



Cisco Unified Communications Operating System Administration Guide

Release 6.0(1)

Americas Headquarters

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

Text Part Number: OL-12538-01

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, iPhone, 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. (0612R)

Cisco Unified Communications Operating System Administration Guide
© 2007 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface xi

CHAPTER 1

| | |
|---|------------|
| Introduction | 1-1 |
| Overview | 1-1 |
| Browser Requirements | 1-1 |
| Operating System Status and Configuration | 1-2 |
| Settings | 1-2 |
| Security Configuration | 1-3 |
| Software Upgrades | 1-3 |
| Services | 1-3 |
| Command Line Interface | 1-3 |

CHAPTER 2

| | |
|---|------------|
| Log In To Cisco Unified Communications Operating System Administration | 2-1 |
| Logging In To Cisco Unified Communications Operating System Administration | 2-1 |
| Recovering the Administrator Password | 2-2 |

CHAPTER 3

| | |
|---------------------------------|------------|
| Status and Configuration | 3-1 |
| Cluster Nodes | 3-1 |
| Hardware Status | 3-2 |
| Network Status | 3-2 |
| Installed Software | 3-3 |
| System Status | 3-4 |
| Rebuilding RAID Drives | 3-4 |

CHAPTER 4

| | |
|---|------------|
| Settings | 4-1 |
| IP Settings | 4-1 |
| Ethernet Settings | 4-1 |
| Publisher Settings | 4-2 |
| Changing IP Address on a Subsequent Cisco Unified Communications Manager Node | 4-2 |
| NTP Servers | 4-3 |
| SMTP Settings | 4-3 |
| Time Settings | 4-4 |

CHAPTER 5

System Restart 5-1

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

CHAPTER 6

Security 6-1

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

CHAPTER 7

Software Upgrades 7-1

- Software Upgrade and Installation 7-1
 - Upgrading to Cisco Unified Communications Manager Release 6.0(1) 7-2
 - Obtaining the Upgrade File 7-2
 - Upgrading from Local Source 7-2
 - Upgrading from Remote Source 7-3
 - Stalled Upgrades 7-5
 - Reverting to a Previous Version 7-5
- Dial Plan Installation 7-5
- Locale Installation 7-6
 - Installing Locales 7-6
 - Locale Files 7-7

| | |
|---|-----|
| Error Messages | 7-7 |
| Supported Cisco Unified Communications Products | 7-8 |
| Managing TFTP Server Files | 7-8 |

CHAPTER 8

| | |
|-----------------|------------|
| Services | 8-1 |
| Ping | 8-1 |
| Remote Support | 8-2 |

APPENDIX A

| | |
|---------------------------------|------------|
| Command Line Interface | A-1 |
| Overview | A-1 |
| Starting a CLI Session | A-1 |
| CLI Basics | A-2 |
| Completing Commands | A-2 |
| Getting Help on Commands | A-2 |
| Ending a CLI Session | A-3 |
| Cisco IPT Platform CLI Commands | A-3 |
| delete account | A-3 |
| delete dns | A-4 |
| delete ipsec | A-4 |
| delete process | A-5 |
| delete smtp | A-5 |
| file check | A-5 |
| file delete | A-6 |
| file dump | A-7 |
| file get | A-8 |
| file list | A-9 |
| file search | A-10 |
| file tail | A-11 |
| file view | A-11 |
| run sql | A-12 |
| set account | A-13 |
| set commandcount | A-13 |
| set ipsec | A-13 |
| set logging | A-14 |
| set network dhcp | A-14 |
| set network dns | A-14 |
| set network dns options | A-15 |
| set network domain | A-15 |
| set network failover | A-16 |

| | |
|-----------------------------|------|
| set network gateway | A-16 |
| set network ip | A-17 |
| set network mtu | A-17 |
| set network max_ip_contrack | A-17 |
| set network nic | A-18 |
| set network pmtud | A-18 |
| set network status | A-19 |
| set password | A-19 |
| set smtp | A-19 |
| set timezone | A-20 |
| set trace | A-20 |
| set web-security | A-21 |
| set workingdir | A-21 |
| show account | A-22 |
| show cert | A-22 |
| show environment | A-23 |
| show firewall list | A-23 |
| show hardware | A-24 |
| show ipsec | A-24 |
| show logins | A-25 |
| show memory | A-25 |
| show myself | A-25 |
| show network | A-26 |
| show open | A-27 |
| show packages | A-27 |
| show perf counterhelp | A-28 |
| show perf list categories | A-28 |
| show perf list classes | A-28 |
| show perf list counter | A-29 |
| show perf list instances | A-29 |
| show perf query class | A-30 |
| show perf query counter | A-30 |
| show perf query instance | A-30 |
| show perf query path | A-31 |
| show process | A-31 |
| show registry | A-32 |
| show risdb | A-33 |
| show smtp | A-34 |
| show stats io | A-34 |
| show status | A-34 |

| | |
|-----------------------------|------|
| show tech all | A-35 |
| show tech ccm_service | A-35 |
| show tech database | A-35 |
| show tech dbintegrity | A-36 |
| show tech dbinuse | A-36 |
| show tech dbschema | A-36 |
| show tech dbstateinfo | A-36 |
| show tech devdefaults | A-37 |
| show tech gateway | A-37 |
| show tech locales | A-37 |
| show tech network | A-37 |
| show tech notify | A-38 |
| show tech params all | A-38 |
| show tech params enterprise | A-38 |
| show tech params service | A-39 |
| show tech prefs | A-39 |
| show tech procedures | A-39 |
| show tech routepatterns | A-39 |
| show tech routeplan | A-39 |
| show tech runtime | A-40 |
| show tech systables | A-40 |
| show tech system | A-40 |
| show tech table | A-41 |
| show tech triggers | A-41 |
| show tech version | A-41 |
| show timezone | A-42 |
| show trace | A-42 |
| show ups status | A-43 |
| show version | A-43 |
| show web-security | A-43 |
| show workingdir | A-43 |
| unset ipsec | A-44 |
| unset network | A-44 |
| utils core list | A-45 |
| utils core analyze | A-45 |
| utils csa disable | A-45 |
| utils csa enable | A-45 |
| utils csa status | A-46 |
| utils dbreplication status | A-46 |
| utils dbreplication stop | A-46 |

utils dbreplication repair **A-46**

utils dbreplication reset **A-46**

utils disaster_recovery backup tape **A-47**

utils disaster_recovery backup network **A-47**

utils disaster_recovery cancel_backup **A-47**

utils disaster_recovery restore tape **A-48**

utils disaster_recovery restore network **A-48**

utils disaster_recovery show_backupfiles network **A-49**

utils disaster_recovery show_backupfiles tape **A-49**

utils disaster_recovery show_registration **A-49**

utils disaster_recovery show_tapeid **A-50**

utils disaster_recovery status **A-50**

utils fior **A-50**

utils iothrottle enable **A-51**

utils iothrottle disable **A-51**

utils iothrottle status **A-51**

utils netdump client **A-51**

utils netdump server **A-52**

utils network arp **A-53**

utils network capture eth0 **A-53**

utils network host **A-54**

utils network ping **A-55**

utils network tracert **A-55**

utils ntp **A-55**

utils remote_account **A-56**

utils reset_ui_administrator_name **A-56**

utils reset_ui_administrator_password **A-56**

utils service list **A-57**

utils service **A-57**

utils sftp handshake **A-58**

utils snmp test **A-58**

utils soap_realtimeservice test **A-58**

utils system **A-58**

utils system upgrade **A-59**

INDEX



Preface

Purpose

This document 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

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

Organization

The following table shows how this guide is organized:

| Chapter | Description |
|--|--|
| Introduction | This chapter provides an overview of the functions that are available through the Cisco Unified Communications Operating System. |
| Log In To Cisco Unified Communications Operating System Administration | This chapter provides procedures for logging in to the Cisco Unified Communications Operating System and for recovering a lost Administrator password. |
| Status and Configuration | This chapter provides procedures for displaying operating system status and configuration settings. |
| Settings | This chapter provides procedures for viewing and changing the Ethernet settings, IP settings, and NTP settings. |
| System Restart | This chapter provides procedures for restarting and shutting down the system. |
| Security | This chapter provides procedures for certificate management and for IPSec management. |

| Chapter | Description |
|--|---|
| 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 *Cisco Unified Communications Manager Documentation Guide* for further information about related Cisco IP telephony applications and products.

