to advertise the network prefix to servers on the network. • DHCP—Select this option to use the DHCPv6 protocol to assign addresses to your server (note that you must be running a DHCPv6 server on the network to provide the addresses). • Manual Entry—Select this option if you want to enter an address manually in the IPv6 Address field. **Note** Cisco recommends that the Cisco Unity Connection server use a static non-link-local IPv6 address. If the server obtains the IPv6 address from the DHCPv6 server or via stateless address autoconfiguration, ensure that the server only obtains one non-link-local IPv6 address from the DHCPv6 server. **Note** Unless you specify Manual Entry, the IPv6 Address and Subnet Mask fields remain read only.
IPv6 Address	If you chose Manual Entry as the Address Source, enter an IPv6 address. For example, enter: 2001:0DB8:BBBB:CCCC:0987:65FF:FE01:2345
Subnet Mask	If you chose Manual Entry as the Address Source, enter a prefix length (from 0 through 128), indicating the number of bits in the address that correspond to the prefix of the network. For example, enter: 64
Update with Reboot	Check this check box if you want an immediate reboot of the server to occur when you save the updated settings. **Note** For the IPv6 settings to take effect, you must reboot the system.

Publisher Settings

This feature is only applicable if Cisco Unified Communications Manager is installed alone on the server.

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:

Caution If Connection is installed on a virtual machine, changing which NTP server is the first server in the list also changes the calculated value of the license MAC and invalidates the Connection license.

For information on getting replacement Connection licenses, see the "Managing Licenses in Cisco Unity Connection" chapter of the *System Administration Guide for Cisco Unity Connection 9.x* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

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

Procedure

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

The NTP Server Settings window displays.

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

Note To avoid potential compatibility, accuracy, and network jitter problems, the external NTP servers that you specify for the primary node should be NTP v4 (version 4). If you are usingIPv6 addressing, external NTP servers must be NTP v4.

- 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.

Caution If Connection is installed on a virtual machine, changing the SMTP hostname or IP address also changes the calculated value of the license MAC and invalidates the Connection license.

For information on getting replacement Connection licenses, see the "Managing Licenses in Cisco Unity Connection" chapter of the *System Administration Guide for Cisco Unity Connection 9.x* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

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 4-3 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.

CHAPTER 5

System Restart

This section provides procedures for using the following restart options:

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 Unifed Communications Solutions*.

CHAPTER 6

Security

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

Set Internet Explorer Security Options

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:

- 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

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

Procedure

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

The Certificate List window displays.

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

Step 3 Click the file name of the certificate.

The Certificate Configuration window displays.

Step 4 Click **Download**.

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

Delete and Regenerate a Certificate

These sections describe 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" 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 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**.

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.
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 6-7.
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 6-8 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 6-8 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.

	Task	For More Information
Step 7	If you updated the certificate for CAPF or Cisco Unified Communications Manager, generate a new CTL file.	See the *Cisco Unified Communications Manager Security Guide*.
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. **Note** If you updated the Tomcat certificate, you also must restart the Connection IMAP Server service in Cisco Unity Connection Serviceability. See the Cisco Unified Communications Manager *Serviceability Administration Guide* 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 no longer displays 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.

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.

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

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. **Note** 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.

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

Field	Description
Protocol	Specifies the specific protocol, or Any: • TCP • UDP • Any
Encryption Algorithm	From the drop-down list, choose the encryption algorithm. Choices include • DES • 3DES
Hash Algorithm	Specifies the hash algorithm • 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 • 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, 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**.

CHAPTER 7

Software Upgrades

For information on upgrading Cisco Unity Connection to the shipping version, see the applicable chapter in the *Reconfiguration and Upgrade Guide for Cisco Unity Connection Release 9.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/upgrade/guide/9xcucrugx.html.

For information on installing Cisco Unity Connection languages, see the "Adding Languages to the Cisco Unity Connection 9.x System" chapter of the *Reconfiguration and Upgrade Guide for Cisco Unity Connection Release 9.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/upgrade/guide/9xcucrugx.html.

Setting Up a Customized Log-on Message

You can upload a text file that contains a customized log-on message that appears in Cisco Unified Communications Operating System Administration, Cisco Unified Serviceability, Disaster Recovery System Administration, Cisco Unity Connection Administration, Cisco Unity Connection Serviceability Administration, Cisco Personal Communications Assistant (CPCA) and the command line interface.

To upload a customized log-on message, follow this procedure:

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to Software **Upgrades > Customized Logon Message**.

The Customized Logon Message window displays.

Step 2 To choose the text file that you want to upload, click **Browse**.

Step 3 Click **Upload File**.

Note You cannot upload a file that is larger than 10kB.

The system displays the customized log-on message.

Step 4 To revert to the default log-on message, click **Delete**.

Your customized log-on message gets deleted, and the system displays the default log-on message.

CHAPTER 8

Services

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

This chapter contains the following sections:

Ping

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

To ping another system, follow this procedure:

Procedure

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

The Ping Remote window displays.

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

Step 3 Enter the ping interval in seconds.

Step 4 Enter the packet size.

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

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

Step 6 Choose whether you want to validate IPSec.

Step 7 Click **Ping**.

The Ping Remote window displays the ping statistics.

Remote Support

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

The remote support process works like this:

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

To set up remote support, follow this procedure:

Procedure

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

The Remote Access Configuration window displays.

Step 2 Enter an account name for the remote account in the **Account Name** field.

The account name must comprise at least six-characters that are all lowercase, alphabetic characters.

Step 3 Enter the account duration, in days, in the **Account Duration** field.

The default account duration specifies 30 days.

Step 4 Click **Save**.

The Remote Support Status window displays. For descriptions of fields on the Remote Support Status window, see Table 8-1.

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

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

Table 8-1 Remote Support Status Fields and Descriptions

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

INDEX

O

P

R

S

T

V