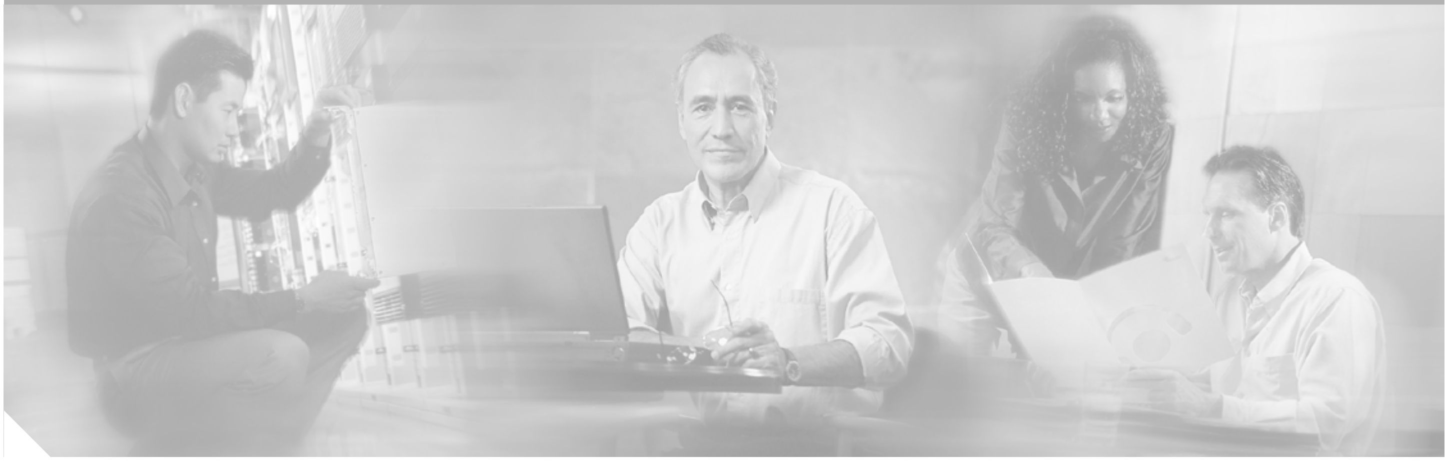

Cisco Unified Communications Operating System Administration Guide

For Cisco Unified Presence Server Release 1.0(3)

Corporate 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: 408 526-4100

Text Part Number: OL-11803-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)

Cisco Unified Communications Operating System Administration Guide
© 2006 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

This preface describes the purpose, audience, organization, and conventions of this guide, and provides information on how to obtain related documentation.

The preface covers these topics:

Purpose

The *Cisco Unified Communications Operating System Administration Guide* provides information about using the Cisco Unified Communications Operating System graphical user interface (GUI) and the command line interface (CLI) to perform many common system- and network-related tasks.

Audience

The *Cisco Unified Communications Operating System Administration Guide* provides information for network administrators who are responsible for managing and supporting the Cisco Unified Presence Server system. Network engineers, system administrators, or telecom engineers use this guide to learn about, and administer, the operating system features. This guide requires knowledge of telephony and IP networking technology.

Organization

The following table shows how this guide is organized:

Chapter	Description
Introduction	This chapter provides an overview of the functions that are available through the Cisco Unified Communications Operating System.
Log Into Cisco Unified Communications Operating System Administration	This chapter provides procedures for logging in to the Cisco Unified Communications Operating System and for recovering a lost Administrator password.
Platform Status and Configuration	This chapter provides procedures for displaying operating system status and configuration settings.
Settings	This chapter provides procedures for viewing and changing the Ethernet settings, IP settings, and NTP settings.
System Restart	This chapter provides procedures for restarting and shutting down the system.
Security	This chapter provides procedures for certificate management and for IPSec management.
Software Upgrades	This chapter provides procedures for installing software upgrades and for uploading files to the TFTP server.
Services	This chapter provides procedures for using the utilities that the operating system provides, including ping and remote support.
Command Line Interface	This appendix provides information on the Command Line Interface, including available commands, command syntax, and parameters.

Related Documentation

Refer to the following documents for further information about related Cisco IP telephony applications and products:

- *Cisco Unified Presence Server Administration Guide*

  The *Cisco Unified Presence Server Administration Guide* provides step-by-step instructions for configuring, maintaining, and administering the Cisco Unified Presence Server.

- *Cisco Unified Presence Server Serviceability Administration Guide*

  This document provides descriptions of Cisco Unified Presence Server serviceability and remote serviceability and step-by-step instructions for configuring alarms, traces, and other reporting.

- *Disaster Recovery System Administration Guide*

  This document describes how to configure the backup settings, back up Cisco Unified Presence Server data, and restore the data.

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
	This pointer highlights an important line of text in an example.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords, are in angle brackets.

Notes use the following conventions:

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

Timesavers use the following conventions:

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

Tips use the following conventions:

Tip Means *the information contains useful tips.*

Cautions use the following conventions:

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

Warnings use the following conventions:

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

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

http://www.cisco.com/univercd/home/home.htm

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

If you do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Support site area by entering your comments in the feedback form available in every online document.

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.

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive these announcements by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. Registered users can access the tool at this URL:

http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

To register as a Cisco.com user, go to this URL:

http://tools.cisco.com/RPF/register/register.do

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Support website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Support Website

The Cisco Support website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

http://www.cisco.com/en/US/support/index.html

Access to all tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Before you submit a request for service online or by phone, use the **Cisco Product Identification Tool** to locate your product serial number. You can access this tool from the Cisco Support website by clicking the **Get Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Tip **Displaying and Searching on Cisco.com**

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing **F5**.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. After using the Search box on the Cisco.com home page, click the **Advanced Search** link next to the Search box on the resulting page and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411
Australia: 1 800 805 227
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

  http://www.cisco.com/offer/subscribe

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Internet Protocol Journal* is s a quarterly journal published by Cisco for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- "What's New in Cisco Documentation" is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of "What's New in Cisco Documentation" at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Introduction

For Cisco Unified Presence Server 1.0(3), you can perform many common system administration functions through the Cisco Unified Communications Operating System.

This chapter comprises the following topics:

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

Overview

Cisco Unified Communications Operating System Administration allows you to configure and manage the Cisco Unified Communications Operating System by doing these tasks:

- Check software and hardware status.
- Check and update IP addresses.
- Ping other network devices.
- Manage NTP servers.
- Upgrade system software and options.
- Restart the system.

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

Browser Requirements

You can access Cisco Unified Presence Server Administration, Cisco Unified Presence Server Serviceability, and Cisco Unified Communications Administration by using the following browsers:

- Microsoft Internet Explorer version 6.0 or later

- Netscape Navigator version 7.1 or later

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

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, “Platform Status and Configuration.”

Settings

From the **Settings** menu, you can view and update the following operating system settings:

- Ethernet—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.”

Restart Options

From the **Restart** menu**,** 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 Presence Server Locale Installers 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 For Cisco Unified Presence Server 1.0(3), you must do all software installations and upgrades by using the Software Upgrades menu options. The system can upload and process only software that Cisco Systems approved.

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

Services

The application provides the following operating system utilities:

- Ping—Checks connectivity with other network devices.
- Remote Support—Sets up an account that Cisco support personnel can use to access the system. This account automatically expires after the number of days that you specify.

For more information see Chapter 8, "Services."

Command Line Interface

The command line interface, which you can access from the console or through a secure shell connection to the server, provides a subset of the operating system functionality that is available through the operating system user interface. Keep in mind that the command line interface is designed for system emergencies and not as a replacement for the user interface.

For more information see Appendix A, "Command Line Interface."

CHAPTER 2

Log Into Cisco Unified Communications Operating System Administration

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

Logging Into Cisco Unified Communications Operating System Administration

To access Cisco Unified Communications Operating System Administration and log in, follow this procedure:

Procedure

Step 1 Log in to Cisco Unified Presence Server Administration.

Step 2 From the Navigation menu in the upper, right corner of the Cisco Unified Presence Server 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*/iptplatform.

Step 3 Enter your Administrator username and password.

Note The Administrator username and password get established during installation or created using the command line interface.

Step 4 Click **Submit.**

The Cisco Unified Communications Operating System Administration window displays.

Recovering the Administrator Password

If you lose the Administrator password and cannot access the system, use the following procedure to reset the Administrator password.

Note During this procedure, you will be required to 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 admin 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.

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 a new Administrator password.

Note The system resets the Administrator username to **admin**. If you want to set up a different Administrator username and password, use the CLI command **set password**. For more information, see Appendix A, “Command Line Interface.”

Step 7 Reenter the new password.

The system checks the new password for strength. If the password does not contain enough different characters, you get prompted to enter a new password.

Step 8 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.

Platform Status and Configuration

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

- Cluster Nodes
- Hardware Status
- Logs
- Network Status
- Installed Software
- System Status

You can view the status of the operating system, platform hardware, or the network.

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 Platform Hardware status window displays.

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

Table 3-2 Platform Hardware Status Field Descriptions

Field	Description
Hardware Platform	Displays the model identity of the platform server.
Number of Processors	Displays the number of processors in the platform server.
CPU Type	Displays the type of processor in the platform server.
Memory	Displays the total amount of memory in MBytes.
Detailed Report	Displays a detailed summary of the platform hardware.

Logs

To view system logs, you must install the Cisco Unified Presence Server Real-Time Monitoring Tool (RTMT). For more information on installing and using the RTMT, see the *Cisco Unified Presence Server Serviceability Administration Guide*.

Network Status

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 Settings Field Descriptions

Field	Description
Status	Indicates whether the port is Up or Down for Ethernet ports 0 and 1.
DHCP	Indicates whether DHCP is enabled for Ethernet port 0.
MAC Address	Displays the hardware address of the port.
Speed	Displays the speed of the connection.
Duplex	Displays the duplex mode.
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 there is an active link.
Auto Negotiation	Indicates whether auto negotiation is active.
MTU	Displays the maximum transmission unit.
Queue Length	Displays the length of the queue.
Receive Statistics	Displays information on received bytes and packets.
Transmit Statistics	Displays information on transmitted bytes and packets.
Primary DNS	Displays the IP address of the primary domain name server.
Secondary DNS	Displays the IP address of the secondary domain name server.
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 on page 3-4 for descriptions of the fields on the Platform Status window.

Table 3-5 Platform Status Field Descriptions

Field	Description
Host Name	Displays the name of the Cisco MCS host where Cisco Unified Communications Operating System is installed.
Date/Time	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 Ver	Displays the operating system version.
Platform Ver	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 Platform 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.

Settings

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 or change the IP settings, follow this procedure:

Caution Be aware that if you modify the IP Settings, you may lose contact with the Cisco Unified CallManager server.

Procedure

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

The Ethernet Settings window displays.

Step 2 To modify the Ethernet settings, enter the new values in the appropriate fields. For a description of the fields on the Ethernet Settings window, see Table 4-1.

