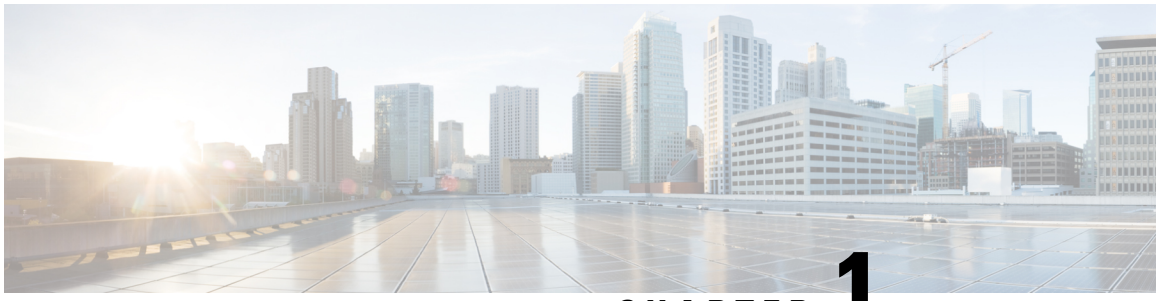
Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection Release 11.x

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

CONTENTS



CHAPTER 1

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.

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 with 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 "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 use for sending e-mail notifications.

For more information, see "Settings"

From the **Settings > Version** window**,** you can select 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 select 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 "Version Settings".

Security Configuration

The operating system security options enable you to manage security certificates and Secure Internet Protocol (IPSec). From the **Security** menu, you can select 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 "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 with 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 "Software Upgrades".

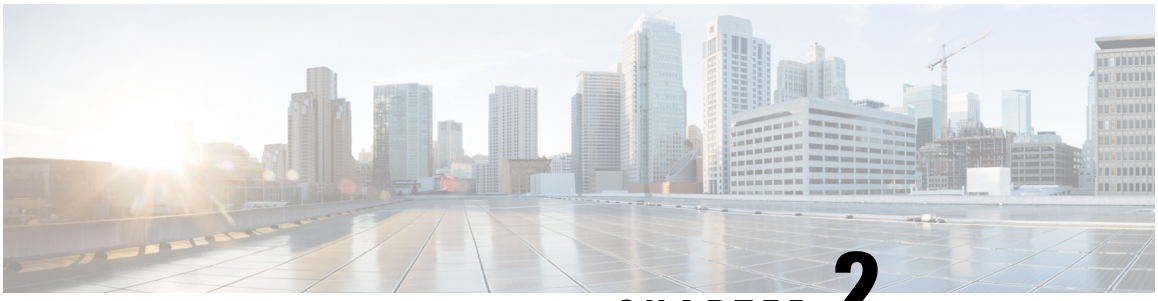
The application provides the following operating system utilities:

- 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 "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.

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.

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, select **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 with 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, otherwise the cluster nodes does 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.

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:

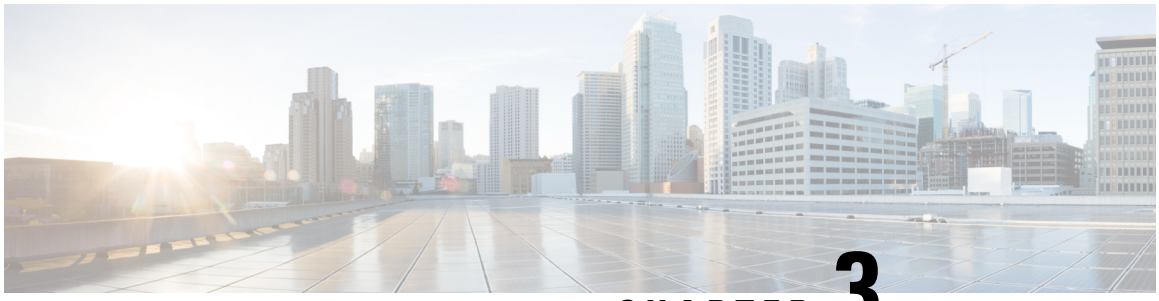
- Enter **a** to reset the administrator password.
- Enter **s** to reset the security password.
- Enter **q** to quit.