Conventions

This document uses the following conventions:

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

Notes use the following conventions:



Note

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

Timesavers use the following conventions:

**Timesaver**

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

Tips use the following conventions:

**Tip**

Means *the information contains useful tips*.

Cautions use the following conventions:

**Caution**

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

Warnings use the following conventions:

**Warning**

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

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: <http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>. If you require further assistance please contact us by sending email to export@cisco.com.



CHAPTER 1

Introduction

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

This chapter comprises the following topics:

- [Overview](#)
- [Browser Requirements](#)
- [Operating System Status and Configuration](#)
- [Security Configuration](#)
- [Software Upgrades](#)
- [Services](#)
- [Command Line Interface](#)

Overview

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

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

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

Browser Requirements

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

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

**Note**

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

The URL of the Cisco Unified Communications Operating System server (**https://servername**) must be included in the browser's "Trusted Site Zone" or the "Local Intranet Site Zone" for all product features to work correctly.

Operating System Status and Configuration

From the **Show** menu, you can check the status of various operating system components, including

- Cluster and nodes
- Hardware
- Network
- System
- Installed software and options

For more information see [Chapter 3, "Status and Configuration."](#)

Settings

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

- IP—Updates the IP addresses and Dynamic Host Configuration Protocol (DHCP) client settings that were entered when the application was installed.
- NTP Server settings—Configures the IP addresses of an external NTP server; add or delete an NTP server.
- SMTP settings—Configures the SMTP host that the operating system will use for sending e-mail notifications.

For more information see [Chapter 4, "Settings."](#)

From the **Settings > Version** window, you can choose from the following options for restarting or shutting down the system:

- Switch Versions—Switches the active and inactive disk partitions and restarts the system. You normally choose this option after the inactive partition has been updated and you want to start running a newer software version.
- Current Version—Restarts the system without switching partitions.
- Shutdown System—Stops all running software and shuts down the server.

**Note**

This command does not power down the server. To power down the server, press the power button.

For more information see [Chapter 5, "System Restart."](#)

Security Configuration

The operating system security options enable you to manage security certificates and Secure Internet Protocol (IPSec). From the **Security** menu, you can choose the following security options:

- **Certificate Management**—Manages certificates, Certificate Trust Lists (CTL), and Certificate Signing Requests (CSR). You can display, upload, download, delete, and regenerate certificates. Through Certificate Management, you can also monitor the expiration dates of the certificates on the server.
- **IPSEC Management**—Displays or updates existing IPSEC policies; sets up new IPSEC policies and associations.

For more information see [Chapter 6, “Security.”](#)

Software Upgrades

The software upgrade options enable you to upgrade the software version that is running on the operating system or to install specific software options, including Cisco Unified Communications Operating System Locale Installers, dial plans, and TFTP server files.

From the **Install/Upgrade** menu option, you can upgrade system software from either a local disc or a remote server. The upgraded software gets installed on the inactive partition, and you can then restart the system and switch partitions, so the system starts running on the newer software version.

**Note**

For Cisco Unified Communications Operating System 6.0(1), you must do all software installations and upgrades by using the software upgrades features included in the Cisco Unified Communications Operating System GUI and CLI user interfaces. The system can upload and process only software that Cisco Systems approved. You cannot install or use third-party or Windows-based software applications that you may have been using with a previous version of Cisco Unified Communications Operating System with Cisco Unified Communications Manager 6.0(1).

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

A command line interface is accessible from the console or through a secure shell connection to the server. For more information see [Appendix A, “Command Line Interface.”](#)



CHAPTER 2

Log In To Cisco Unified Communications Operating System Administration

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

Logging In To Cisco Unified Communications Operating System Administration

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

**Note**

Do not use the browser controls (for example, the Back button) while you are using Cisco Unified Communications Operating System Administration.

Procedure

- Step 1** Log in to Cisco Unified Communications Manager Administration.
- Step 2** From the Navigation menu in the upper, right corner of the Cisco Unified Communications Manager Administration window, choose **Cisco Unified OS Administration** and click **Go**.

The Cisco Unified Communications Operating System Administration Logon window displays.

**Note**

You can also access Cisco Unified Communications Operating System Administration directly by entering the following URL:
`http://server-name/cmplatform`

- Step 3** Enter your Administrator username and password.

**Note**

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

- Step 4** Click **Submit**.

The Cisco Unified Communications Operating System Administration window displays.

Recovering 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.



CHAPTER 3

Status and Configuration

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

- [Cluster Nodes](#)
- [Hardware Status](#)
- [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 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 |
|----------------------|---|
| Platform Type | Displays the model identity of the platform server. |
| Processor Speed | Displays the processor speed. |
| 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. |
| Object ID | Displays the object ID. |
| OS Version | Displays the operating system version. |

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 | Displays the date and time based on the continent and region that were specified during operating system installation. |
| Time Zone | Displays the time zone that was chosen during installation. |
| Locale | Displays the language that was chosen during operating system installation. |
| Product Version | Displays the operating system version. |
| Platform Version | Displays the platform version. |

Rebuilding RAID Drives

A RAID drive may fail and may require manual intervention to rebuild one of the physical drives in a logical pair during normal operation.

RAIDed disks, also termed RAID arrays, get arranged in logical pairs. A single logical pair comprises two physical drives. The system keeps the pair of drives in sync with the same data in real time to provide redundancy ultimately for data integrity and assurance. When one physical drive fails to synchronize or begins to experience read or write failures, you may need to rebuild the drive. Many things can cause the failure, but the main concern remains whether the data in a logical drive pair is compromised due to failures in one of the physical drives.

Monitoring software usually detects RAID failures, and failures get reported as a failed drive or a loss of drive redundancy. The procedure for rebuilding a failing drive follows and applies to all Cisco MCS model 7825, 7835, and 7845 servers.

First, check the status of the RAID array by using the CLI **show hardware** command and verify whether the Status field reads Ok or Okay. An example follows:

```
admin:show hardware
HW Platform       : 7835I
Processors        : 1
Type              : Intel(R) Xeon(TM) CPU 3.06GHz
CPU Speed         : 3066
Memory           : 2048 MBytes
Object ID         : 1.3.6.1.4.1.9.1.585
OS Version        : UCOS 2.0.1.0-37
RAID Details      :
Found 1 IBM ServeRAID controller(s).
Read configuration has been initiated for controller 1...
-----
Logical drive information
-----
Logical drive number 1
  Status of logical drive      : Okay (OKAY)
  RAID level                   : 1
  Size (in MB)                 : 70006
  Write cache status          : Temporary write through (TWT)
  Number of chunks             : 2
  Stripe-unit size             : 8 KB
  Access blocked               : No
  Part of array                : A
Array A stripe order (Channel/SCSI ID) : 1,0 1,1 Command completed successfully.
```

If the RAID array status field does not read Ok or Okay (for example, shows Degraded or Critical), perform the following steps:

-
- Step 1** Log in to console and enter the CLI command, **utils system shutdown**.
 - Step 2** Power off the server (press power off button).
 - Step 3** Extract the failed disk drive.
 - Step 4** Power up the server (press power on button).