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

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

Table 4-1 Ethernet Settings Fields and Descriptions

Field	Description
DHCP	Indicates whether DHCP is Enabled or Disabled.
Port Settings IP Address	Shows the IP address of the system.
Mask	Shows the IP subnet mask address.
Gateway IP Address	Shows the IP address of the network gateway.

Publisher Settings

On subsequent or subscriber nodes, you can view or change the IP address of the first node or publisher for the node.

Note You cannot change the Publisher Settings on Cisco Unified Presence Server.

To view or change the publisher IP settings, follow this procedure:

Procedure

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

The Publisher Settings window displays.

Note You can only view and change the publisher IP address on subsequent nodes of the cluster, not on the publisher itself.

Step 2 Enter the new publisher IP address.

Step 3 Click **Save**.

Changing IP Address on the Second Cisco Unified Presence Server Node

If the IP address of the first Cisco Unified Presence Server node gets changed while a subsequent node is offline, you may find that you cannot log in to Cisco Unified Presence Server Administration on the subsequent node. If this occurs, follow this procedure:

Procedure

Step 1 Log in directly to operating system administration on the subsequent node by using the following IP address:

http://*server-name*/iptplatform

where *server-name* specifies the host name or IP address of the subsequent node.

Step 2 Enter your Administrator user name and password and click **Submit**.

Step 3 Navigate to **Settings>IP>Publisher**.

Step 4 Enter the new IP address for the publisher and click **Save**.

Step 5 Restart the subsequent node.

NTP Servers

Ensure that external NTP server is stratum 9 or higher (1-9). To add, delete, or modify an external NTP server, follow this procedure:

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

Procedure

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

The NTP Server Settings window displays.

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

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

Note Any change you make to the NTP servers can take up to five 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 NTP server, you must restart all the 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, from the Certificate Expiry Monitor, for example, you must configure an SMTP host.

To access the SMTP settings, follow this procedure:

Procedure

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

The SMTP Settings window displays.

Step 2 Enter or modify the SMTP hostname or IP address.

Step 3 Click **Save**.

Time Settings

To manually configure the time, follow this procedure:

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

Procedure

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

Step 2 Enter the date and time for the system.

Step 3 Click **Save**.

System Restart

This section provides procedures for using the following restart options:

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

Switch Versions and Restart

You can use this option both when you are upgrading to a newer software version or when you need to fall back to an earlier software version. To shut down the system that is running on the active disk partition and then automatically restart the system 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 **Restart>Switch Versions**.

The Switch Software Version window displays, which shows the software version on both the active and inactive partitions.

Step 2 To switch versions and restart, click **Switch Version**. 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 **Restart>Current Version**.

The Restart Current Version window displays.

Step 2 To restart the system, click **Restart**, or to stop the operation, click **Cancel**.

If you click **Restart**, the system restarts on the current partition without switching versions.

Shut Down the System

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

To shut down the system, follow this procedure:

⚠ **Caution** This procedure causes the system to shut down.

Procedure

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

The Shutdown System window displays.

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

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

Note The hardware does not power down automatically.

Security

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

- Manage Certificates and Certificate Trust Lists
- Display Certificates
- Download a Certificate or CTL
- Delete and Regenerate a Certificate
- Upload a Certificate or Certificate Trust List
- Download a Certificate Signing Request
- Monitor Certificate Expiration Dates
- IPSEC Management
- Display or Change an Existing IPSec Policy
- Set Up a New IPSec Policy

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 Certificate Management menu options allow you to perform the following functions:

- Display certificates
- Upload certificates and Certificate Trust Lists (CTL)
- Download certificates and CTLs
- Delete certificates
- Regenerate certificates
- Download and generate Certificate Signing Requests (CSR)
- Monitor certificate expiration dates

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

Display Certificates

To display existing certificates, follow this procedure:

Procedure

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

The Select Certificates or Trust Store window displays.

Step 2 Check the check box for the type of certificate that you want to display: Own Certificates or Trust Certificates.

The Display Certificates or Trust Units window displays.

Step 3 Check the check box for the certificate type that you want to display.

The Display Certificates or Trust Store window displays.

Step 4 Check the check box for the certificate of trust store that you want to display.

The Details of a Certificate window displays.

Step 5 After you have viewed the certificate details, choose another menu option to close the Details of Certificate window.

Download a Certificate or CTL

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

Procedure

Step 1 Navigate to **Security** > **Certificate Management** > **Download Cert/CTL**.

The Select Certificate/CTL/CSR Download windows displays.

Step 2 Check the check box for the appropriate download type: Own Cert, Trust Cert, or CTL file. Click **Next**.

The Download Certificates or Trust Units window displays.

Step 3 Check the check box for the existing certificate type that you want to download and click **Next**.

The Display Certificate/CTL/CSR Download window displays.

Step 4 Check the check box for existing certificates that you want to download and click **Next**.

The Certificate/CTL/CSR Download window displays.

Step 5 Click the **Continue** link.

A directory listing that shows the certificates that you chose displays.

Step 6 To save the certificate or CTL to your PC, right-click the name of the certificate or CTL and choose **Save As**.

Step 7 Enter the location where you want to save the certificate or CTL.

Step 8 Click **Save**.

Delete and Regenerate a Certificate

Deleting a Certificate

To delete a trusted certificate, follow this procedure:

Caution Deleting a certificate can affect your system operations.

Procedure

Step 1 Navigate to **Security > Certificate Management > Delete/Regenerate Cert**.

Step 2 Check the **Delete Trust Cert** check box and click **Next**.

The Display Certificates or Trust Units For Delete/Regenerate window displays.

Step 3 Check the check box for the existing certificate type that you want to delete and click **Next**.

The Delete Certificates or Trust Store window displays.

Step 4 Check the Existing Certificate Name check box for the certificate that you want to delete and 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** > **Delete/Regenerate Cert**.

The Select Certificates or Trust Store for Deletion window displays.

Step 2 Check the **Regenerate Self-Signed Cert** check box and click **Next**.

Step 3 Check the appropriate **Existing Certificates Types** check box for the certificate that you want to regenerate and click **Next**.

Step 4 Check the appropriate **Existing Certificate** check box and click **Regenerate**.

Upload a Certificate or Certificate Trust List

Caution Uploading a new certificate or certificate trust list (CTL) file can affect your system operations.

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.

To upload a CA root certificate, application certificate, or CTL file to the server, follow these steps:

Procedure

Step 1 Navigate to **Security** > **Certificate Management** > **Upload Certificate/CTL**.

The Select Certificate/CTL Upload window displays.

Step 2 Choose one of the radio buttons; then, click **Next**:

- Upload Own Cert—To upload an application certificate that is issued by a third party CA.
- Upload Trust Cert—To upload a CA root certificate or a trusted application certificate.
- Upload CTL File—To upload a CTL file.

The Certificate type for the upload including CTL window displays.

Step 3 In the Certificate type for the upload including CTL window, do the following steps:

a. Select the type of certificate or CTL from the **Existing certificate types** list.

b. 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 Cert Name (without any extensions)** text box. If you are uploading a CA root certificate or CTL, leave this text box empty.

c. Click **Next**.

The Upload Certificate/CTL window displays.

Step 4 In the Upload Certificate/CTL window, do the following steps:

a. Select the file to upload by doing one of the following steps:

   - In the **File Name for Upload** text box, enter the path to the file.
   - Click the **Browse** button and navigate to the file; then, click **Open**.

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

Download a Certificate Signing Request

To download a Certificate Signing Request, follow this procedure:

Procedure

Step 1 Navigate to **Security** > **Certificate Management** > **Download/Generate CSR**.

The Select Certificate type for CSR window displays.

Step 2 Check the **Existing Certificate Types** check box for the CSR that you want to download.

Step 3 Check the **Download CSR if any** check box.

The Certificate/CTL/CSR Download window displays.

Step 4 Click **Continue**.

A directory listing shows the certificates that you chose.

Step 5 To save the CSR to your PC, right-click the name of the certificate or CTL and choose **Save As**.

Step 6 Enter the location where you want to save the certificate or CTL.

Step 7 Click **Save**.

Using Third Party CA Certificates

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

	Task	For More Information
Step 1	Generate a CSR on the server.	See the "Generating a Certificate Signing Request" section on page 6-6.
Step 2	Download the CSR to your PC.	See the "Download a Certificate Signing Request" section on page 6-5.
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 6-6 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 6-6 for additional notes.
Step 5	Upload the CA root certificate to the server.	See the "Upload a Certificate or Certificate Trust List" section on page 6-4.
Step 6	Upload the application certificate to the server.	See the "Upload a Certificate or Certificate Trust List" section on page 6-4.

	Task	For More Information
Step 7	If you updated the certificate for CAPF or Cisco Unified Presence Server, generate a new CTL file.	See the *Cisco Unified CallManager Security Guide*.
Step 8	Restart the services that affects 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 Presence Server, restart the TFTP service. See the *Cisco Unified Presence Server 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** > **Download/Generate CSR**.

The Select Certificate type for CSR window displays.

Step 2 Choose the type of certificate to generate in the **Existing Certificate Types** area.

Step 3 Choose the **Generate a new CSR** radio button.

Step 4 Click **Next**.

The Cert/IPSEC Operation (CSR/Config/Assoc Create) Done window displays and states that the CSR successfully generated.

Obtaining Third-Party CA Certificates

To use an application certificate that a third-party CA issues, you must obtain from the CA both the signed application certificate and the CA root certificate. Get information about obtaining these certificates from your CA. The process varies among CAs.

CAPF and Cisco Unified Presence Server 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 the final window of the CSR generation process lists.

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 DER encoding formats.

Cisco verified third-party certificates that were obtained from Microsoft, Keon, and Verisign CAs. Certificates from other CAs might work but have not been verified.

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 Management** > **Cert Expiry Monitor** > **Display Config**.

The Show Cert Expiry Monitoring Config window, which shows a summary of the current configuration information, displays.

Step 2 To configure the Certificate Expiration Monitor, navigate to **Security** > **Certificate Management** > **Cert Expiry Monitor** > **Change Config**.

The Change Cert Expiry Monitoring Config window displays.

Step 3 Enter the required configuration information. See Table 6-1 for a description of the Certificate Expiration Monitor fields.

Step 4 To save your changes, click **Submit**.

Table 6-1 Certificate Expiration Monitor Field Descriptions

Field	Description
Notification/Alert Start Time	Enter the number of days before the certificate expires that you want to be notified.
Initial Frequency of Notification	Enter the frequency for notification, either in hours or days.
Click on the right to Enable/Disable	To turn on e-mail notification, click **Enable**.
Email IDs entered for Notification	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 IPSec menu options allow you to perform the following functions:

- Display or change an existing IPSec policy
- Set up a new IPSec policy

Note IPSec does not get set up automatically between nodes in the cluster during installation.

Display or Change an Existing IPSec Policy

To display or change 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 you system.

Procedure

Step 1 Navigate to **Security > IPSEC Management > Display/Change IPSEC**.

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

The Display IPSEC Policy window displays.

Step 2 Check the appropriate Existing Policy check box and click **Next**.