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.



CHAPTER 3

Status and Configuration

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

Cluster Node

To view information on the nodes in the cluster, follow this 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 1: cluster nodesfields (table)nodes, clusterfields (table)Cluster Nodes Field Descriptions.

Table 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:

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 2: hardware, statusfields (table)statushardwarefields (table)operating systemhardware statusfields (table)Hardware Status Field Descriptions

Table 2: Hardware Status Field Descriptions

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

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:

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: statusnetworkfields (table)network statusfields (table)operating systemnetwork status fields (table)Network Configuration Field Descriptions for descriptions of the fields on the Network Settings window.

Table 3: Network Configuration Field Descriptions

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

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 4: softwareinstalledfields (table)installed softwarefields (table)Software Packages Field Descriptions.

Table 4: Software Packages Field Descriptions

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

System Status

To view the system status, follow this 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 5: statussystemfields (table)systemstatusfields (table)System Status Field Descriptions for descriptions of the fields on the Platform Status window.

Table 5: System Status Field Descriptions

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

Field	Description
Uptime	Displays system uptime information.
CPU	Displays the percentage of CPU capacity that is idle, the percentage that is running system processes, and the percentage that is running user processes.
Memory	Displays information about memory usage, including the amount of total memory, free memory, and used memory in KBytes.
Disk/active	Displays the amount of total, free, and used disk space on the active disk.
Disk/inactive	Displays the amount of total, free, and used disk space on the inactive disk.
Disk/logging	Displays the amount of total, free, and disk space that is used for disk logging.

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.

Step 1 From the Cisco Unified Communications Operating System Administration window, select **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.

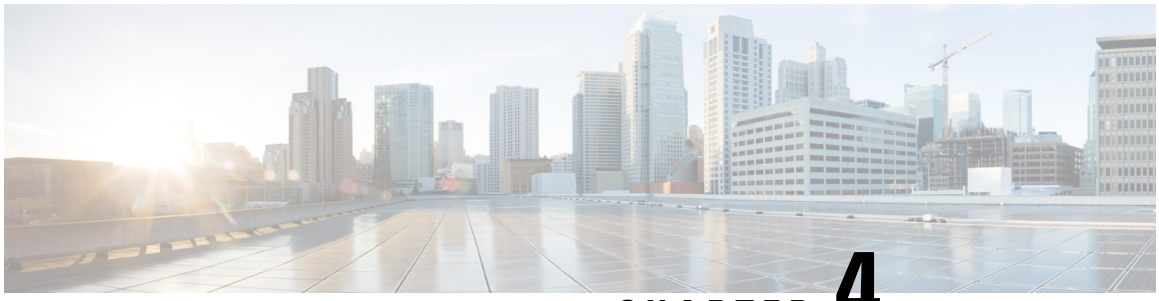
Step 3 Click **Find**.

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 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

Overview

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

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.

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.

Caution 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* Unity Connection at http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html.

Caution For information on changing the host name of a Unity Connection 11.x server refer, *Install, Upgrade, and Maintenance Guide for* Cisco Unity Connection 11x at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/install_upgrade/guide/b_11xcuciumg.html.

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 7: settingsEthernetfields (table)Ethernet Configuration Fields and Descriptions.

Table 7: 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 and later. 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:

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 8: 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.
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:

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

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**.

  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, select **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:

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:

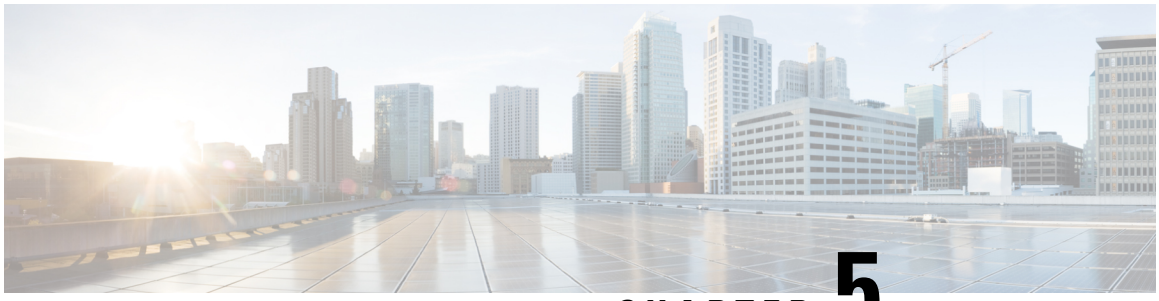
Note Before you can manually configure the server time, you must delete any NTP servers that you have configured. See the NTP Servers for more information.

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

Version Settings

Version Settings

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 with the software version on the inactive partition, follow this procedure:

Caution This procedure causes the system to restart and become temporarily out of service.

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.

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.

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.

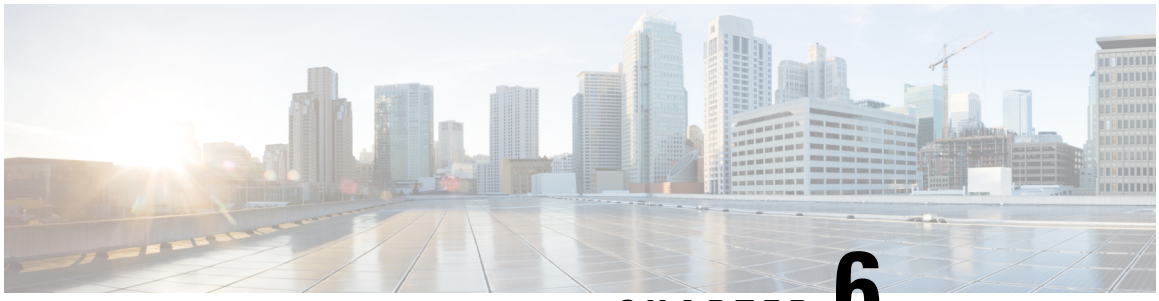
Step 2 To shut down the system, click **Shutdown** or, to stop the operation, click **Cancel**.

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

Note The hardware may require several minutes to power down.

Alternate Procedure

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

Security

Set Internet Explorer Security Options

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

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:

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

Display Certificates

To display existing certificates, follow this 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. The SHA-512 checksum value is also displayed for the certificate to check the file integrity.

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:

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

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 select 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.

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.

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 Select a certificate name from the Certificate Name list. For a description of the certificate names that display, see Table 9: Certificate Names and Descriptions.

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. For information on performing a backup, refer to the *Install, Upgrade and Maintenance Guide for Cisco Unity Connection*.

Table 9: Certificate Names and Descriptions

Name	Description
tomcat	This self-signed root certificate gets generated during installation for Unity Connection server and the certificate type is RSA key based.
ipsec	This self-signed root certificate gets generated during installation for IPSec connections with MGCP and H.323 gateways.
tomcat-ECDSA	This self-signed root certificate gets generated during installation for Unity Connection server and the certificate type is EC key based. **Note** CallManager is used only in the naming convention of the certificate, however, the certificate generated is specific to Unity Connection Server.

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

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

Table 10: 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.	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
Step 2	Generate a CSR on the server.	See the Generating a Certificate Signing Request.
Step 3	Download the CSR to your PC.	See the Downloading a Certificate Signing Request.
Step 4	Use the CSR to obtain an application certificate from a CA.	Get information about obtaining application certificates from your CA. See Third-Party CA Certificates for additional notes.
Step 5	Obtain the CA root certificate.	Get information about obtaining a root certificate from your CA. See Third-Party CA Certificates for additional notes.
Step 6	Upload the CA root certificate to the server.	See the Upload Trust Certificate.
Step 7	Upload the application certificate to the server.	See the Upload Application Certificate.

	Task	For More Information
Step 8	Restart the services that are affected by the new certificate.	For all certificate types, restart the corresponding service: • If you update Tomcat certificate, you must restart the Cisco tomcat service, Connection IMAP Server, Cisco Dirsync service, Connection Jetty service, SMTP service and Connection Conversation Manager service. • If you update tomcat-ECDSA certificate, you must also restart the Connection Conversation Manager service. See the Cisco Unified Communications Manager Serviceability Administration Guide for information about restarting services.