If the server is an IBM server (for example, a 7825I, 7835I, or 7845I), the following menu will appear during system reboot:

```
1:ServeRAID-5i Slot 2, Logical drv=1, Firmware=7.12.07, Status=Fail
1 Drive(s) not responding or found at new location(s)
Press F2 Detailed information
      F4 Retry the command
      F5 Change the configuration and set the drive(s) defunct
      F10 Continue without changing the configuration
```

- Step 5** Press **F5**

- Step 6** After the login prompt appears in the console window, log in and check the status of the RAID array by using the CLI **show hardware** command; the Status field should read Degraded or Critical.
- Step 7** Insert the failed disk drive into the original slot; be sure to lock it properly in place.
- Step 8** Check the status of the RAID array by using the CLI **show hardware** command; the Status field will read Rebuilding or Critical.
- Step 9** After an hour, recheck the status of the RAID array by using the CLI **show hardware** command and verify that the Status field reads Ok or Okay.

If the status does not read Ok or Okay, you may need to replace the physical drive.



CHAPTER 4

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:

Procedure

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

The Ethernet Settings window displays.

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



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

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

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.

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 a Subsequent Cisco Unified Communications Manager Node

If the IP address of the first Cisco Unified Communications Manager node gets changed while a subsequent node is offline, you may not be able to log in to Cisco Unified Communications Manager Administration on the subsequent node. If this occurs, follow this 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, you must configure an SMTP host.

To access the SMTP settings, follow this procedure:

Procedure

- Step 1** From the Cisco Unified Communications Operating System Administration window, navigate to **Settings>SMTP**.
The SMTP Settings window displays.
- Step 2** Enter or modify the SMTP hostname or IP address.
- Step 3** Click **Save**.
-

Time Settings

To manually configure the time, follow this procedure:

**Note**

Before you can manually configure the server time, you must delete any NTP servers that you have configured. See [NTP Servers](#) for more information.

Procedure

- Step 1** From the Cisco Unified Communications Operating System Administration window, navigate to **Settings>Time**.
- Step 2** Enter the date and time for the system.
- Step 3** Click **Save**.
-



CHAPTER 5

System Restart

This section provides procedures for using the following restart options:

- [Switch Versions and Restart](#)
- [Restart Current Version](#)
- [Shut Down the System](#)

Switch Versions and Restart

You can use this option both when you are upgrading to a newer software version or when you need to fall back to an earlier software version. To shut down the system that is running on the active disk partition and then automatically restart the system using the software version on the inactive partition, follow this procedure:



Caution

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

Procedure

-
- Step 1** From the Cisco Unified Communications Operating System Administration window, navigate to **Settings > Version**.
- The Version Settings window displays, which shows the software version on both the active and inactive partitions.
- Step 2** To switch versions and restart, click **Switch Versions**. To stop the operation, click **Cancel**.
- If you click **Switch Version**, the system restarts, and the partition that is currently inactive becomes active.
-

Restart Current Version

To restart the system on the current partition without switching versions, follow this procedure:



Caution

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

Procedure

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

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

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

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

Shut Down the System

**Caution**

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

To shut down the system, follow this procedure:

**Caution**

This procedure causes the system to shut down.

Procedure

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

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

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

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

**Note**

The hardware does not power down automatically.



CHAPTER 6

Security

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

- [Set Internet Explorer Security Options](#)
- [Manage Certificates and Certificate Trust Lists](#)
- [IPSEC Management](#)

Set Internet Explorer Security Options

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

Procedure

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

Manage Certificates and Certificate Trust Lists

The functions that you can perform from the Certificate Management menu are described in the following topics:

- [“Display Certificates” section on page 6-2](#)
- [“Download a Certificate or CTL” section on page 6-2](#)
- [“Delete and Regenerate a Certificate” section on page 6-2](#)
- [“Upload a Certificate or Certificate Trust List” section on page 6-3](#)

- [“Using Third-Party CA Certificates” section on page 6-5](#)

**Note**

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

Display Certificates

To display existing certificates, follow this procedure:

Procedure

-
- Step 1** Navigate to **Security>Certificate Management**.
The Certificate List window displays.
 - Step 2** You can use the Find controls to filter the certificate list.
 - Step 3** To view details of a certificate or trust store, click its file name.
The Certificate Configuration window displays information about the certificate.
 - Step 4** To return to the Certificate List window, select **Back To Find/List** in the Related Links list; then, click **Go**.
-

Download a Certificate or CTL

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

Procedure

-
- Step 1** Navigate to **Security>Certificate Management**.
The Certificate List window displays.
 - Step 2** You can use the Find controls to filter the certificate list.
 - Step 3** Click the file name of the certificate or CTL.
The Certificate Configuration window displays.
 - Step 4** Click **Download**.
 - Step 5** In the File Download dialog box, click **Save**.
-

Delete and Regenerate a Certificate

These sections describe deleting and regenerating a certificate:

- [“Deleting a Certificate” section on page 6-3](#)

- [“Regenerating a Certificate” section on page 6-3](#)

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**.
The Certificate List window displays.
- Step 2** You can use the Find controls to filter the certificate list.
- Step 3** Click the file name of the certificate or CTL.
The Certificate Configuration window displays.
- Step 4** Click **Delete**.
-

Regenerating a Certificate

To regenerate a certificate, follow this procedure:



Caution

Regenerating a certificate can affect your system operations.

Procedure

- Step 1** Navigate to **Security>Certificate Management**.
The Certificate List window displays.
- Step 2** Click **Generate New**.
The Generate Certificate dialog box opens.
- Step 3** Choose a certificate name from the Certificate Name list.
- Step 4** Click **Generate New**.
-

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.

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

- “Upload a Certificate” section on page 6-4
- “Upload a Certificate Trust List” section on page 6-4
- “Upload a Directory Trust Certificate” section on page 6-5

Upload a Certificate

Procedure

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

Upload a Certificate Trust List

Procedure

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

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

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

Upload a Directory Trust Certificate

Procedure

-
- Step 1** Navigate to **Security>Certificate Management**.
The Certificate List window displays.
- Step 2** Click **Upload CTL**.
The Upload Certificate Trust List dialog box opens.
- Step 3** Select **directory-trust** from the **Certificate Name** list.
- Step 4** Enter the file to upload in the **Upload File** field.
- Step 5** To upload the file, click the **Upload File** button.
- Step 6** Log into Cisco Unified Serviceability.
- Step 7** Navigate to **Tools > Control Center - Feature Services**.
- Step 8** Restart the service **Cisco Dirsync**.
- Step 9** Log in to the Cisco Unified Communications Operating System CLI as an administrator.
- Step 10** To restart the Tomcat service, enter the command **utils service restart Cisco Tomcat**.
- Step 11** After the services have been restarted, you can add the directory agreement for SSL.
-

Using Third-Party CA Certificates

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

| | Task | For More Information |
|---------------|---|--|
| Step 1 | Generate a CSR on the server. | See the “Generating a Certificate Signing Request” section on page 6-6. |
| Step 2 | Download the CSR to your PC. | See the “Download a Certificate Signing Request” section on page 6-6. |
| Step 3 | Use the CSR to obtain an application certificate from a CA. | Get information about obtaining application certificates from your CA. See “Obtaining Third-Party CA Certificates” section on page 6-7 for additional notes. |
| Step 4 | Obtain the CA root certificate. | Get information about obtaining a root certificate from your CA. See “Obtaining Third-Party CA Certificates” section on page 6-7 for additional notes. |

| | Task | For More Information |
|---------------|---|---|
| Step 5 | Upload the CA root certificate to the server. | See the “Upload a Certificate” section on page 6-4. |
| Step 6 | Upload the application certificate to the server. | See the “Upload a Certificate” section on page 6-4. |
| Step 7 | If you updated the certificate for CAPF or Cisco Unified Communications Manager, generate a new CTL file. | See the <i>Cisco Unified Communications Manager Security Guide</i> . |
| Step 8 | Restart the services that are affected by the new certificate. | For all certificate types, restart the corresponding service (for example, restart the Tomcat service if you updated the Tomcat certificate). In addition, if you updated the certificate for CAPF or Cisco Unified Communications Manager, restart the TFTP service. See the <i>Cisco Unified Communications Manager Serviceability Administration Guide</i> for information about restarting services. |

Generating a Certificate Signing Request

To generate a Certificate Signing Request (CSR), follow these steps:

Procedure

-
- Step 1** Navigate to **Security>Certificate Management**.
The Certificate List window displays.
 - Step 2** Click **Generate CSR**.
The Generate Certificate Signing Request dialog box opens.
 - Step 3** Select the certificate name from the **Certificate Name** list.
 - Step 4** Click **Generate CSR**.
-

Download a Certificate Signing Request

To download a Certificate Signing Request, follow this procedure:

Procedure

-
- Step 1** Navigate to **Security>Certificate Management**.
The Certificate List window displays.
 - Step 2** Click **Download CSR**.
The Download Certificate Signing Request dialog box opens.
 - Step 3** Select the certificate name from the **Certificate Name** list.
 - Step 4** Click **Download CSR**.