Step 3 Perform one of the following actions:

- To view an IPSec policy, click the **Display Detail** link.
- To delete an IPSec policy, click **Delete**.
- To activate an IPSec policy, click **Enable**.
- To deactivate an IPSec policy, click **Disable**.

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

Step 4 If you click the Display Detail link, the Association Details window displays. For an explanation of the fields in this window, see Table 6-2.

Set Up a New IPSec Policy

To set up a new IPSec policy and association, follow this procedure:

Note Because any changes 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 Management > Setup New IPSEC**.

The Setup Select window displays.

Step 2 Check the **Certificate** or **Pre-Shared Key** check box.

- If you check Certificate, check **Same Type** or **Different Type** node.
- If you check Pre-Shared Key, enter the key name.

Step 3 Click **Next**.

The Setup IPSEC Policy and Association window displays.

Step 4 Enter the appropriate information on the Setup IPSEC Policy and Association window. For a description of the fields on this window, see Table 6-2.

Step 5 To set up the new IPSec policy, click **Submit**.

Table 6-2 IPSEC Policy and Association Field Descriptions

Field	Description
Policy Name	Specifies the name of the IPSec policy.
Dest. Address Type	Specifies the Destination Address Type: • IP—Dotted IP address of the destination • FQDN—Fully qualified domain name of the destination
Source Address Type	Specifies the Source Address Type: • IP—Dotted IP address of the source • FQDN—Fully qualified domain name of the source
Tunnel/Transport	Specifies tunnel or transport.
Protocol	Specifies the specific protocol, or Any: • TCP • UDP • Any
Dest. Port	Specifies the port number to use at the destination.
Phase 1 Life Time in Seconds	Specifies the lifetime for phase 1, IKE negotiation, in seconds.
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
Phase 2 Life Time in Seconds	Specifies the lifetime for phase 2, IKE negotiation, in seconds.
AH Algorithm	Because this field is not functional, use the ESP Algorithm field instead to select an authentication algorithm.
Assoc. Name	Specifies the association name that is given to each IPSec association.
Dest. Address	Specifies the IP address or FQDN of the destination.
Source Address	Specifies the IP address or FQDN of the source.
Remote Port	Specifies the port number at the destination.
Source Port	Specifies the port number at the source.

Table 6-2 IPSEC Policy and Association Field Descriptions (continued)

Field	Description
Encryption Algorithm	From the drop-down list, choose the encryption algorithm. Choices include: • DES • 3DES
Phase 1 DH Value	From the drop-down list, choose the phase 1 DH value. Choices include: 2, 1, 5, 14, 16, 17, and 18.
ESP Algorithm	From the drop-down list, choose the ESP algorithm. Choices include: • NULL_ENC • DES • 3DES • BLOWFISH • RIJNDAEL
Phase 2 DH Value	From the drop-down list, choose the phase 2 DH value. Choices include: 2, 1, 5, 14, 16, 17, and 18.

Software Upgrades

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

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

Software Upgrade and Installation

The Software Upgrade windows enable you to upgrade the Cisco Unified Communications Operating System software from either a local or a remote source.

The software upgrade process also enables you to back out of an upgrade if problems occur. You install the software for the upgrade on the system inactive partition and perform a restart to switch the system to the newer version of the software. During this process, the upgraded software becomes the active partition, and your current software becomes the inactive partition. Your configuration information migrates automatically to the upgraded version in the active partition.

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

Starting with Cisco Unified CallManager version 5.0(4), CAPF uses the Certificate Manager Infrastructure to manage its certificates and keys. Because of this, when you upgrade to version 5.0(4), CAPF keys and certificates automatically regenerate. You must then rerun the CTL Client application to upgrade the CTL file. For information on using CAPF with Cisco Unified CallManager, refer to the *Cisco Unified CallManager Security Guide*.

From Local Source

You can install software from a CD or DVD that is located in the local disc drive and then start the upgrade process.

Note Be sure to back up your system data before starting the software upgrade process. For more information, see the *Disaster Recovery System Administration Guide*.

To install or upgrade software from a CD or DVD, follow this procedure:

Procedure

Step 1 If you plan to download the upgrade file, create a CD or DVD by doing the following steps:

Note If you download an upgrade file from Cisco.com using Internet Explorer and have WinZip (or a similar zip utility) installed on your PC, the file extension gets changed from .gz.sgn to .gz.gz. To successfully install the upgrade, you must rename the file and change the extension back to .gz.sgn.

a. Download the appropriate upgrade file from Cisco.com.

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

b. Copy the upgrade file to a writeble CD or DVD.

Step 2 Insert the CD or DVD into the disc drive on the local server that is to be upgraded.

Note Because of their size, some upgrade files may not fit on a CD and will require a DVD.

Step 3 Choose **Software Upgrades > Install/Upgrade**.

Step 4 For the software location source, choose **DVD/CD**.

Step 5 If you burned the patch file to a subdirectory on the CD or DVD, enter the path in the Directory field.

Step 6 To continue the upgrade process, click **Next**.

Step 7 Choose the upgrade version that you want to install and click **Next**.

Step 8 In the next window, monitor the progress of the download, which includes the filename and the number of megabytes that are getting transferred.

When the download completes, the Checksum window displays.

Step 9 Verify the checksum value against the checksum for the file that you downloaded that is shown on Cisco.com.

Caution The two checksum values must match to ensure the authenticity and integrity of the upgrade file. If the checksum values do not match, download a fresh version of the file from Cisco.com and try the upgrade again.

Step 10 After determining that the cheksums match, click **Next** to proceed with the software upgrade.

A Warning window displays the current and upgrade software versions.

Step 11 To continue with the software upgrade, click **Next**.

The Post Installation Options window displays.

Step 12 Choose whether you want the system to automatically reboot to the upgraded partition after installing the upgrade software:

- To install the upgrade and automatically reboot to the upgraded partition, choose **Reboot to upgraded partition**.

- To install the upgrade and then manually reboot to the upgraded partition at a later time, choose **Do not reboot after upgrade**.

Step 13 Click **Upgrade**.

The Upgrade Status windows displays and displays the Upgrade log.

Step 14 When the installation completes, click **Finish**.

Step 15 To restart the system and activate the upgrade, choose **Restart > Switch Versions**.

The Switch Software Version window displays.

Step 16 To switch software versions and restart the system, click **Switch Versions**.

The system restarts running the upgraded software.

From Remote Source

To install software from a network drive or remote server, use the following procedure.

Note Be sure to back up your system data before starting the software upgrade process. For more information, see the *Disaster Recovery System Administration Guide*.

Procedure

Step 1 Navigate to **Software Upgrades > Install**.

Step 2 For the Software Location Source, choose **Remote File System**.

Step 3 Enter the directory name for the software upgrade, if required.

If the upgrade file is located on a Linux or Unix server, you must enter a forward slash at the beginning of the directory path you want to specify. For example, if the upgrade file is in the patches directory, you must enter `/patches`. If the upgrade file is located on a Windows server, check with your system administrator for the correct directory path.

Step 4 Enter the required upgrade information as described in the following table:

Field	Description
Remote Server	Host name or IP address of the remote server from which software will be downloaded.
Remote User	Name of a user who is configured on the remote server.
Remote Password	Password that is configured for this user on the remote server.
Download Protocol	Choose sftp or ftp.

Note You must choose **Remote File System** to enable the remote server configuration fields.

Step 5 Click **Next**.

The system checks for available upgrades.

Step 6 Choose the upgrade or option that you want to install and click **Next**.

Step 7 In the next window, monitor the progress of the download, which includes the filename and the number of megabytes that are getting transferred.

When the download completes, the Checksum window displays.

Step 8 Verify the checksum value against the checksum for the file that you downloaded that was shown on Cisco.com.

Caution The two checksum values must match to ensure the authenticity and integrity of the upgrade file. If the checksum values do not match, download a fresh version of the file from Cisco.com and try the upgrade again.

Step 9 After determining that the cheksums match, click **Next** to proceed with the software upgrade.

A Warning window displays the current and upgrade software versions.

Step 10 To continue with the software upgrade, click **Next**.

The Post Installation Options window displays.

Step 11 Choose whether you want the system to automatically reboot to the upgraded partition after installing the upgrade software:

- To install the upgrade and automatically reboot to the upgraded partition, choose **Reboot to upgraded partition**.
- To install the upgrade and then manually reboot to the upgraded partition at a later time, choose **Do not reboot after upgrade**.

Step 12 Click **Upgrade**.

The Upgrade Status window, which shows the Upgrade log, displays.

Step 13 When the installation completes, click **Finish**.

Step 14 To restart the system and activate the upgrade, choose **Restart** > **Switch Versions**.

The system restarts running the upgraded software.

Note After upgrading from Cisco Unified Presence Server Release 1.0(2) to Release 1.0(3), ensure that LDAP search works in Cisco Unified Personal Communicator. If LDAP search does not work, delete the Cisco Unified Personal Communicator LDAP Profile in Cisco Unified Presence Server Administration and then recreate it. For more information, see the LDAP Profile chapter in the *Cisco Unified Presence Server Administration Guide*.

Locale Installation

Cisco provides locale-specific versions of the Cisco Unified CallManager Locale Installer on www.cisco.com. Installed by the system administrator, the locale installer allows the user to view/receive the chosen translated text or tones, if applicable, when a user works with supported interfaces.

User Locales

User locale files provide translated text and voice prompts, if available, for phone displays, user applications, and user web pages in the locale that the user chooses. User-only locale installers exist on the web.

Network Locales

Network locale files provide country-specific phone tones and gateway tones, if available. Network-only locale installers exist on the web.

Cisco may combine multiple network locales in a single locale installer.

Note The Cisco Media Convergence Server (MCS) or Cisco-approved, customer-provided server can support multiple locales. Installing multiple locale installers ensures that the user can choose from a multitude of locales.

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

Installing Locales

You can install locale files from either a local or a remote source by using the same process that is described earlier in this chapter for installing software upgrades. See Software Upgrade and Installation for more information about this process.

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

See Locale Files for information on the locale files that you must install. You can install more than one locale before you restart the server.

Locale Files

When installing locales, you must install both the following files:

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

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

- Combined Network Locale file—Contains country-specific files for all countries for various network items, including phone tones, annunciators, and gateway tones. The combined network locale file uses the following naming convention:

  cm-locale-combinednetworklocale-*version*.cop

Error Messages

See Table 7-1 for a description of the error messages that can occur during Locale Installer activation. If an error occurs, you can view the error messages in the installation log.