Generating a Certificate Signing Request

To regenerate a certificate signing request, follow this 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 or tomcat-ECDSA from the Certificate Purpose drop-down list box. Click **Generate CSR**.

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 Subject Alternate Names field.

Step 7 From the Key Length drop-down list box, select value as per the certificate purpose.

- If tomcat or ipsec is the certificate purpose, select 1024, 2048, 3072, or 4096.
- If tomcat-ECDSA is the certificate purpose, select 256, 384 or 521.

Step 8 From the Hash Algorithm drop-down list box, select as per the certificate purpose.

- If tomcat or ipsec is the certificate purpose, select SHA1 or SHA256.
- If tomcat-ECDSA is the certificate purpose, select SHA384 SHA512.

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.

Downloading a Certificate Signing Request

To download a Certificate Signing Request, follow this 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:

Step 1 Sign in to the Unity Connection server with an SSH application.

Step 2 Run the following CLI command to restart the Tomcat service:

utils service restart Cisco Tomcat

Third-Party CA Certificates

To use an application certificate that a third-party CA issues, you must obtain both the signed application certificate and the CA root certificate from the CA or PKCS#7 Certificate Chain (DER format), which contains both the application certificate and CA certificates. Retrieve information about obtaining these certificates from your CA. The process varies among CAs.

Cisco Unified Operating System Administration generates CSRs in PEM encoding format. The system accepts certificates in DER and PEM encoding formats and PKCS#7 Certificate chain in PEM format. For all certificate types, you must obtain and upload a CA root certificate and an application certificate on each node.

Cisco Unified Operating System Administration 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, shown as follows:

```
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Key Usage:
Digital Signature, Key Encipherment, Data Encipherment
```

Note You can generate a certificate signing request (CSR) for your certificates and have them signed by a third party CA with a SHA256 signature. You can then uploads this signed certificate back to Cisco Unified Operating System Administration, allowing for Tomcat and other certificates to be support SHA256.

Upload Trust Certificate

To upload a trust certificate, follow this procedure:

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

The Certificate List window displays.

Step 2 Click **Upload Certificate/Certificate Chain**.

The Upload Certificate Trust List dialog box opens.

Step 3 Select the certificate name from the **Certificate Purpose** drop-down list.

Step 4 Enter the name of the CA root certificate in the **Description** text box.

Step 5 Select the file to upload, click the **Browse** button and navigate to the file; then, click **Open**.

Step 6 To upload the file to the server, click the **Upload** button.

Note In case of trust certificate, the system automatically distributes the certificate to other nodes of the cluster.

Upload Application Certificate

Cisco Unified Communications Operating System supports certificates that a third-party CA issues with PKCS#10 Certificate Signing Request (CSR).

Step 1 Generate a CSR on the server.

Step 2 Download the CSR to your PC.

Step 3 Use the CSR to obtain an application certificate from a CA or PKCS#7 format certificate chain, which may contain application certificate along with CA certificate.

Step 4 Obtain the CA certificate or certificate chain.

To upload tomcat application certificate, select **tomcat** from Certificate Purpose list.

To upload ipsec application certificate, select **ipsec** from Certificate Purpose list.

To upload tomcat-ECDSA application certificate, select **tomcat-ECDSA** from Certificate Purpose list.

Step 5 Select the certificate from the **Certificate Purpose** drop-down list.

Step 6 Select the file to upload, click the **Browse** button and navigate to the file; then, click **Open**.

Step 7 To upload the file to the server, click the **Upload** button.

Note The system does not distribute application 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. However, in case of SAN certificate, the system distributes the certificates to other cluster nodes automatically.

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:

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 11: certificatesexpiration monitor fields (table)Certificate Monitor Field Descriptions for a description of the Certificate Monitor Expiration fields.

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

Table 11: 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.