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

Obtaining Third-Party CA Certificates

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

CAPF and Cisco Unified Communications Manager CSRs include extensions that you must include in your request for an application certificate from the CA. If your CA does not support the ExtensionRequest mechanism, you must enable the X.509 extensions that are listed on the final page of the CSR generation process.

Cisco Unified Communications Operating System generates certificates in DER and PEM encoding formats and generates CSRs in PEM encoding format. It accepts certificates in DER and 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 Monitor**.
- The Certificate Monitor window displays.
- Step 2** Enter the required configuration information. See [Table 6-1](#) for a description of the Certificate Monitor Expiration fields.
- Step 3** To save your changes, click **Save**.
-

Table 6-1 Certificate Monitor Field Descriptions

| Field | Description |
|-------------------------|---|
| Notification Start Time | Enter the number of days before the certificate expires that you want to be notified. |
| Notification Frequency | Enter the frequency for notification, either in hours or days. |

Table 6-1 Certificate Monitor Field Descriptions (continued)

| Field | Description |
|----------------------------|--|
| Enable E-mail Notification | Select the check box to enable e-mail notification. |
| Email IDs | Enter the e-mail address to which you want notifications sent. Note For the system to send notifications, you must configure an SMTP host. |

IPSEC Management

The functions that you can perform with the IPsec menu are described in the following topics:

- “Set Up a New IPsec Policy” section on page 6-8
- “Managing Existing IPsec Policies” section on page 6-10

**Note**

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

Set Up a New IPsec Policy

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

**Note**

Because any changes that you make to an IPsec policy during a system upgrade will get lost, do not modify or create IPsec policies during an upgrade.

**Caution**

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

Procedure

- Step 1** Navigate to **Security > IPSEC Configuration**.
The IPSEC Policy List window displays.
- Step 2** Click **Add New**.
The IPSEC Policy Configuration window displays.
- Step 3** Enter the appropriate information on the IPSEC Policy Configuration window. For a description of the fields on this window, see [Table 6-2](#).
- Step 4** To set up the new IPsec policy, click **Save**.

Table 6-2 *IPSEC Policy and Association Field Descriptions*

| Field | Description |
|-----------------------|--|
| Policy Name | Specifies the name of the IPsec policy. The name can contain only letters, digits, and hyphens. |
| Association Name | Specifies the association name that is given to each IPsec association. The name can contain only letters, digits, and hyphens. |
| Authentication Method | Specifies the authentication method. |
| Preshared Key | Specifies the preshared key if you selected Pre-shared Key in the Authentication Name field. |
| Peer Type | Specifies whether the peer is the same type or different. |
| Destination Address | Specifies the IP address or FQDN of the destination. |
| Destination Port | Specifies the port number at the destination. |
| Source Address | Specifies the IP address or FQDN of the source. |
| Source Port | Specifies the port number at the source. |
| Mode | Specifies Tunnel or Transport mode. |
| Remote Port | Specifies the port number to use at the destination. |
| Protocol | Specifies the specific protocol, or Any: <ul style="list-style-type: none"> • TCP • UDP • Any |
| Encryption Algorithm | From the drop-down list, choose the encryption algorithm. Choices include <ul style="list-style-type: none"> • DES • 3DES |
| Hash Algorithm | Specifies the hash algorithm <ul style="list-style-type: none"> • SHA1—Hash algorithm that is used in phase 1 IKE negotiation • MD5—Hash algorithm that is used in phase 1 IKE negotiation |
| ESP Algorithm | From the drop-down list, choose the ESP algorithm. Choices include <ul style="list-style-type: none"> • NULL_ENC • DES • 3DES • BLOWFISH • RIJNDAEL |
| Phase One Life Time | Specifies the lifetime for phase One, IKE negotiation, in seconds. |

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

| Field | Description |
|---------------------|---|
| Phase One DH | From the drop-down list, choose the phase One DH value. Choices include: 2, 1, 5, 14, 16, 17, and 18. |
| Phase Two Life Time | Specifies the lifetime for phase Two, IKE negotiation, in seconds. |
| Phase Two DH | From the drop-down list, choose the phase Two DH value. Choices include: 2, 1, 5, 14, 16, 17, and 18. |
| Enable Policy | Check the check box to enable the policy. |

Managing Existing IPsec Policies

To display, enable or disable, or delete an existing IPsec policy, follow this procedure:



Note

Because any changes that you make to an IPsec policy during a system upgrade will get lost, do not modify or create IPsec policies during an upgrade.



Caution

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



Caution

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

Procedure

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



Note

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

The IPSEC Policy List window displays.

Step 2 To display, enable, or disable a policy, follow these steps:

- a. Click the policy name.
The IPSEC Policy Configuration window displays.
- b. To enable or disable the policy, use the **Enable Policy** check box.
- c. Click **Save**.

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

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

- b. Click **Delete Selected**.
-



CHAPTER 7

Software Upgrades

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

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

Software Upgrade and Installation

With this version of Cisco Unified Communications Manager, you can install upgrade software on your server while the system continues to operate. Two partitions exist on your system: an active, bootable partition and an inactive, bootable partition. The system boots up and operates entirely on the partition that is marked as the active partition.

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

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



Note

You can only make changes to the database on the active partition. The database on the inactive partition does not get updated. If you make changes to the database after an upgrade, you must repeat those changes after switching the partition.

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

You must install the upgrade patch on the first node before installing it on subscriber nodes. You can install the upgrade patch on multiple subscriber servers at the same time. When you are ready to activate the new version, you must activate the new software on the first node before activating it on all other nodes.

**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*.

Upgrading to Cisco Unified Communications Manager Release 6.0(1)

Starting with Cisco Unified Communications Manager version 6.0(1), CAPF uses the Certificate Manager Infrastructure to manage its certificates and keys. Because of this, when you upgrade to version 6.0(1) or higher, CAPF keys and certificates automatically get regenerated. You must then rerun the CTL Client application to upgrade the CTL file. For information on using CAPF with Cisco Unified Communications Manager, refer to the *Cisco Unified Communications Manager Security Guide*.

Obtain licenses for Cisco Unified Communications Manager 6.0(1) before upgrading to this release. You must import your new licenses after upgrading to enable the system. Refer to *Cisco Unified Communications Manager Administration Guide* for information about licensing and obtaining licenses.

Obtaining the Upgrade File

Before you begin the upgrade process, you must obtain the appropriate upgrade file from Cisco.com.

If you are upgrading from Cisco Unified Communications Manager release 5.x, the upgrade file name has the following format:

```
cisco-ipt-k9-patchX.X.X.X-X.tar.gz.sgn
```

Where X.X.X.X-X represents the release and build number.

**Note**

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

**Note**

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

If you are upgrading from Cisco Unified Communications Manager release 6.x, the upgrade file has the extension `sgn.iso`.

You can access the upgrade file during the installation process from either a local disk (CD or DVD) or from a remote FTP or TFTP server.

Upgrading 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.