Table 7-1 Locale Installer Error Messages and Descriptions

Message	Description
[LOCALE] File not found: <language>_<country>_user_locale.csv, the user locale has not been added to the database.	This error occurs when the system cannot locate the CSV file, which contains user locale information to add to the database. This indicates an error with the build process.
[LOCALE] File not found: <country>_network_locale.csv, the network locale has not been added to the database.	This error occurs when the system cannot locate the CSV file, which contains network locale information to add to the database This indicates an error with the build process.
[LOCALE] CallManager CSV file installer installdb is not present or not executable	A Cisco Unified CallManager application called installdb must be present; it reads information that is contained in a CSV file and applies it correctly to the Cisco Unified CallManager database. If this application is not found, it either was not installed with Cisco Unified CallManager (very unlikely), has been deleted (more likely), or the server does not have Cisco Unified CallManager installed (most likely). Installation of the locale will terminate because locales will not work without the correct records that are held in the database.
[LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maDialogs_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maMessages_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maGlobalUI_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/LocaleMasterVersion.txt.Checksum.	These errors could occur when the system fails to create a checksum file, caused by an absent Java executable, /usr/local/thirdparty/java/j2sdk/jre/bin/java, an absent or damaged Java archive file, /usr/local/cm/jar/cmutil.jar, or absent or damaged Java class, com.cisco.ccm.util.Zipper. Even if these errors occur, the locale will continue to work correctly, with the exception of Cisco Unified CallManager Assistant, which cannot detect a change in localized Cisco Unified CallManager Assistant files.
[LOCALE] Could not find /usr/local/cm/application_locale/cmservices/ipma/LocaleMasterVersion.txt in order to update Unified CM Assistant locale information.	This error occurs when the file has not been found in the correct location, which is most likely due to an error in the build process.
[LOCALE] Addition of <RPM-file-name> to the Cisco Unified CallManager database has failed!	This error occurs because of the collective result of any failure that occurs when a locale is being installed; it indicates a terminal condition.

Uploading TFTP Server Files

You can use the Upload TFTP Server File option to upload various files for use by the phones to the server. Files that you can upload include custom phone rings, callback tones, and backgrounds. This option uploads files only to the specific server to which you connected, and other nodes in the cluster do not get upgraded.

Files upload into the tftp directory by default. You can also upload files to a subdirectory of the tftp directory.

If you have two Cisco TFTP servers that are configured in the cluster, you must perform the following procedure on both servers. This process does not distribute files to all servers, nor to both of the Cisco TFTP servers in a cluster.

To upload TFTP server files, follow this procedure:

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Software Upgrades>Upload TFTP Server File**.

The Upload TFTP Server File window displays and shows a listing of the current uploaded files.

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

Step 3 To upload the file to a subdirectory of the tftp directory, enter the subdirectory in the **Subdirectory of the tftp directory where file will be uploaded** field.

Step 4 To start the upload, click **Upload File**.

The Status area indicates when the file uploads successfully.

Step 5 After the file uploads, restart the Cisco TFTP service.

Note If you plan to upload several files, restart the Cisco TFTP service only once, after you have uploaded all of the files.

For information about restarting services, refer to *Cisco Unified CallManager Serviceability Administration Guide*.

Note If you want to modify a file that is already in the TFTP directory, you can use the CLI command **file list tftp** to see the files in the TFTP directory and **file get tftp** to get a copy of a file in the TFTP directory. For more information, see Appendix A, “Command Line Interface.”

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.

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 complete.

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 as follows:

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

Step 2 If no remote support account is configured, click **Add**.

Step 3 Enter an account name for the remote account and the account life in days.

Note Ensure the account name at least six-characters long and all lowercase, alphabetic characters.

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 Cisco personnel.

Table 8-1 Remote Support Status Fields and Descriptions

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

APPENDIX A

Command Line Interface

Overview

This appendix describes commands that you can use on the Cisco IPT Platform to perform basic operating system functions. The Cisco IPT Platform Administration GUI application also makes these functions available. Typically you would use the command-line interface (CLI) only when a problem occurs while you are using the Cisco IPT Platform Administration interface.

Starting a CLI Session

You can access the Cisco IPT Platform CLI remotely or locally:

- From a web client workstation, such as the workstation that you use for Cisco IPT Platform Administration, you can use SSH to connect securely to the Cisco IPT Platform.
- You can access the Cisco IPT Platform CLI directly by using the monitor and keyboard that you used during installation or by using a terminal server that is connected to the serial port. Use this method if a problem exists with the IP address.

Before You Begin

Ensure you have the following information that gets defined during installation:

- A primary IP address and hostname
- An administrator ID
- A password

You will need this information to log in to the Cisco IPT Platform.

Perform the following steps to start a CLI session:

Step 1 Do one of the following actions depending on your method of access:

- From a remote system, use SSH to connect securely to the Cisco IPT Platform. In your SSH client, enter

  ssh *adminname@hostname*

  where ***adminname*** specifies the Administrator ID and ***hostname*** specifies the hostname that was defined during installation.

  For example, **ssh admin@ipt-1**.

- From a direct connection, you receive this prompt automatically:

  ```
  ipt-1 login:
  ```

  where **ipt-1** represents the host name of the system.

  Enter the administrator ID that was defined during installation.

In either case, the system prompts you for a password.

Step 2 Enter the password that was defined at installation.

The CLI prompt displays. The prompt represents the Administrator ID; for example:

admin:

You can now use any CLI command.

CLI Basics

The following section contains basic tips for using the command line interface.

Completing Commands

To complete commands, use **Tab**:

- Enter the start of a command and press **Tab** to complete the command. For example, if you enter **se** and press **Tab**, **set** gets completed.
- Enter a full command name and press **Tab** to display all the commands or subcommands that are available. For example, if you enter **set** and press Tab, you see all the **set** subcommands. An * identifies the commands that have subcommands.
- If you reach a command, keep pressing **Tab**, and the current command line repeats; this indicates that no additional expansion is available.

Getting Help on Commands

You can get two kinds of help on any command:

- Detailed help that includes a definition of the command and an example of its use
- Short query help that includes only command syntax

Procedure

To get detailed help, at the CLI prompt, enter

help *command*

Where *command* specifies the command name or the command and parameter. See Example A-1.

To query only command syntax, at the CLI prompt, enter

*command***?**

Where *command* represents the command name or the command and parameter. See Example A-2.

Note If you enter a **?** after a menu command, such as **set**, it acts like the Tab key and lists the commands that are available.

Example A-1 Detailed Help Example:

```
admin:help file list activelog

activelog help:
This will list active logging files

options are:
page    - pause output
detail  - show detailed listing
reverse - reverse sort order
date    - sort by date
size    - sort by size

file-spec can contain '*' as wildcards

Example:
admin:file list activelog platform detail
02 Dec,2004 12:00:59      <dir>    drf
02 Dec,2004 12:00:59      <dir>    log
16 Nov,2004 21:45:43        8,557  enGui.log
27 Oct,2004 11:54:33       47,916  startup.log
dir count = 2, file count = 2
```

Example A-2 Query Example:

```
admin:file list activelog?
Syntax:
file list activelog file-spec [options]
file-spec   mandatory   file to view
options     optional    page|detail|reverse|[date|size]
```

Ending a CLI Session

At the CLI prompt, enter **quit**. If you are logged in remotely, you get logged off, and the ssh session gets dropped. If you are logged in locally, you get logged off, and the login prompt returns.

Cisco IPT Platform CLI Commands

The following tables list and describe the CLI commands that are available for the Cisco Unified Communications Operating System and for Cisco Unified CallManager.

File Commands

The following table lists and explains the CLI File commands:

Table A-1 File Commands

Command	Parameters and Options	Description
file check	[*detection-size-kb*] Where *detection-size-kb* specifies the minimum file size change that is required for the command to display the file as changed. Default minimum size: 100 KB The command notifies you about a possible impact to system performance and asks you whether you want to continue. **Warning** **Because running this command can affect system performance, Cisco recommends that you run the command during off-peak hours.** **Options** None	This command checks the /usr directory tree to see whether any files or directories have been added, removed, or changed in size since the last fresh installation or upgrade and displays the results. The display includes both deleted and new files. Command privilege level: 0 Allowed during upgrade: No

Table A-1 File Commands (continued)

Command	Parameters and Options	Description
file delete	**activelog** *directory/filename* [**detail**] [**noconfirm**] **inactivelog** *directory/filename* [**detail**] [**noconfirm**] **install** *directory/filename* [**detail**] [**noconfirm**] **tftp** *directory/filename* [**detail**] Where - **activelog** specifies a log on the active side. - **inactivelog** specifies a log on the inactive side. - **install** specifies an installation log. - **tftp** specifies a TFTP file. You can use the wildcard character, *, for *filename*. ⚠ **Caution** You cannot recover a deleted file except, possibly, by using the Disaster Recovery System. If you delete a TFTP data file on the inactive side, you may need to manually restore that file if you switch versions to the inactive side. **Options** - **detail**—Displays a listing of deleted files with the date and time. - **noconfirm**—Deletes files without asking you to confirm each deletion.	This command deletes one or more files. Command privilege level: 1 Allowed during upgrade: Yes **Example: Delete the install log** `file delete install install.log`
file dump	**activelog** *directory/filename* **[detail] [hex**] **inactivelog** *directory/filename* **[detail] [hex**] **install** *directory/filename* **[detail] [hex**] **tftp** *directory/filename* **[detail] [hex**] Where - **activelog** specifies a log on the active side. - **inactivelog** specifies a log on the inactive side. - **install** specifies an installation log. - **tftp** specifies a TFTP file. You can use the wildcard character, *, for *filename* as long as it resolves to one file. **Options** - **detail**—Displays listing with the date and time. - **hex**—Displays output in hexadecimal.	This command dumps the contents of a file to the screen, a page at a time. Command privilege level: 1 for logs, 0 for TFTP files Allowed during upgrade: Yes **Example: Dump contents of file _cdrIndex.idx** `file dump activelog cm/cdr/_cdrIndex.idx`

Table A-1 File Commands (continued)

Command	Parameters and Options	Description

file get	**activelog** *directory/filename* [**reltime**] [**abstime**] [**match**] [**recurs**]
	inactivelog *directory/filename* [**reltime**] [**abstime**] [**match**] [**recurs**]
	install *directory/filename* [**reltime**] [**abstime**] [**match**] [**recurs**]
	tftp *directory/filename* [**reltime**] [**abstime**] [**match**] [**recurs**]
	Where
	• **activelog** specifies a log on the active side.
	• **inactivelog** specifies a log on the inactive side.
	• **install** specifies an installation log.
	• **tftp** specifies a TFTP file.
	Options
	• **abstime**—Absolute time period, specified as
	hh:mm:MM/DD/YY hh:mm:MM/DD/YY
	• **reltime—**Relative time period, specified as
	minutes | hours | days | weeks | months <value>
	• **match**—Match a particular string in the filename, specified as
	`<string value>`
	• **recurs**—Get all files, including subdirectories
	After the command identifies the specified files, you get prompted to enter an SFTP host, username, and password.
		This command sends the file to another system by using SFTP.
		Command privilege level: 0
		Allowed during upgrade: Yes
		Example 1: Get all files in the activelog operating system directory that match the string "plat"
		`file get activelog platform match plat`
		Example 2: Get all operating system log files for a particular time period
		`file get activelog platform/log abstime 18:00:9/27/200 18:00:9/28/2005`

Table A-1 File Commands (continued)