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:

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:

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 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:

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 Do not modify or create IPSec policies during an upgrade because any changes that you make to an IPSec policy during a system upgrade gets lost.

Caution IPSec affects the performance of your system, especially with encryption.

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 12: IPSecpolicy fields (table)IPSEC Policy and Association Field Descriptions.

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

Table 12: IPSEC Policy and Association Field Descriptions

Field	Description
Policy Group Name	Specifies the name of the IPSec policy group. The name can contain only letters, digits, and hyphens.
Policy Name	Specifies the name of the IPSec policy. The name can contain only letters, digits, and hyphens.

Field	Description
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.
Protocol	Specifies the specific protocol, or Any: • TCP • UDP • Any
Encryption Algorithm	From the drop-down list, select 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

Field	Description
ESP Algorithm	From the drop-down list select the ESP algorithm. Choices include • NULL_ENC • DES • 3DES • BLOWFISH • RIJNDAEL
Phase One Life Time	Specifies the lifetime for phase One, IKE negotiation, in seconds.
Phase One DH	From the drop-down list, select 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, select 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 Do not modify or create IPSec policies during an upgrade because any changes made to an IPSec policy during a system upgrade, gets lost.

Caution IPSec affects the performance of your system, especially with encryption.

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

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 with 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**.

Bulk Certificate Management

To support the Extension Mobility Cross Cluster (EMCC) feature, the system allows you to execute a bulk import and export operation to and from a common SFTP server that has been configured by the cluster administrator. For more information about using Bulk Certificate Management, see the *Cisco Unified Communications Manager Security Guide.*

For Bulk Certificate Management, use the following procedure:

Step 1 Navigate to **Security** > **Bulk Certificate Management**. The Bulk Certificate Management window displays.

Step 2 Enter the appropriate information on the Bulk Certificate Management window. For a description of the fields on this window, see Table 13: Bulk Certificate Management Field Description.

Step 3 To save the values you entered, click **Save**

Step 4 To export certificates, click **Export**. The Bulk Certificate Export popup window displays.

Step 5 From the drop-down menu, choose the type of certificate you want to export:

- Tomcat
- TFTP
- All

Step 6 Click **Export**.

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

Table 13: Bulk Certificate Management Field Description

Field	Description
IP Address	Enter the IP address of the common server where you want to export the certificates

Field	Description
Port	Enter the port number. Default: 22
User ID	Enter the User ID you want to use to log into the server.
Password	Enter the appropriate password.
Directory	Enter a directory on the server where you want to save the certificates. Example: /users/cisco.

Session Management

Platform Administrator is allowed to terminate the active web sessions of a user or administrator for the following web interfaces of Cisco Unity Connection:

- Cisco Unity Connection Administration
- Cisco Unity Connection Serviceability
- Cisco Personal Communications Assistant
- Cisco Unity Connection Web Inbox
- Cisco Unity Connection SRSV

To terminate the active web sessions of a user or administrator, use the following procedure:

Step 1 Navigate to **Security** > **Session Management**. The Session Management window displays.

Step 2 On the Session Management window, enter the alias of the active logged-in user in **User ID** field.

Step 3 Select **Terminate Session** to terminate the active web sessions of the user.

Note In case of a cluster, you must terminate the web sessions for each node of the cluster.

Note Session termination is not applicable for platform users. To terminate the active web sessions, platform user must logout the sessions or wait until the sessions are timed out.

Cipher Management

Cisco Unity Connection supports **Cipher Management** that allows administrator to control set of ciphers that are used for every TLS and SSH connection. You can configure the recommended ciphers for various secure interfaces of Cisco Unity Connection.

TLS Interfaces

You can configure ciphers for the TLS interfaces mentioned in below.

Interfaces	Description
All TLS	You can configure the ciphers for all supported TLS interfaces of Cisco Unity Connection. Example: SIP, SCCP, HTTPS, Jetty, SMTP, LDAP and IMAP inerfaces.
HTTPS TLS	You can configure the ciphers for all Cisco Tomcat interfaces of Cisco Unity Connection.
SIP TLS	You can configure the ciphers for SIP interfaces of Cisco Unity Connection. Example: Telephony User Interface to support secure SIP call in Unity Connection. **Note** Cipher configuration for SIP interface is not supported for unrestricted version of Cisco Unity Connection.