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

Procedure

Step 1 Create an upgrade disk by using the upgrade file that you downloaded from Cisco.com.

- If you are using an upgrade file with the tar.gz.sgn extension, copy the upgrade file to a writeable DVD.
- If you are using an upgrade file with the sgn.iso extension, you must create an ISO image on a writable DVD from the upgrade file. Just copying the .iso file to the DVD will not work.

- Step 2** Insert the new DVD into the disc drive on the local server that is to be upgraded.
- Step 3** Log into Cisco Unified Communications Operating System Administration.
- Step 4** Navigate to **Software Upgrades > Install/Upgrade**.
The Software Installation/Upgrade window displays.
- Step 5** Choose **DVD/CD** from the **Source** list.
- Step 6** Enter the path to the patch file on the CD or DVD in the Directory field.
If the file is in the root directory, or if you created an ISO image DVD, enter a slash (/) in the Directory field.
- Step 7** To continue the upgrade process, click **Next**.
- Step 8** Choose the upgrade version that you want to install and click **Next**.
- Step 9** In the next window, monitor the progress of the download.
When the download completes, the next window displays a checksum value if you are using an upgrade file with the tar.gz.sg extension. No checksum is displayed if you burned an ISO image DVD.
- Step 10** 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 11** Click **Next**.
- Step 12** If you want to install the upgrade and automatically reboot to the upgraded partition, choose **Reboot to upgraded partition**. The system restarts running the upgraded software.
- Step 13** If you want to install the upgrade and then manually reboot to the upgraded partition at a later time, do the following steps:
- a. Choose **Do not reboot after upgrade**.
 - b. Click **Next**.
The Upgrade Status window displays the Upgrade log.
 - c. When the installation completes, click **Finish**.
 - d. To restart the system and activate the upgrade, choose **Settings > Version**; then, click **Switch Version**.

The system restarts running the upgraded software.

Upgrading from Remote Source

To upgrade the software from a network location or remote server, use the following procedure.

Procedure

-
- Step 1** Put the upgrade file on an FTP or SFTP server that the server you are upgrading can access.
- Step 2** Log into Cisco Unified Communications Operating System Administration.
- Step 3** Navigate to **Software Upgrades > Install/Upgrade**.
The Software Installation/Upgrade window displays.
- Step 4** Choose **Remote Filesystem** from the **Source** list.
- Step 5** Enter the path to the directory that contains the patch file on the remote system in the **Directory** field.
If the upgrade file is located on a Linux or Unix server, you must enter a forward slash at the beginning of the directory path. For example, if the upgrade file is in the patches directory, you must enter **/patches**. If the upgrade file is located on a Windows server, check with your system administrator for the correct directory path.
- If you are upgrading from Cisco Unified Communications Manager release 5.x, the upgrade file has the extension tar.gz.sgn.
 - If you are upgrading from Cisco Unified Communications Manager release 6.x, the upgrade file has the extension sgn.iso.
- Step 6** In the **Server** field, enter the server name or IP address.
- Step 7** In the **User Name** field, enter your user name on the remote server.
- Step 8** In the **User Password** field, enter your password on the remote server.
- Step 9** Select the transfer protocol from the **Transfer Protocol** field.
- Step 10** To continue the upgrade process, click **Next**.
- Step 11** Choose the upgrade version that you want to install and click **Next**.
- Step 12** In the next window, monitor the progress of the download.
When the download completes, the next window displays a checksum value if you are using an upgrade file with the tar.gz.sg extension. No checksum is displayed if you burned an ISO image DVD.
- Step 13** When the download completes, verify the checksum value against the checksum (if available) for the file you that 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 14** Click **Next**.
- Step 15** If you want to install the upgrade and automatically reboot to the upgraded partition, choose **Reboot to upgraded partition**. The system restarts running the upgraded software.
- Step 16** If you want to install the upgrade and then manually reboot to the upgraded partition at a later time, do the following steps:
- a. Choose **Do not reboot after upgrade**.
 - b. Click **Next**.
The Upgrade Status window displays the Upgrade log.
 - c. When the installation completes, click **Finish**.

- d. To restart the system and activate the upgrade, choose **Settings > Version**; then, click **Switch Version**.

The system restarts running the upgraded software.

Stalled Upgrades

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

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

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

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

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

Reverting to a Previous Version

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

Procedure

- Step 1** Open Cisco Unified Communications Operating System Administration directly by entering the following URL:
`https://server-name/cmplatform`
where *server-name* is the host name or IP address of the Cisco Unified Communications Manager server.
 - Step 2** Enter your Administrator username and password.
 - Step 3** Choose **Settings>Version**.
The Version Settings window displays.
 - Step 4** Click the **Switch Versions** button.
When you verify that you want to restart the system, the system restarts running the upgraded software. This restart might take several minutes.
-

Dial Plan Installation

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

After the dial plan files are installed on the system, log in to Cisco Unified Communications Manager Administration and then navigate to **Call Routing>Dial Plan Installer** to complete installing the dial plans.

Locale Installation

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

User Locales

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

Network Locales

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

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

**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.

**Caution**

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 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 messages that can occur during Locale Installer activation. If an error occurs, you can view the 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] Communications Manager CSV file installer installdb is not present or not executable | A Cisco Unified Communications Manager application called installdb must be present; it reads information that is contained in a CSV file and applies it correctly to the Cisco Unified Communications Manager database. If this application is not found, it either was not installed with Cisco Unified Communications Manager (very unlikely), has been deleted (more likely), or the server does not have Cisco Unified Communications Manager installed (most likely). Installation of the locale will terminate because locales will not work without the correct records that are held in the database. |

Table 7-1 *Locale Installer Error Messages and Descriptions (continued)*

| Message | Description |
|--|--|
| [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maDialogs_<ll>_<CC>.properties.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.cm.util.Zipper. Even if these errors occur, the locale will continue to work correctly, with the exception of Cisco Unified Communications Manager Assistant, which cannot detect a change in localized Cisco Unified Communications Manager Assistant files. |
| [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. | |
| [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 Communications Manager 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. |

Supported Cisco Unified Communications Products

For a list of products that Cisco Unified Communications Manager Locale Installers support, see the *Cisco IP Telephony Locale Installer for Cisco Unified Communications Manager*, which is available at this URL:

<http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-locale-51>

Managing TFTP Server Files

You can upload files for use by the phones to the TFTP server on 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 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 and delete TFTP server files, follow this procedure:

Procedure

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

The TFTP File Management window displays and shows a listing of the current uploaded files. You can filter the file list by using the Find controls.

- Step 2** To upload a file, follow this procedure:

- a. Click **Upload File**.

The Upload File dialog box opens.

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

- c. To upload the file to a subdirectory of the `tftp` directory, enter the subdirectory in the **Directory** field.

- d. To start the upload, click **Upload File**.

The Status area indicates when the file uploads successfully.

- e. After the file uploads, restart the Cisco TFTP service.



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

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

- Step 3** To delete files, follow this procedure:

- a. Check the check boxes next to the files that you want to delete.

You can also click **Select All** to select all of the files, or **Clear All** to clear all selection.

- b. Click **Delete Selected**.
-



Note If you want to modify a file that is already in the `tftp` directory, you can use the CLI command **file list tftp** to see the files in the TFTP directory and **file get tftp** to get a copy of a file in the TFTP directory. For more information, see [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 completes.

Step 6 Choose whether you want to validate IPSec.

Step 7 Click **Ping**.

The Ping Remote window displays the ping statistics.

Remote Support

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

The remote support process works like this:

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

To set up remote support, follow this procedure:

Procedure

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

The Remote Access Configuration window displays.

- Step 2** Enter an account name for the remote account and the account life in days.



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

- Step 3** Click **Save**.

The Remote Support Status window displays. For descriptions of fields on the Remote Support Status window, see [Table 8-1](#).

- Step 4** To access the system by using the generated pass phrase, contact your Cisco personnel.