Command	Parameters and Options	Description

file list	**activelog** *directory* [**page] [detail] [reverse]** [**date** | **size**]
	inactivelog *directory* [**page] [detail] [reverse]** [**date** | **size**]
	install *directory* [**page] [detail] [reverse]** [**date** | **size**]
	tftp *directory* [**page] [detail] [reverse]** [**date** | **size**]
	Where
	• **activelog** specifies a log on the active side.
	• **inactivelog** specifies a log on the inactive side.
	• **install** specifies an installation log.
	• **tftp** specifies a TFTP file.
	Note You can use a wildcard character, *, for directory name as long as it resolves to one directory.
	Options
	• **detail**—Long listing with date and time
	• **date**—Sort by date
	• **size**—Sort by file size
	• **reverse**—Reverse sort direction
	• **page**—Displays the output one screen at a time
		This command lists the log files in an available log directory.
		Command privilege level: 1 for logs, 0 for TFTP files
		Allowed during upgrade: Yes
		Example 1: List Operating System Log files with details
		`file list activelog platform/log page detail`
		Example 2: List directories in CDR Repository
		`file list activelog cm/cdr_repository`
		Example 3: List CDR files in a specified directory by size
		`file list activelog cm/cdr_repository/processed/20050812 size`

Table A-1 File Commands (continued)

Command	Parameters and Options	Description
file search	**activelog** *directory/filename reg-exp* **[abstime** *hh*:*mm*:*ss mm*/*dd*/*yyyy hh*:*mm*:*ss mm*/*dd*/*yyyy*] [**ignorecase**] **[reltime** {**days|hours|minutes}** *timevalue*] **inactivelog** *directory/filename reg-exp* **[abstime** *hh*:*mm*:*ss mm*/*dd*/*yyyy hh*:*mm*:*ss mm*/*dd*/*yyyy*] [**ignorecase**] **[reltime** {**days|hours|minutes}** *timevalue*] **install** *directory/filename reg-exp* **[abstime** *hh*:*mm*:*ss mm*/*dd*/*yyyy hh*:*mm*:*ss mm*/*dd*/*yyyy*] [**ignorecase**] **[reltime** {**days|hours|minutes}** *timevalue*] **tftp** *directory/filename reg-exp* **[abstime** *hh*:*mm*:*ss mm*/*dd*/*yyyy hh*:*mm*:*ss mm*/*dd*/*yyyy*] [**ignorecase] [reltime** {**days|hours|minutes}** *timevalue*] Where • **activelog** specifies a log on the active side. • **inactivelog** specifies a log on the inactive side. • **install** specifies an installation log. • **tftp** specifies a TFTP file. • *reg-exp* represents a regular expression. **Note** You can use the wildcard character, *, to represent all or part of the filename. **Options** • **abstime**—Specifies which files to search based on file creation time. Enter a start time and an end time. • **days|hours|minutes**—Specifies whether the file age is in days, hours, or minutes. • **ignorecase**—Ignores case when searching • **reltime**—Specifies which files to search based on file creation time. Enter the age of files to search. • *hh*:*mm*:*ss mm*/*dd*/*yyyy*—An absolute time, in the format hours:minutes:seconds month/day/year. • *timevalue*—The age of files to search. The unit of this value is specified with the {**days|hours|minutes}** option.	This command searches the content of a log and displays the matching lines a page at a time. Write the search term in the form of a regular expression, which is a special text string for describing a search pattern. If the search term is found in only one file, the filename appears at the top of the output. If the search term is found in multiple files, each line of the output begins with the filename in which the matching line was found. Command privilege level: 0 Allowed during upgrade: Yes **Example** `file search activelog platform/log/platform.log Err[a-z] ignorecase`

Table A-1 File Commands (continued)

Command	Parameters and Options	Description
file tail	**activelog** *directory/filename* [**detail] [hex] [lines**] **inactivelog** *directory/filename* [**detail] [hex] [lines**] **install** *directory/filename* [**detail] [hex] [lines**] **tftp** *directory/filename* [**detail] [hex] [lines**] Where - **activelog** specifies a log on the active side. - **inactivelog** specifies a log on the inactive side. - **install** specifies an installation log. - **tftp** specifies a TFTP file. **Note** You can use the wildcard character, *, for filename as long as it resolves to one file. **Options** - **detail**—Long listing with date and time - **hex**—Hexadecimal listing - **lines**—Number of lines to display	This command tails (prints the last few lines) of a log file. Command privilege level: 1 for logs, 0 for TFTP files Allowed during upgrade: Yes **Example: Tail the operating system CLI log file** `file tail activelog platform/log/cli00001.log`

file view	**activelog** *directory/filename*
	inactivelog *directory/filename*
	install *directory/filename*
	tftp *directory/filename*
	Where
	- **activelog** specifies a log on the active side.
	- **inactivelog** specifies a log on the inactive side.
	- **install** specifies an installation log.
	- **tftp** specifies a TFTP file.
	Note You can use the wildcard character, *, for filename as long as it resolves to one file.
	Caution Do not use this command to view binary files because this can corrupt the terminal session.
		This command displays the contents of a file.
		Command privilege level: 0
		Allowed during upgrade: Yes
		Example 1: Display the install log
		`file view install install.log`
		Example 2: Display a particular CDR file
		`file view activelog /cm/cdr_repository/processed/20058012/{filename}`

Show Commands

The following table lists and explains the CLI Show commands:

Table A-2 Show Commands

Command	Parameters and Options	Description
show account	None	This command lists current administrator accounts, except the master administrator account. Command privilege level: 4 Allowed during upgrade: Yes
show cert	**own** *filename* **trust** *filename* **list {own | trust}** Where • *filename* represents the name of the certificate file. • **own** specifies owned certificates. • **trust** specifies trusted certificates. • **list** specifies a certificate trust list. **Options** None	This command displays certificate contents and certificate trust lists. Command privilege level: 1 Allowed during upgrade: Yes **Example: Display own certificate trust lists** `show cert list own`
show firewall	**list** [**detail**] [**page**] [**file** *filename*] Where • **detail**—Displays detailed statistics on every available device on the system • **page**—Displays the output one page at a time • **file** *filename*—Outputs the information to a file **Note** The file option saves the information to platform/cli/*filename*.txt. Ensure the file name does not contain the "." character.	This command displays system aspects of the server. Command privilege level: 1 Allowed during upgrade: Yes
show hardware	None	This command displays the following information on the platform hardware: • Platform • Serial number • BIOS build level • BIOS manufacturer • Active processors • RAID controller status Command privilege level: 0 Allowed during upgrade: Yes

Table A-2 Show Commands (continued)

Command	Parameters and Options	Description
show ipsec	**policy** **association** *policy* **information** *policy association* **status** Where - **policy** displays all IPSec policies on the node. - **association** displays the association list and status for the policy. - **information** displays the association details and status for the policy. - **status** displays the status of all IPsec tunnels that are defined in the system. - *policy* represents the name of a specific IPSec policy. - *association* represents the association name. **Options** None	This command displays information on IPSec policies and associations. Command privilege level: 1 Allowed during upgrade: yes **Example: Display IPSec policies** `show ipsec policy`
show logins	*number* Where *number* specifies the number of most recent logins to display. The default specifies 20.	This command lists recent logins to the server.
show myself	None	This command displays information about the current account. Command privilege level: 0 Allowed during upgrade: Yes

Table A-2 Show Commands (continued)

Command	Parameters and Options	Description
show network	**eth0** [**detail**] **failover** [**detail**] [**page**] **route** [**detail**] **status** [**detail**] [**listen**] [**process**] [**all**] [**nodns**] [**search stext**] **max_ip_conntrack** **all** [**detail**] Where • **eth0** specifies Ethernet 0. • **failover** specifies Network Fault Tolerance information. • **route** specifies network routing information. • **status** specifies active Internet connections. • **max_ip_conntrack** specifies max_ip_conntrack information. • **all** specifies all basic network information. **Options** • **detail**—Displays additional information • **page**—Displays information 1 page at a time. • **listen**—Displays only listening sockets • **process**—Displays the process ID and name of the program to which each socket belongs • **all**—Displays both listening and nonlistening sockets • **nodns**—Displays numerical addresses without any DNS information • **search stext**—Searches for the stext in the output	This command displays network information. The **eth0** parameter Ethernet port 0 settings, including DHCP and DNS configurations and options. Command privilege level: 0 Allowed during upgrade: Yes **Example: Display active Internet connections** `show network status`

Table A-2 Show Commands (continued)

Command	Parameters and Options	Description
show open	**files** [**all**] [**process** *processID*] [**regexp** *reg_exp*] **ports** [**all**] [**regexp** *reg_exp*] Where • **files** displays open files on the system. • **ports** displays open ports on the system. **Options** • **all**—Displays all open files or ports • **process**—Displays open files that belong to the specified process • *processID*—Specifies a process • **regexp**—Displays open files or ports that match the specified regular expression. • *reg_exp*—A regular expression	This command displays open files and ports on the system.
show packages	**active** *name* [**page**] **inactive** *name* [**page**] Where *name* represents the package name. To display all active or inactive packages, use the wildcard character, *. **Options** **page**—Displays the output one page at a time	This command displays the name and version for installed packages. Command privilege level: 0 Allowed during upgrade: Yes
show perf	**counterhelp** *class-name counter-name* Where • *class-name* represents the class name that contains the counter. • *counter-name* represents the counter that you want to view. **Note** If the class name or counter name contains white spaces, enclose the name in double quotation marks. **Options** None	This command displays the explanation text for the specified perfmon counter. Command privilege level: 0 Allowed during upgrade: Yes
show perf	list categories **Options** None	This command lists all categories in the perfmon system. Command privilege level: 0 Allowed during upgrade: Yes

Table A-2 Show Commands (continued)

Command	Parameters and Options	Description
show perf	list classes [**-t** *category*] [**-d**] **Options** - **-d**—Displays detailed information - **-t** *category*—Displays perfmon classes for the specified category	This commands lists the perfmon classes or objects. Command privilege level: 0 Allowed during upgrade: Yes
show perf	**list counters** *class-name* [**-d**] Where *class-name* represents a perfmon class name for which you want to list the counters. **Note** If the class name contains white spaces, enclose the name in double quotation marks. **Options** **-d**—Displays detailed information	This command lists perfmon counters for the specified perfmon class. Command privilege level: 0 Allowed during upgrade: Yes
show perf	**list instances** *class-name* [**-d**] Where *class-name* represents a perfmon class name for which you want to list the counters. **Note** If the class name contains white spaces, enclose the name in double quotation marks. **Options** **-d**—Displays detailed information	The command lists the perfmon instances for the specified perfmon class. Command privilege level: 0 Allowed during upgrade: Yes
show perf	**query class** *class-name* [,*class-name* ...] Where *class-name* specifies the perfmon class that you want to query. You can specify a maximum of 5 classes per command. **Note** If the class name contains white spaces, enclose the name in double quotation marks. **Options** None	This command queries a perfmon class and displays all the instances and counter values of each instance. Command privilege level: 0 Allowed during upgrade: Yes

Table A-2 Show Commands (continued)