SSH Interfaces

You can configure ciphers and algorithm for the SSH interfaces mentioned below.

Interfaces	Description
SSH Ciphers	You can configure the cipher for SSH interfaces of Cisco Unity Connection.
SSH Key Exchange	You can configure the SSH Key Exchange algorithm for SSH interfaces of Cisco Unity Connection.
SSH MAC	You can configure the SSH MAC algorithm for SSH interfaces of Cisco Unity Connection.

For information on recommended ciphers, see the "Cipher Management" section in the *Security Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Configuring Cipher String

To configure the cipher string for TLS and SSH interfaces, do the following procedure:

Step 1 Navigate to **Security** > **Cipher Management**. The Cipher Management page appears.

Step 2 On the Cipher Management page, enter the cipher string in **Cipher String** field for **All TLS**, **HTTPS TLS** and **SIP TLS** interfaces.

Note The cipher string configured either for **HTTPS TLS** or **SIP TLS** interface overrides the cipher string configured in ALL TLS field.

Note The ciphers configured on the **Cipher Management** page will override the cipher configuration of **Edit General Configuration** page. Hence it is recommended to use **Cipher Management** page for configuring the ciphers for TLS and HTTPS interfaces.

Step 3 Enter the cipher string in **Cipher String** field for SSH Ciphers.

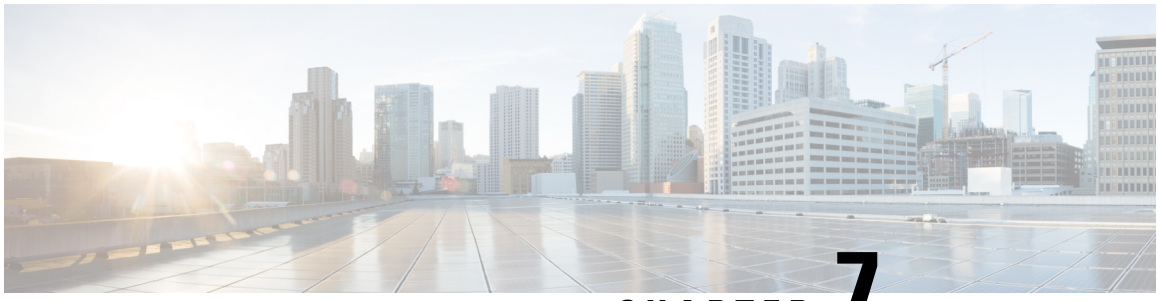
Step 4 Enter the algorithm string in **Algorithm String** field to configure the key algorithm for SSH Key Exchange.

Step 5 Enter the algorithm string in **Algorithm String** field to configure the MAC algorithm for SSH MAC.

Step 6 Select **Save**.

After saving the page, you must do the following:

- Reboot both nodes in the cluster for successful configuration of ciphers on **All TLS**, **SSH Ciphers**, **SSH Key Exchange** and **SSH MAC** interfaces.
- Restart the Cisco Tomcat service for successful configuration of ciphers on **HTTPS TLS** interface.
- Restart the Connection Conversation Manager service for successful configuration of ciphers on **SIP TLS** interface.



CHAPTER 7

Software Upgrades

For information on upgrading Cisco Unity Connection to the shipping version, see the"Upgrading Cisco Unity Connection" chapter in the *Install, Upgrade and Maintain guide for Cisco Unity Connection Release 11.x* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/install_upgrade/guide/b_11xcuciumg.html.

For information on installing Cisco Unity Connection languages, see the "Maintaining Cisco Unity Connection Server" chapter in the *Install, Upgrade and Maintain guide for Cisco Unity Connection Release 11.x* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/install_upgrade/guide/b_11xcuciumg.html .