- Step 5** To delete the remote access support account, click the **Delete** button.

Table 8-1 Remote Support Status Fields and Descriptions

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



APPENDIX **A**

Command Line Interface

Overview

This appendix describes the CLI commands that are available on the Cisco Unified Communications Operating System server.

Starting a CLI Session

You can access the Cisco Unified Communications Operating System CLI remotely or locally:

- From a web client workstation, such as the workstation that you use for Cisco Unified Communications Operating System Administration, you can use SSH to connect securely to the Cisco Unified Communications Operating System.
- You can access the Cisco Unified Communications Operating System 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 your administrator ID.

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

Step 2 Enter your password.

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

```
admin:
```

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 sections list and describe the CLI commands that are available for the Cisco Unified Communications Operating System.

delete account

This command allows you to delete an administrator account.

Command Syntax

delete account *account-name*

Parameters

- *account-name* represents the name of an administrator account.

Requirements

Command privilege level: 4

Allowed during upgrade: No

delete dns

This command allows you to delete the IP address for a DNS server.

Command Syntax

delete dns *ip-address*

Parameters

- *ip-address* represents the IP address of the DNS server you want to delete.

Usage Guidelines

The system asks whether you want to continue to execute this command.

**Caution**

If you continue, this command causes a temporary loss of network connectivity.

Requirements

Command privilege level: 1

Allowed during upgrade: No

delete ipsec

This command allows you to delete IPsec policies and associations.

Command Syntax

delete ipsec

policy {**ALL** | *policy-name*}

association *policy name* {**ALL** | *association-name*}

Parameters

- *policy-name* represents an IPsec policy.
- *association-name* represents an IPsec association.

Requirements

Command privilege level: 1

Allowed during upgrade: No

delete process

This command allows you to delete a particular process.

Command Syntax

delete process *process-id* [**force** | **terminate** | **crash**]

Parameters

- *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

Usage Guidelines



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.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

delete smtp

This command allows you to delete the SMTP host.

Command Syntax

delete smtp

Requirements

Command privilege level: 1

Allowed during upgrade: No

file check

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.

Command Syntax

file check [*detection-size-kb*]

Options

detection-size-kb specifies the minimum file size change that is required for the command to display the file as changed.

Usage Guidelines

The command notifies you about a possible impact to system performance and asks you whether you want to continue.



Caution

Because running this command can affect system performance, Cisco recommends that you run the command during off-peak hours.

The display includes both deleted and new files.

Defaults

The default value of *detection-size-kb* is 100 KB.

Requirements

Command privilege level: 0

Allowed during upgrade: No

file delete

This command deletes one or more files.

Command Syntax

file delete

activelog *directory/filename* [**detail**] [**noconfirm**]

inactivelog *directory/filename* [**detail**] [**noconfirm**]

install *directory/filename* [**detail**] [**noconfirm**]

tftp *directory/filename* [**detail**]

Parameters

- **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.
- *directory/filename* specifies the path and filename of the file(s) to delete. You can use the wildcard character, *, for *filename*.

Options

- **detail**—Displays a listing of deleted files with the date and time.
- **noconfirm**—Deletes files without asking you to confirm each deletion.

Usage Guidelines

**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.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Example

The following example deletes the install log.

```
file delete install install.log
```

file dump

This command dumps the contents of a file to the screen, a page at a time.

Command Syntax

file dump

activelog *directory/filename* [**detail**] [**hex**]

inactivelog *directory/filename* [**detail**] [**hex**]

install *directory/filename* [**detail**] [**hex**]

tftp *directory/filename* [**detail**] [**hex**]

Parameters

- **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.
- *directory/filename* specifies the path and filename of the file to dump. 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

Requirements

Command privilege level: 1 for logs, 0 for TFTP files

Allowed during upgrade: Yes

Example

This command dumps contents of file `_cdrIndex.idx`.

```
file dump activelog cm/cdr/_cdrIndex.idx
```

file get

This command sends the file to another system by using SFTP.

Command Syntax**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]
```

Parameters

- **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.
- *directory/filename* specifies the path to the file(s) to delete. You can use the wildcard character, *, for *filename* as long as it resolves to one 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

Usage Guidelines

After the command identifies the specified files, you get prompted to enter an SFTP host, username, and password.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Examples

This command gets all files in the activelog operating system directory that match the string “plat”.

```
file get activelog platform match plat
```

This command gets all operating system log files for a particular time period.

```
file get activelog platform/log abstime 18:00:9/27/2005 18:00:9/28/2005
```

file list

This command lists the log files in an available log directory.

Command Syntax

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]
```

Parameters

- **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.
- *directory* specifies the path to the directory to list. You can use a wildcard character, *, for *directory* 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

Requirements

Command privilege level: 1 for logs, 0 for TFTP files

Allowed during upgrade: Yes

Examples

This example lists operating system log files with details.

```
file list activelog platform/log page detail
```

This example lists directories in CDR repository.

```
file list activelog cm/cdr_repository
```

This example lists CDR files in a specified directory by size.

```
file list activelog cm/cdr_repository/processed/20050812 size
```

file search

This command searches the content of a log and displays the matching lines a page at a time.

Command Syntax

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*]

Parameters

- **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.
- *directory/filename* represents the path to the file(s) to search. 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.

Usage Guidelines

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.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
file search activelog platform/log/platform.log Err[a-z] ignorecase
```

file tail

This command tails (prints the last few lines) of a log file.

Command Syntax**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]
```

Parameters

- **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.
- *directory/filename* specifies the path to the file to tail. 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

Requirements

Command privilege level: 1 for logs, 0 for TFTP files

Allowed during upgrade: Yes

Example

This example tails the operating system CLI log file.

```
file tail activelog platform/log/cli00001.log
```

file view

This command displays the contents of a file.

Command Syntax**file view**

```
activelog directory/filename
```

inactivelog *directory/filename*

install *directory/filename*

tftp *directory/filename*

Parameters

- **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.
- *directory/filename* specifies the path to the file to view. You can use the wildcard character, *, for *filename* as long as it resolves to one file.

Usage Guidelines



Caution

Do not use this command to view binary files because this can corrupt the terminal session.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Examples

This example displays the install log.

```
file view install install.log
```

This example displays a particular CDR file.

```
file view activelog /cm/cdr_repository/processed/20058012/{filename}
```

run sql

This command allows you to run an SQL command.

Command Syntax

run sql *sql_statement*

Parameters

- *sql_statement* represents the SQL command to run.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Example

This example runs an SQL command.

```
run sql select name from device
```

set account

This command sets up a new account on the operating system.

Command Syntax

```
set account name
```

Parameters

- *name* represents the username for the new account.

Usage Guidelines

After you enter the username, the system prompts you to enter the privilege level and password for the new account.

Requirements

Command privilege level: 0

Allowed during upgrade: No

set commandcount

This command changes the CLI command prompt, so it displays how many CLI commands have executed.

Command Syntax

```
set commandcount {enable | disable}
```

Parameters

- *unit-name* represents the name of the certificate that you want to regenerate.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set ipsec

This command allows you to set IPSec policies and associations.

Command Syntax

```
set ipsec
```

```
policy {ALL | policy-name}
```

```
association policy-name {ALL | association-name}
```

Parameters

- *policy-name* represents an IPsec policy.
- *association-name* represents an IPsec association.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set logging

This command allows you to enable or disable logging.

Command Syntax

```
set logging {enable | disable}
```

Requirements

Command privilege level: 0

Allowed during upgrade: No

set network dhcp

This command enables or disables DHCP for Ethernet interface 0. You cannot configure Ethernet interface 1.

Command Syntax

```
set network dhcp eth0 {enable | disable}
```

Parameters

- **eth0** specifies Ethernet interface 0.

Usage Guidelines

The system asks whether you want to continue to execute this command.

**Caution**

If you continue, this command causes the system to restart. Cisco also recommends that you restart all nodes whenever any IP address gets changed.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set network dns

This command sets the IP address for the primary or secondary DNS server.