Command	Parameters and Options	Description
show perf	**query counter** *class-name counter-name* [,*counter-name*...] Where • *class-name* specifies the perfmon class that you want to query. • *counter-name* specifies the counter to view. You can specify a maximum of 5 counters per command. **Note** If the class name or counter name contains white spaces, enclose the name in double quotation marks. **Options** None	This command queries the specified counter and displays the counter value of all instances. Command privilege level: 0 Allowed during upgrade: Yes
show perf	**query instance** *class-name instance-name* [,*instance-name*...] Where • *class-name* specifies the perfmon class that you want to query. • *instance-name* specifies the perfmon instance to view. You can specify a maximum of 5 instances per command. **Note** If the class name or instance name contains white spaces, enclose the name in double quotation marks. **Options** None	This command queries the specified instance and displays all its counter values. **Note** This command does not apply to singleton perfmon classes. Command privilege level: 0 Allowed during upgrade: Yes
show perf	**query path** *path-spec* [,*path-spec*...] Where *path-spec* gets defined as follows: • For an instance-based perfmon class, specify *path-spec* as *class-name*(*instance-name*)\counter-name. • For a noninstance-based perfmon class (a singleton), specify *path-spec* as *class-name\counter-name*. You can specify a maximum of 5 paths per command. **Note** If the path name contains white spaces, enclose the name in double quotation marks. **Options** None	This command queries a specified perfmon path. Command privilege level: 0 Allowed during upgrade: Yes **Example** `show perf query path “Cisco Phones(phone-0)\CallsAttempted”, “Cisco Unified CallManager\T1ChannelsActive”`

Table A-2 Show Commands (continued)

Command	Parameters and Options	Description
show process	**load** [**cont**] [**clear**] [**noidle**] [**num** *xx*] [**thread**] [**cpu**] [**memory**] [**time**] [**specified**] [**page**] **list [page] [short] [detail] [thread] [fd] [cont] [clear] [process id** *id***] [argument id** *id***] [owner name** *name***]** Where • **load** displays the CPU load for each active process. • **list** displays all processes. **Options** • **cont**—Command repeats continuously • **clear**—Clears screen before displaying output • **noidle**—Ignore idle or zombie processes • **num** *xx*—Sets the number of processes to display (Default=10, **all** = all processes) • **thread**—Displays threads • **cpu**—Displays output by CPU usage • **memory**—Sorts output by memory usage • short—Displays short listing • **time**—Sorts output by time usage • **page**—Displays one page at a time • **detail**—Displays a detailed listing • **process id** *id*—Shows only specific process number or command name • **argument name** *name*—Show only specific process with argument name • **thread**—Include thread processes in the listing • **fd**—Show file descriptors that are associated with a process	This command displays process and load information. Command privilege level: 1 Allowed during upgrade: Yes **Example: Show detailed process listing one page at a time** `show process list detail page`
show registry	*system component* **[***name***] [page]** **Where** • *system* represents the registry system name. • *component* represents the registry component name. • *name* represents the name of the parameter to show. **Note** To display all items, enter the wildcard character, *. **Display Options** **page**—Displays one page at a time	This command displays the contents of the registry. Command privilege level: 1 Allowed during upgrade: Yes **Example: show contents of the cm system, dbl/sdi component** `show registry cm dbl/sdi`

Table A-2 Show Commands (continued)

Command	Parameters and Options	Description
show risdb	**list** [**file** *filename*] **query** *table1 table2 table3* ... [**file** *filename*] Where - **list** displays the tables supported in the Realtime Information Service (RIS) database. - **query** displays the contents of the RIS tables. **Options** **file** *filename*—Outputs the information to a file **Note** The file option saves the information to platform/cli/*filename*.txt. The file name cannot contain the "." character.	This command displays RIS database table information. Command privilege level: 0 Allowed during upgrade: Yes **Example: Display list of RIS database tables** `show risdb list`
show smtp	None	This command displays the name of the SMTP host. Command privilege level: 0 Allowed during upgrade: Yes
show stats	**io** [**kilo**] [**detail**] [**page**] [**file** *filename*] **Options** - **kilo**—Displays statistics in kilobytes - **detail**—Displays detailed statistics on every available device on the system and overrides the kilo option - **file** *filename*—Outputs the information to a file **Note** The file option saves the information to platform/cli/*filename*.txt. The file name cannot contain the "." character.	This command displays system IO statistics. Command privilege level: 1 Allowed during upgrade: Yes
show status	None	This command displays the following basic platform status: - Host name - Date - Time zone - Locale - Product version - Platform version - CPU usage - Memory and disk usage Command privilege level: 0

Table A-2 Show Commands (continued)

Command	Parameters and Options	Description
show tech	**all** [**page**] [**file** *filename*] **Options** • **page**—Displays one page at a time • **file** *filename*—Outputs the information to a file **Note** The file option saves the information to platform/cli/*filename*.txt. The file name cannot contain the "." character.	This command displays the combined output of all **show tech** commands. Command privilege level: 1 Allowed during upgrade: Yes
show tech	**ccm_service** **Options** None	This command displays information on all Cisco Unified CallManager services that can run on the system. Command privilege level: 0 Allowed during upgrade: Yes
show tech	**database** **Options** None	This command creates a CSV file of the entire database. Command privilege level: 1 Allowed during upgrade: Yes
show tech	**dbinuse** **Options** None	This command displays the database in use. Command privilege level: 1 Allowed during upgrade: Yes
show tech	**dbschema** **Options** None	This command displays the database schema in a CSV file. Command privilege level: 1 Allowed during upgrade: Yes
show tech	**devdefaults** **Options** None	This command displays the device defaults table. Command privilege level: 1 Allowed during upgrade: Yes
show tech	**gateway** **Options** None	This command displays the gateway table from the database. Command privilege level: 1 Allowed during upgrade: Yes
show tech	locales **Options** None	This command displays the locale information for devices, device pools, and end users. Command privilege level: 1 Allowed during upgrade: Yes

Table A-2 Show Commands (continued)

Command	Parameters and Options	Description
show tech	**network** [**page**] [**file** *filename*] **Options** • **page**—Displays one page at a time • **file** *filename*—Outputs the information to a file **Note** The file option saves the information to platform/cli/*filename*.txt. The file name cannot contain the "." character.	This command displays network aspects of the server. Command privilege level: 1 Allowed during upgrade: Yes
show tech	**notify** **Options** None	This command displays the database change notify monitor. Command privilege level: 1 Allowed during upgrade: Yes
show tech	**params all** **Options** None	This command displays all the database parameters. Command privilege level: 1 Allowed during upgrade: Yes
show tech	**params enterprise** **Options** None	This command displays the database enterprise parameters. Command privilege level: 1 Allowed during upgrade: Yes
show tech	**params service** **Options** None	This command displays the database service parameters. Command privilege level: 1 Allowed during upgrade: Yes
show tech	**procedures** **Options** None	This command displays the procedures in use for the database. Command privilege level: 1 Allowed during upgrade: Yes
show tech	**routepatterns** **Options** None	This command displays the route patterns that are configured for the system. Command privilege level: 1 Allowed during upgrade: Yes
show tech	**routeplan** **Options** None	This command displays the route plan that are configured for the system. Command privilege level: 1 Allowed during upgrade: Yes

Table A-2 Show Commands (continued)

Command	Parameters and Options	Description
show tech	**runtime** [**page**] [**file** *filename*] **Options** **page**—Displays one page at a time **file** *filename*—Outputs the information to a file **Note** The file option saves the information to platform/cli/*filename*.txt. The file name cannot contain the "." character.	This command displays runtime aspects of the server. Command privilege level: 1 Allowed during upgrade: Yes
show tech	**systables** **Options** None	This command displays the name of all tables in the sysmaster database. Command privilege level: 1 Allowed during upgrade: Yes
show tech	**system** [**page**] [**file** *filename*] **Options** **page**—Displays one page at a time **file** *filename*—Outputs the information to a file **Note** The file option saves the information to platform/cli/*filename*.txt. The file name cannot contain the "." character.	This command displays system aspects of the server. Command privilege level: 1 Allowed during upgrade: Yes
show tech	**table** *table_name* [**page**] [**csv**] Where *table_name* represents the name of the table to display. **Options** **page**—Displays the output one page at a time **csv**—Sends the output to a comma separated values file	This command displays the contents of the specified database table. Command privilege level: 1 Allowed during upgrade: Yes
show tech	**triggers** **Options** None	This command displays table names and the triggers that are associated with those tables. Command privilege level: 1 Allowed during upgrade: Yes
show tech	**version [page]** **Options** Page—Displays the output one page at a time	This command displays the version of the installed components. Command privilege level: 1 Allowed during upgrade: Yes

Table A-2 Show Commands (continued)

Command	Parameters and Options	Description
show timezone	**config** **list** [**page**] Where • **config** displays the current time zone settings. • **list** displays the available time zones. **Options** **page**—Displays the output one page at a time	This command displays time zone information. Command privilege level: 0 Allowed during upgrade: Yes
show trace	[*task_name*] Where *task_name* represents the name of the task for which you want to display the trace information. **Note** If you do not enter any parameters, the command returns a list of available tasks. **Options** None	This command displays trace information for a particular task. Command privilege level: 0 Allowed during upgrade: Yes **Example: Display trace information for cdp** `show trace cdps`
show version	**active** **inactive** **Options** None	This command displays the software version on the active or inactive partition. Command privilege level: 0 Allowed during upgrade: Yes
show web-security	None	This command displays the contents of the current web-security certificate. Command privilege level: 0 Allowed during upgrade: Yes
show workingdir	None	This command retrieves the current working directory for activelog, inactivelog, install, and TFTP. Command privilege level: 0 Allowed during upgrade: Yes

Set Commands

The following table lists and explains the CLI Set commands.