• Software Upgrades, on page 41

Software Upgrades

For information on upgrading Cisco Unity Connection to the shipping version, see the"Upgrading Cisco Unity Connection" chapter in the *Install, Upgrade and Maintain guide for Cisco Unity Connection Release 11.x* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/install_upgrade/guide/b_11xcuciumg.html.

For information on installing Cisco Unity Connection languages, see the "Maintaining Cisco Unity Connection Server" chapter in the *Install, Upgrade and Maintain guide for Cisco Unity Connection Release 11.x* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/install_upgrade/guide/b_11xcuciumg.html .

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 with 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 "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 "Services".

Device Load Management

For information on Device Load Management, see the *Install, Upgrade and Maintain guide for Cisco Unity Connection Release 11.x* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/install_upgrade/guide/b_11xcuciumg.html.

Setting Up a Customized Log-on Message

To upload a customized log-on message, follow this 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 Click **Browse** to select the text file (.txt) that contains the log-on message, which you want to display.

Step 3 Click **Upload File**.

The customized log-on message will be displayed on the login screen as well as home screen of the following interfaces of Unity Connection:

- Cisco Unity Connection Administration
- Cisco Unity Connection Serviceability
- Cisco Unified Operating System Administration
- Cisco Unified Serviceability
- Disaster Recovery System Administration
- Cisco Prime License Manager
- Cisco Personal Communication Assistant
- Real-Time Monitoring Tool
- Command Line Interface

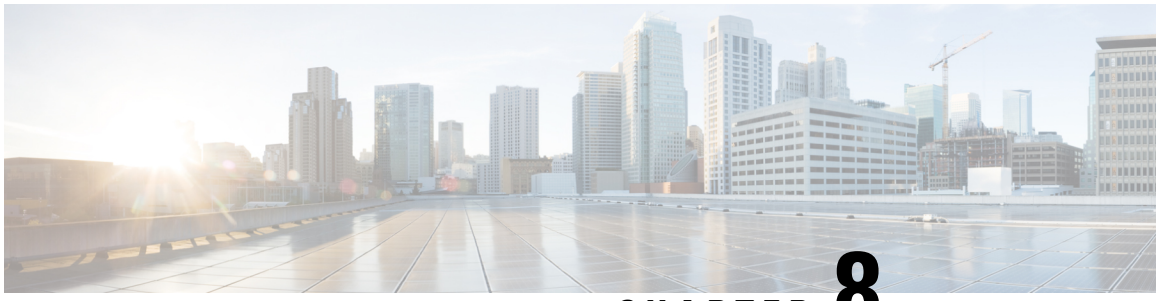
Note You cannot upload a file that is larger than 10kB.

Step 4 *(Optional)* Check the **Require User Acknowledgment** check box to display the customized log-on message in pop-up window as well whenever a user accesses the above interfaces along with Web Inbox. To successfully log in to the interface, user must explicitly acknowledge the pop-up window by clicking **OK**.

Note In case of Web Inbox, customized log-on message is displayed only in pop-up window

Step 5 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

Services

Overview

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

Ping

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

To ping another system, follow this 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 Select whether you want to validate IPSec.

Step 7 Click **Ping**.

The Ping Remote window displays the ping statistics.

Setting Up 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:

Step 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.

Step 2 When the remote support account is set up, a pass phrase gets generated.

Step 3 The customer calls Cisco support and provides the remote support account name and pass phrase.

Step 4 Cisco support enters the pass phrase into a decoder program that generates a password from the pass phrase.

Step 5 Cisco support logs into the remote support account on the customer system with the decoded password.

Step 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:

Step 7 From the Cisco Unified Communications Operating System Administration window, navigate to **Services** > **Remote Support**.

The Remote Access Configuration window displays.

Step 8 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 9 Enter the account duration, in days, in the **Account Duration** field.

The default account duration specifies 30 days.

Step 10 Click **Save**.

The Remote Support Status window displays. For descriptions of fields on the Remote Support Status window, see Table 14: remote supportstatus fields (table)Remote Support Status Fields and Descriptions.

Step 11 To access the system with the generated pass phrase, contact your Cisco personnel.

Step 12 To delete the remote access support account, click the **Delete** button.

Table 14: 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