Command Syntax

set network dns {primary | secondary} *ip-address*

Parameters

- *ip-address* represents the IP address of the primary or secondary DNS server.

Usage Guidelines

The system asks whether you want to continue to execute this command.

**Caution**

If you continue, this command causes a temporary loss of network connectivity.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set network dns options

This command sets DNS options.

Command Syntax

set network dns options [timeout *seconds*] [attempts *number*] [rotate]

Parameters

- **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.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

set network domain

This command sets the domain name for the system.

Command Syntax

set network domain *domain-name*

Parameters

- *domain-name* represents the system domain that you want to assign.

Usage Guidelines

The system asks whether you want to continue to execute this command.

**Caution**

If you continue, this command causes a temporary loss of network connectivity.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set network failover

This command enables and disables Network Fault Tolerance on the Media Convergence Server network interface card.

Command Syntax

failover {enable | disable}

Parameters

- **enable** enables Network Fault Tolerance.
- **disable** disables Network Fault Tolerance.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set network gateway

This command enables you to configure the IP address of the network gateway.

Command Syntax

set network gateway *ip-address*

Parameters

- *ip-address* represents the IP address of the network gateway that you want to assign.

Usage Guidelines

The system asks whether you want to continue to execute this command.

**Caution**

If you continue, this command causes the system to restart.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set network ip

This command sets the IP address for Ethernet interface 0. You cannot configure Ethernet interface 1.

Command Syntax

```
set network ip eth0 ip-address ip-mask
```

Parameters

- **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.

Usage Guidelines

The system asks whether you want to continue to execute this command.

**Caution**

If you continue, this command causes the system to restart.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set network mtu

This command sets the maximum MTU value.

Command Syntax

```
set network mtu mtu_max
```

Parameters

- *mtu_max* specifies the maximum MTU value.

Usage Guidelines

The system asks whether you want to continue to execute this command.

**Caution**

If you continue, the system will temporarily lose network connectivity.

set network max_ip_contrack

This command sets the ip_contrack_max value.

Command Syntax

```
set network max_ip_contrack ip_contrack_max
```

Parameters

- *ip_contrack_max* specifies the value for *ip_contrack_max*.

set network nic

This command sets the properties of the Ethernet Interface 0. You cannot configure Ethernet interface 1.

Command Syntax

```
set network nic eth0 [auto en | dis] [speed 10 | 100] [duplex half | full]
```

Parameters

- **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.

Usage Guidelines

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.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set network pmtud

This command enables and disables Path MTU Discovery.

Command Syntax

```
set network pmtud [enable | disable]
```

Parameters

- **enable** enables Path MTU Discovery.
- **disable** disables Path MTU Discovery.

Usage Guidelines

The system asks whether you want to continue to execute this command.

**Caution**

If you continue, the system will temporarily lose network connectivity.

set network status

This command sets the status of Ethernet 0 to up or down. You cannot configure Ethernet interface 1.

Command Syntax

```
set network status eth0 { up | down }
```

Parameters

- **eth0** specifies Ethernet interface 0.

Usage Guidelines

The system asks whether you want to continue to execute this command.



Caution

If you continue, the system will temporarily lose network connectivity.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set password

This command allows you to change the administrator and security passwords.

Command Syntax

```
set password { admin | security }
```

Parameters

- **eth0** specifies Ethernet interface 0.

Usage Guidelines

The systems prompts you for the old and new passwords.



Caution

The password must contain at least six characters, and the system checks it for strength.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set smtp

This command sets the SMTP server hostname.

Command Syntax

```
set smtp hostname
```

Parameters

- *hostname* represents the SMTP server name.

Requirements

Command privilege level: 0

Allowed during upgrade: No

set timezone

This command lets you change the system time zone.

Command Syntax

set timezone *timezone*

Parameters

- *timezone* specifies the new timezone.

Usage Guidelines

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.

Requirements

Command privilege level: 0

Allowed during upgrade: No

Example

This example sets the time zone to Pacific time.

```
set timezone Pac
```

set trace

This command sets trace activity for the specified task.

Command Syntax

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*

Parameters

- *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.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set web-security

This command sets the web security certificate information for the operating system.

Command Syntax

set web-security *orgunit orgname locality state country*

Parameters

- *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.

Requirements

Command privilege level: 0

Allowed during upgrade: No

set workingdir

This command sets the working directory for active, inactive, and installation logs.

Command Syntax

set workingdir

activelog *directory*
inactivelog *directory*
install *directory*
tftp *directory*

Parameters

- **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.

Requirements

Command privilege level: 0 for logs, 1 for TFTP

Allowed during upgrade: Yes

show account

This command lists current administrator accounts, except the master administrator account.

Command Syntax

show account

Requirements

Command privilege level: 4

Allowed during upgrade: Yes

show cert

This command displays certificate contents and certificate trust lists.

Command Syntax

show cert

own *filename*
trust *filename*
list {**own** | **trust**}

Parameters

- *filename* represents the name of the certificate file.
- **own** specifies owned certificates.
- **trust** specifies trusted certificates.
- **list** specifies a certificate trust list.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Example

This command displays own certificate trust lists.

```
show cert list own
```

show environment

This command displays information about the server hardware.

Command Syntax

show environment

fans

power-supply

temperatures

Options

- **fans**—Displays information gathered by fan probes
- **power-supply**—Displays information gathered by power supply probes
- **temperatures**—Displays information gathered by temperature probes

show firewall list

This command displays system aspects of the server.

Command Syntax

show firewall list [**detail**] [**page**] [**file filename**]

Options

- **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.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show hardware

This command displays the following information on the platform hardware.

Command Syntax

show hardware

Usage Guidelines

This command displays the following information on the platform hardware:

- Platform
- Serial number
- BIOS build level
- BIOS manufacturer
- Active processors
- RAID controller status

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show ipsec

This command displays information on IPsec policies and associations.

Command Syntax

show ipsec

policy

association *policy*

information *policy association*

status

Parameters

- **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.

Requirements

Command privilege level: 1

Allowed during upgrade: yes

Example

This example displays IPsec policies.

```
show ipsec policy
```

show logins

This command lists recent logins to the server.

Command Syntax

```
show logins number
```

Parameters

number specifies the number of most recent logins to display. The default is 20.

show memory

This command displays information about the server memory.

Command Syntax

```
show memory  
    count  
    module [ALL | module_number]  
    size
```

Options

- **count**—Displays the number of memory modules on the system
- **module**—Displays detailed information about each memory module
- **size**—Displays the total amount of memory

Parameters

ALL displays information about all installed memory modules.

module_number specifies which memory module to display.

show myself

This command displays information about the current account.

Command Syntax

```
show myself
```

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show network

This command displays network information.

Command Syntax

show network

eth0 [detail]

failover [detail] [page]

route [detail]

status [detail] [listen] [process] [all] [nodns] [search stext]

ip_conntrack

max_ip_conntrack

dhcp eth0 status

all [detail]

Parameters

- **eth0** specifies Ethernet 0.
- **failover** specifies Network Fault Tolerance information.
- **route** specifies network routing information.
- **status** specifies active Internet connections.
- **ip_conntrack** specifies ip_conntrack usage information.
- **max_ip_conntrack** specifies max_ip_conntrack information.
- **dhcp eth0 status** displays DHCP status 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

Usage Guidelines

The **eth0** parameter displays Ethernet port 0 settings, including DHCP and DNS configurations and options.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Example

This example displays active Internet connections.

```
show network status
```

show open

This command displays open files and ports on the system.

Syntax Description**show open**

files [**all**] [**process** *processID*] [**regexp** *reg_exp*]

ports [**all**] [**regexp** *reg_exp*]

Parameters

- **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

show packages

This command displays the name and version for installed packages.

Command Syntax**show packages**

active *name* [**page**]

inactive *name* [**page**]

Parameters

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

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show perf counterhelp

This command displays the explanation text for the specified perfmon counter.