Table A-3 Set Commands

Command	Parameters	Description
set account	*name* Where *name* represents the username for the new account. **Note** After you enter the username, the system prompts you to enter the privilege level and password for the new account. **Options** None	This command sets up a new account on the operating system. Command privilege level: 0 Allowed during upgrade: No
set cert	**regen** *unit-name* Where *unit-name* represents the name of the certificate that you want to regenerate. **Options** None	This command enables you to regenerate the specified security certificate. Command privilege level: 1 Allowed during upgrade: No
set commandcount	{**enable** | **disable**} **Options** None	This command changes the CLI command prompt, so it displays how many CLI commands have executed. Command privilege level: 0 Allowed during upgrade: Yes
set ipsec	**policy** {**ALL** | *policy-name*} **association** *policy-name* {**ALL** | *association-name*} Where • *policy-name* represents an IPSec policy. • *association-name* represents an IPSec association. **Options** None	This command allows you to set IPSec policies and associations. Command privilege level: 1 Allowed during upgrade: No
set logging	{**enable** | **disable**} **Options** None	This command allows you to enable or disable logging. Command privilege level: 0 Allowed during upgrade: Yes

Table A-3 Set Commands (continued)

Command	Parameters	Description
set network	**dhcp eth0** {**enable** | **disable**} Where - **eth0** specifies Ethernet interface 0. The system asks whether you want to continue to execute this command. Warning **If you continue, this command causes the system to restart. Cisco also recommends that you restart all nodes whenever any IP address gets changed.** **Options** None	This command enables or disables DHCP for Ethernet interface 0. You cannot configure Ethernet interface 1. Command privilege level: 1 Allowed during upgrade: No
set network	**dns** {**primary** | **secondary**} *ip-address* Where *ip-address* represents the IP address of the primary or secondary DNS server. The system asks whether you want to continue to execute this command. Warning **If you continue, this command causes a temporary loss of network connectivity.** **Options** None	This command sets the IP address for the primary or secondary DNS server. Command privilege level: 1 Allowed during upgrade: No
set network	**dns options** [**timeout** *seconds*] [**attempts** *number*] [**rotate**] Where - **timeout** sets the DNS request timeout. - **attempts** sets the number of times to attempt a DNS request before quitting. - **rotate** causes the system to rotate among the configured DNS servers, distributing the load. - *seconds* specifies the DNS timeout period, in seconds. - *number* specifies the number of attempts. **Options** None	This command sets DNS options. Command privilege level: 0 Allowed during upgrade: Yes

Table A-3 Set Commands (continued)

Command	Parameters	Description
set network	**domain** *domain-name* Where *domain-name* represents the system domain that you want to assign. The system asks whether you want to continue to execute this command. **Warning** **If you continue, this command causes a temporary loss of network connectivity.** **Options** None	This command sets the domain name for the system. Command privilege level: 1 Allowed during upgrade: No
set network	**failover** {**enable** | **disable**} Where • **enable** enables Network Fault Tolerance. • **disable** disables Network Fault Tolerance. **Options** None	This command enables and disables Network Fault Tolerance. Command privilege level: 1 Allowed during upgrade: No
set network	**gateway** *ip-address* Where *ip-address* represents the IP address of the network gateway that you want to assign. The system asks whether you want to continue to execute this command. **Warning** **If you continue, this command causes the system to restart.** **Options** None	This command enables you to configure the IP address of the network gateway. Command privilege level: 1 Allowed during upgrade: No

Table A-3 Set Commands (continued)

Command	Parameters	Description
set network	**ip eth0** *ip-address ip-mask* Where • **eth0** specifies Ethernet interface 0. • *ip-address* represents the IP address that you want assign. • *ip-mask* represents the IP mask that you want to assign. The system asks whether you want to continue to execute this command. **Caution** If you continue, this command causes the system to restart. **Options** None	This command sets the IP address for Ethernet interface 0. You cannot configure Ethernet interface 1. Command privilege level: 1 Allowed during upgrade: No
set network	**mtu** *mtu_max* Where *mtu_max* specifies the maximum MTU value. The system asks whether you want to continue to execute this command. **Caution** If you continue, the system will temporarily lose network connectivity. **Options** None	This command sets the maximum MTU value.
set network	**max_ip_conntrack** *ip_conntrack_max* Where *ip_conntrack_max* specifies the value for ip_conntrack_max.	This command sets the ip_conntrack_max value.

Table A-3 Set Commands (continued)

Command	Parameters	Description
set network	**nic eth0** [**auto en** | **dis**] [**speed 10** | **100**] [**duplex half** | **full**] Where - **eth0** specifies Ethernet interface 0. - **auto** specifies whether auto negotiation gets enabled or disabled. - **speed** specifies whether the speed of the Ethernet connection: 10 or 100 Mbps. - **duplex** specifies half-duplex or full-duplex. The system asks whether you want to continue to execute this command. **Note** You can enable only one active NIC at a time. **Caution** If you continue, this command causes a temporary loss of network connections while the NIC gets reset. **Options** None	This command sets the properties of the Ethernet Interface 0. You cannot configure Ethernet interface 1. Command privilege level: 1 Allowed during upgrade: No
set network	**pmtud** [**enable** | **disable**] Where - **enable** enables Path MTU Discovery. - **disable** disables Path MTU Discovery. The system asks whether you want to continue to execute this command. **Caution** If you continue, the system will temporarily lose network connectivity. **Options** None	This command enables and disables Path MTU Discovery.
set network	**status eth0** {**up** | **down**} Where **eth0** specifies Ethernet interface 0. **Options** None	This command sets the status of Ethernet 0 to up or down. You cannot configure Ethernet interface 1. Command privilege level: 1 Allowed during upgrade: No

Table A-3 Set Commands (continued)

Command	Parameters	Description
set password	{**admin** | **security**} The systems prompts you for the old and new passwords. **Note** The password must contain at least six characters, and the system checks it for strength.	This command allows you to change the administrator and security passwords. Command privilege level: 1 Allowed during upgrade: No
set smtp	*hostname* Where *hostname* represents the SMTP server name. **Options** None	This command sets the SMTP server hostname. Command privilege level: 0 Allowed during upgrade: No
set timezone	*timezone* **Note** Enter enough characters to uniquely identify the new time zone. Be aware that the time-zone name is case-sensitive. ⚠ **Caution** You must restart the system after you change the time zone. **Options** None	This command lets you change the system time zone. Command privilege level: 0 Allowed during upgrade: No **Example: Set the time zone to Pacific time** `set timezone Pac`

Table A-3 Set Commands (continued)

Command	Parameters	Description
set trace	**enable Error** *tname* **enable Special** *tname* **enable State_Transition** *tname* **enable Significant** *tname* **enable Entry_exit** *tname* **enable Arbitrary** *tname* **enable Detailed** *tname* **disable** *tname* Where • *tname* represents the task for which you want to enable or disable traces. • **enable Error** sets task trace settings to the error level. • **enable Special** sets task trace settings to the special level. • **enable State_Transition** sets task trace settings to the state transition level. • **enable Significant** sets task trace settings to the significant level. • **enable Entry_exit** sets task trace settings to the entry_exit level. • **enable Arbitrary** sets task trace settings to the arbitrary level. • **enable Detailed** sets task trace settings to the detailed level. • **disable** unsets the task trace settings. **Options** None	This command sets trace activity for the the specified task. Command privilege level: 1 Allowed during upgrade: No

Table A-3 Set Commands (continued)

Command	Parameters	Description
set web-security	*orgunit orgname locality state country* Where • *orgunit* represents the organizational unit. • *orgname* represents the organizational name. • *locality* represents the organization location. • *state* represents the organization state. • *country* represents the organization country. **Options** None	This command sets the web security certificate information for the operating system. Command privilege level: 0 Allowed during upgrade: No
set workingdir	**activelog** *directory* **inactivelog** *directory* **install** *directory* **tftp** *directory* Where • **activelog** sets the working directory for active logs. • **inactivelog** set the working directory for inactive logs. • **install** sets the working directory for installation logs. • **tftp** sets the working directory for TFTP files. • *directory* represents the current working directory. **Options** None	This command sets the working directory for active, inactive, and installation logs. Command privilege level: 0 for logs, 1 for TFTP Allowed during upgrade: Yes

Unset Commands

The following table lists and explains the CLI Unset commands:

Table A-4 Unset Commands

Command	Parameters	Description
unset ipsec	**policy** {**ALL** | *policy-name*} **association** *policy-name* {**ALL** | *association-name*} Where • *policy-name* represents the name of an IPSec policy. • *association-name* represents the name of an IPSec association. **Options** None	This command allows you to disable IPSec policies and associations. Command privilege level: 1 Allowed during upgrade: No
unset network	**dns options** [**timeout**] [**attempts**] [**rotate**] Where • **timeout** sets the wait time before the system considers a DNS query failed to the default. • **attempts** sets the number of DNS attempts to make before failing to the default. • **rotate** sets the method for selecting a nameserver to the default. This affects how loads are distributed across nameservers. The system asks whether you want to continue to execute this command. ⚠ **Caution** If you continue, the system will temporarily lose network connectivity. **Options** None	This command unsets DNS options.

Delete Commands

The following table lists and explains the CLI Delete commands:

Table A-5 Delete Commands

Command	Parameters	Description
delete account	*account-name* Where *account-name* represents the name of an administrator account. **Options** None	This command allows you to delete an administrator account. Command privilege level: 4 Allowed during upgrade: No
delete dns	*ip-address* Where *ip-address* represents the IP address of the DNS server you want to delete. The system asks whether you want to continue to execute this command. **Warning** **If you continue, this command causes a temporary loss of network connectivity.** **Options** None	This command allows you to delete the IP address for a DNS server. Command privilege level: 1 Allowed during upgrade: No
delete ipsec	**policy** {**ALL** | *policy-name*} **association** *policy name* {**ALL** | *association-name*} Where • *policy-name* represents an IPSec policy. • *association-name* represents an IPSec association. **Options** None	This command allows you to delete IPSec policies and associations. Command privilege level: 1 Allowed during upgrade: No

Table A-5 Delete Commands (continued)

Command	Parameters	Description
delete process	*process-id* [**force** | **terminate** | **crash**] Where • *process-id* represents the process ID number. **Options** • **force—**Tells the process to stop • **terminate**—Tells the operating system to terminate the process • **crash**—Crashes the process and produces a crash dump **Note** Use the **force** option only if the command alone does not delete the process and use the **terminate** option only if **force** does not delete the process.	This command allows you to delete a particular process. Command privilege level: 1 Allowed during upgrade: Yes
delete smtp	None	This command allows you to delete the SMTP host. Command privilege level: 1 Allowed during upgrade: No

Utility Commands

The following table lists and explains the CLI Utility commands:

Table A-6 Utility Commands

Command	Parameters	Description
utils core	list	This command lists all existing core files.
utils core	**analyze** *core file name* Where *core file name* specifies the name of a core file. **Options** None	This command generates a backtrace for the specified core file, a thread list, and the current value of all CPU registers. The command creates a file of the same name as the core file, with a .txt extension, in the same directory as the core file. This command works only on the active partition
utils csa	**disable** The system disables CSA. **Options** None	This command stops Cisco Security Agent (CSA). Command privilege level: 1 Allowed during upgrade: No

Table A-6 Utility Commands (continued)

Command	Parameters	Description
utils csa	**enable** The system prompts you to confirm that you want to enable CSA. ⚠ **Caution** You must restart the system after you start CSA. **Options** None	This command enables Cisco Security Agent (CSA). Command privilege level: 1 Allowed during upgrade: No
utils csa	**status** The system indicates whether CSA is running. **Options** None	This command displays the current status of Cisco Security Agent (CSA). Command privilege level: 0 Allowed during upgrade: No
utils dbreplication	status **Options** None	This command displays the status of database replication.
utils dbreplication	stop **Options** None	This command stops the automatic setup of database replication.
utils dbreplication	repair **Options** None	This command repairs database replication.
utils dbreplication	reset **Options** None	This command resets and restarts database replication.
utils disaster_ recovery	**backup tape** *tapeid* Where *tapeid* represents the ID of an available tape device. **Options** None	This command starts a backup job and stores the resulting tar file on tape. Command privilege level: 1 Allowed during upgrade: Yes

Table A-6 Utility Commands (continued)

Command	Parameters	Description
utils disaster_ recovery	**backup** network *path servername username* Where • *path* represents the location of the backup files on the remote server. • *servername* represents the IP address or host name of the server where you stored the backup files. • *username* represents the username that is needed to log in to the remote server. **Note** The system prompts you to enter the password for the account on the remote server. **Options** None	This command starts a backup job and stores the resulting tar file on a remote server. Command privilege level: 1 Allowed during upgrade: Yes
utils disaster_ recovery	**cancel_bakckup** The system prompts you to confirm that you want to cancel the backup job. **Options** None	This command cancels the ongoing backup job. Command privilege level: 1 Allowed during upgrade: Yes
utils disaster_ recovery	**configure_features** *features* Where *features* specifies one or more features to include in the disaster recovery backup. Separate feature names with commas (,). **Options** None	This command allows you to configure the features that the disaster recovery system backs up. Use the command **utils disaster_recovery show_registration** to see a list of the features that are registered on the server. Command privilege level: 1 Allowed during upgrade: No
utils disaster_ recovery	**restore tape** *server tarfilename tapeid* Where • *server* specifies the hostname of the server that you want to restore. • *tarfilename* specifies the name of the file to restore. • *tapeid* specifies the name of the tape device from which to perform the restore job. **Options** None	This command starts a restore job and takes the backup tar file from tape. Command privilege level: 1 Allowed during upgrade: Yes

Table A-6 Utility Commands (continued)

Command	Parameters	Description
utils disaster_ recovery	**restore network** *restore_server tarfilename path servername username* Where - *restore_server* specifies the hostname of the server that you want to restore. - *tarfilename* specifies the name of the file to restore. - *path* represents the location of the backup files on the remote server. - *servername* represents the IP address or host name of the server where you stored the backup files. - *username* represents the username that is needed to log in to the remote server. **Note** The system prompts you to enter the password for the account on the remote server. **Options** None	This command starts a restore job and takes the backup tar file from a remote server. Command privilege level: 1 Allowed during upgrade: Yes
utils disaster_ recovery	show_backupfiles network *path servername username* Where - *path* represents the location of the backup files on the remote server. - *servername* represents the IP address or host name of the server where you stored the backup files. - *username* represents the username that is needed to log in to the remote server. **Note** The system prompts you to enter the password for the account on the remote server. **Options** None	This command displays information about the backup files that are stored on a remote server. Command privilege level: 1 Allowed during upgrade: No
utils disaster_ recovery	**show_bakcupfiles tape** *tapeid* Where *tapeid* represents the ID of an available tape device. **Options** None	This command displays information about the backup files that are stored on a tape. Command privilege level: 1 Allowed during upgrade: No

Table A-6 Utility Commands (continued)

Command	Parameters	Description
utils disaster_ recovery	**show_registration** *hostname* Where *hostname* specifies the server for which you want to display registration information. **Options** None	This command displays the registered features and components on the specified server. Command privilege level: 1 Allowed during upgrade: No
utils disaster_ recovery	**show_tapeid** **Options** None	This command displays a list of tape device IDs. Command privilege level: 1 Allowed during upgrade: No
utils disaster_ recovery	**status** *operation* Where *operation* specifies the name of the ongoing operation: **backup** or **restore**. **Options** None	This command displays the status of the current backup or restore job. Command privilege level: 1 Allowed during upgrade: No
utils iothrottle	enable **Options** None	This command enables I/O throttling enhancements. When enabled, I/O throttling enhancements lower the impact of upgrades on an active system.
utils iothrottle	disable **Options** None	This command disables I/O throttling enhancements. This could adversely affect the system during upgrades.
utils iothrottle	status **Options** None	This command displays the status of I/O throttling enhancements.

Table A-6 Utility Commands (continued)

Command	Parameters	Description
utils netdump	**client start** *ip-address-of-netdump-server* **client status** **client stop** Where • **client start** starts the netdump client. • **client status** displays the status of the netdump client. • **client stop** stops the netdump client. • *ip-address-of-netdump-server* specifies the IP address of the netdump server to which the client will send diagnostic information. **Options** None	This command configures the netdump client. In the event of a kernel panic crash, the netdump client sends diagnostic information about the crash to a netdump server. Command privilege level: 0 Allowed during upgrade: No
utils netdump	**server add-client** *ip-address-of-netdump-client* **server delete-client** *ip-address-of-netdump-client* **server list-clients** **server start** **server status** **server stop** Where • **server add-client** adds a netdump client. • **server delete-client** deletes a netdump client. • **server list-clients** lists the clients that are registered with this netdump server. • **server start** starts the netdump server. • **server status** displays the status of the netdump server. • **server stop** stops the netdump server. • *ip-address-of-netdump-client* specifies the IP address of a netdump client. **Options** None	This command configures the netdump server. In the event of a kernel panic crash, a netdump-enabled client system sends diagnostic information about the crash to the netdump server. The following location on the netdump server stores the netdump diagnostic information: /var/log/active/crash/. The subdirectories whose names comprise a client IP address and a date contain netdump information. You can configure each Cisco Unified Communications Operating System server as both a netdump client and server. If the server is on another Cisco Unified Communications Operating System server, only the kernel panic trace signature gets sent to the server; otherwise, an entire core dump gets sent. Command privilege level: 0 Allowed during upgrade: No

Table A-6 Utility Commands (continued)

Command	Parameters	Description
utils network	**arp list** [**host** *host*][**page**][**numeric**] **arp set** {*host*} {*address*} **arp delete** *host* Where • **arp list** lists the contents of the address resolution protocol table. • **arp set** sets an entry in the address resolution protocol table. • **arp delete** deletes an entry in the address resolution table. • *host* represents the host name or IP address of the host to add or delete to the table. • *address* represents the MAC address of the host to be added. Enter the MAC address in the following format: XX:XX:XX:XX:XX:XX. **Options** **page**—Displays the output one page at a time **numeric**—Displays hosts as dotted IP addresses	This command lists, sets, or deletes Address Resolution Protocol (ARP) table entries. Command privilege level: 0 Allowed during upgrade: Yes

Table A-6 Utility Commands (continued)

Command	Parameters	Description
utils network	**capture eth0** [*page*] [*numeric*] [**file** *fname*] [**count** *num*] [**size** *bytes*] [**src** *addr*] [**dest** *addr*] [**port** *num*] Where **eth0** specifies Ethernet interface 0. **Options** • **page**—Displays the output one page at a time **Note** When you use the page or file options, the complete capture of all requested packets must occur before the command completes. • **numeric**—Displays hosts as dotted IP addresses • **file** *fname*—Outputs the information to a file **Note** The file option saves the information to platform/cli/*fname*.cap. The filename cannot contain the "." character. **count** *num*—Sets a count of the number of packets to capture **Note** For screen output, the maximum count equals 1000, and, for file output, the maximum count equals 10,000. • **size** *bytes*—Sets the number of bytes of the packet to capture **Note** For screen output, the maximum number of bytes equals 128, for file output, the maximum of bytes can be any number or **ALL** • **src** *addr*—Specifies the source address of the packet as a host name or IPV4 address • **dest** *addr*—Specifies the destination address of the packet as a host name or IPV4 address • **port** *num*—Specifies the port number of the packet, either source or destination	This command captures IP packets on the specified Ethernet interface. You can display the packets on the screen or save them to a file. Line wrapping can occur in the output. Command privilege level: 0 Allowed during upgrade: Yes
utils network	**host** *hostname* [**server** *server-name*] [**page**] [**detail**] [**srv]** Where *hostname* represents the host name or IP address that you want to resolve. **Options** *server-name*—Specifies an alternate domain name server **page**—Displays the output one screen at a time **detail**—Displays a detailed listing **srv**—Displays DNS SRV records.	This command resolves a host name to an address or an address to a host name. Command privilege level: 0 Allowed during upgrade: Yes

Table A-6 Utility Commands (continued)

Command	Parameters	Description
utils network	**ping** *destination* [*count*] Where *destination* represents the hostname or IP address of the server that you want to ping. **Options** *count*—Specifies the number of times to ping the external server. The default count equals 4.	This command allows you to ping another server. Command privilege level: 0 Allowed during upgrade: Yes
utils network	**tracert** *destination* Where *destination* represents the hostname or IP address of the server to which you want to send a trace. **Options** None	This command traces IP packets that are sent to a remote destination. Command privilege level: 0 Allowed during upgrade: Yes
utils ntp	{**status** | **config**}	This command displays the NTP status or configuration. Command privilege level: 0 Allowed during upgrade: Yes
utils remote_ account	**status** **enable** **disable** **create** *username life* Where • *username* specifies the name of the remote account. The username, which can contain only lowercase characters, must comprise more than six-characters. • *life* specifies the life of the account in days. After the specified number of day, the account expires. **Note** You can have only one remote account that is enabled at a time. **Options** None	This command allows you to enable, disable, create, and check the status of a remote account. **Note** A remote account generates a pass phrase that allows Cisco Systems support personnel to get access to the system for the specified life of the account. Command privilege level: 1 Allowed during upgrade: Yes **Example** `utils remote_account status`
utils service	**list** [**page**] **Options** **page**—Displays the output one page at a time	This command retrieves a list of all services and their status. Command privilege level: 0 Allowed during upgrade: Yes

Table A-6 Utility Commands (continued)

Command	Parameters	Description
utils service	**start** *service-name* **stop** *service-name* **restart** *service-name* Where *service-name* represents the name of the service that you want to stop or start: • System NTP • System SSH • Service Manager • A Cisco DB • Cisco Tomcat • Cisco Database Layer Monitor • Cisco Unified CallManager Serviceability **Options** None	This command stops, starts, or restarts a service. Command privilege level: 1 Allowed during upgrade: No
utils sftp	**handshake** **Options** None	This command exchanges SFTP SSH keys to all members of the cluster.
utils snmp	**test** **Options** None	This commands tests the SNMP host by sending sample alarms to local syslog, remote syslog, and SNMP trap. Command privilege level: 0 Allowed during upgrade: No
utils soap	**realtimeservice test** *remote-ip remote-https-user remote-https-password* Where • *remote-ip* specifies the IP address of the server under test. • *remote-https-user* specifies a username with access to the SOAP API. • *remote-https-password* specifies the password for the account with SOAP API access. **Options** None	This command executes a number of test cases on the remote server. Command privilege level: 0 Allowed during upgrade: N

Table A-6 Utility Commands (continued)

Command	Parameters	Description
utils system	{**restart** | **shutdown** | **switch-version**} **Note** The system prompts you to confirm the action that you choose. The **utils system shutdown** command has a 5-minute timeout. If the system does not shut down within 5 minutes, the command gives you the option of doing a forced shutdown.	This command allows you to restart the system on the same partition, restart the system on the inactive partition, or shut down the system. Command privilege level: 1 Allowed during upgrade: No

Run Commands

The following table lists and explains the CLI Run commands:

Table A-7 Run Commands

Command	Parameters	Description
run sql	*sql_statement* Where sql_statement represents the SQL command to run. **Options** None	This command allows you to run an SQL command. Command privilege level: 1 Allowed during upgrade: No **Example: Run an SQL command** `run sql select name from device`

INDEX