Command Syntax

show perf counterhelp *class-name counter-name*

Parameters

- *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.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show perf list categories

This command lists all categories in the perfmon system.

Command Syntax

show perf list categories

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show perf list classes

This command lists the perfmon classes or objects.

Command Syntax

show perf list classes [**cat** *category*] [**detail**]

Options

- **detail**—Displays detailed information
- **cat** *category*—Displays perfmon classes for the specified category

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show perf list counter

This command lists perfmon counters for the specified perfmon class.

Command Syntax

list counters *class-name* [**detail**]

Parameters

class-name represents a perfmon class name for which you want to list the counters.



Note If the class name or counter name contains white spaces, enclose the name in double quotation marks.

Options

detail—Displays detailed information

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show perf list instances

The command lists the perfmon instances for the specified perfmon class.

Command Syntax

list instances *class-name* [**detail**]

Parameters

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

detail—Displays detailed information

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show perf query class

This command queries a perfmon class and displays all the instances and counter values of each instance.

Command Syntax

```
show perf query class class-name [,class-name...]
```

Parameters

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.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show perf query counter

This command queries the specified counter and displays the counter value of all instances.

Command Syntax

```
show perf query counter class-name counter-name [,counter-name...]
```

Parameters

- *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.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show perf query instance

This command queries the specified instance and displays all its counter values.

Command Syntax

```
show perf query instance class-name instance-name [,instance-name...]
```

Parameters

- *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.

Usage Guidelines

This command does not apply to singleton perfmon classes.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show perf query path

This command queries a specified perfmon path.

Command Syntax

show perf query path *path-spec* [*,path-spec...*]

Parameters

- 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.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
show perf query path "Cisco Phones(phone-0)\CallsAttempted",  
"Cisco Unified Communications Manager\T1ChannelsActive"
```

show process

This command displays process and load information.

Command Syntax

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]
```

Parameters

- **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

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Example

This example shows detailed process listing one page at a time.

```
show process list detail page
```

show registry

This command displays the contents of the registry.

Command Syntax

```
show registry system component [name] [page]
```

Parameters

- *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, *.

Options

page—Displays one page at a time

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Example

This example shows contents of the cm system, dbl/sdi component.

```
show registry cm dbl/sdi
```

show risdb

This command displays RIS database table information.

Command Syntax

show risdb

list [**file** *filename*]

query *table1 table2 table3 ...* [**file** *filename*]

Parameters

- **list** displays the tables that are 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.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Example

This example displays a list of RIS database tables.

```
show risdb list
```

show smtp

This command displays the name of the SMTP host.

Command Syntax

show snmp

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show stats io

This command displays system IO statistics.

Command Syntax

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.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show status

This command displays basic platform status.

Command Syntax

show status

Usage Guidelines

This command displays the following basic platform status:

- Host name
- Date
- Time zone

- Locale
- Product version
- Platform version
- CPU usage
- Memory and disk usage

Requirements

Command privilege level: 0

show tech all

This command displays the combined output of all **show tech** commands.

Command Syntax

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.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show tech ccm_service

This command displays information on all Cisco Unified Communications Manager services that can run on the system.

Command Syntax

show tech ccm_service

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show tech database

This command creates a CSV file of the entire database.

Command Syntax**show tech database****Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

show tech dbintegrity

This command displays the database integrity.

Command Syntax**show tech dbintegrity**

show tech dbinuse

This command displays the database in use.

Command Syntax**show tech dbinuse****Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

show tech dbschema

This command displays the database schema in a CSV file.

Command Syntax**show tech dbschema****Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

show tech dbstateinfo

This command displays the state of the database.

Command Syntax**show tech dbstateinfo**

show tech devdefaults

This command displays the device defaults table.

Command Syntax

```
show tech devdefaults
```

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show tech gateway

This command displays the gateway table from the database.

Command Syntax

```
show tech gateway
```

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show tech locales

This command displays the locale information for devices, device pools, and end users.

Command Syntax

```
show tech locales
```

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show tech network

This command displays network aspects of the server.

Command Syntax

```
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.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show tech notify

This command displays the database change notify monitor.

Command Syntax

show tech notify

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show tech params all

This command displays all the database parameters.

Command Syntax

show tech params all

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show tech params enterprise

This command displays the database enterprise parameters.

Command Syntax

show tech params enterprise

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show tech params service

This command displays the database service parameters.

Command Syntax

```
show tech params service
```

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show tech prefs

This command displays database settings.

Command Syntax

```
show tech prefs
```

show tech procedures

This command displays the procedures that are in use for the database.

Command Syntax

```
show tech procedures
```

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show tech routepatterns

This command displays the route patterns that are configured for the system.

Command Syntax

```
show tech routepatterns
```

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show tech routeplan

This command displays the route plan that are configured for the system.

Command Syntax**show tech routeplan****Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

show tech runtime

This command displays runtime aspects of the server.

Command Syntax**show tech params 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.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show tech systables

This command displays the name of all tables in the sysmaster database.

Command Syntax**show tech systables****Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

show tech system

This command displays system aspects of the server.

Command Syntax**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.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show tech table

This command displays the contents of the specified database table.

Command Syntax

```
show tech table table_name [page] [csv]
```

Parameters

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

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show tech triggers

This command displays table names and the triggers that are associated with those tables.

Command Syntax

```
show tech triggers
```

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show tech version

This command displays the version of the installed components.

Command Syntax

show tech version [page]

Options

Page—Displays the output one page at a time

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show timezone

This command displays time zone information.

Command Syntax

show timezone

config

list [page]

Parameters

- **config** displays the current time zone settings.
- **list** displays the available time zones.

Options

- **page**—Displays the output one page at a time

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show trace

This command displays trace information for a particular task.

Command Syntax

show trace [task_name]

Parameters

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.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Example

This example displays trace information for cdp.

```
show trace cdp
```

show ups status

This command shows the current status of the USB-connected APC smart-UPS device and starts the monitoring service if not already started.

This command to give full status is only available on 7835-H2 and 7825-H2 servers.

Command Syntax

```
show ups status
```

show version

This command displays the software version on the active or inactive partition.

Command Syntax

```
show version
```

```
active
```

```
inactive
```

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show web-security

This command displays the contents of the current web-security certificate.

Command Syntax

```
show web-security
```

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show workingdir

This command retrieves the current working directory for activelog, inactivelog, install, and TFTP.

Command Syntax**show workingdir****Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

unset ipsec

This command allows you to disable IPSec policies and associations.

Command Syntax**unset ipsec****policy** {**ALL** | *policy-name*}**association** *policy-name* {**ALL** | *association-name*}**Parameters**

- *policy-name* represents the name of an IPSec policy.
- *association-name* represents the name of an IPSec association.

Requirements

Command privilege level: 1

Allowed during upgrade: No

unset network

This command unsets DNS options.

Command Syntax**unset network dns options** [**timeout**] [**attempts**] [**rotate**]**Parameters**

- **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.

Usage Guidelines

The system asks whether you want to continue to execute this command.

**Caution**

If you continue, the system will temporarily lose network connectivity.

utils core list

This command lists all existing core files.

Command Syntax

utils core list

utils core analyze

This command generates a backtrace for the specified core file, a thread list, and the current value of all CPU registers.

Command Syntax

utils core analyze *core file name*

Parameters

- *core file name* specifies the name of a core file.

Usage Guidelines

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

This command stops Cisco Security Agent (CSA).

Command Syntax

utils csa disable

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils csa enable

This command enables Cisco Security Agent (CSA).

Command Syntax

utils csa enable

Usage Guidelines

The system prompts you to confirm that you want to enable CSA.



Caution

You must restart the system after you start CSA.ca

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils csa status

This command displays the current status of Cisco Security Agent (CSA).

Command Syntax

utils csa status

Usage Guidelines

The system indicates whether CSA is running.

Requirements

Command privilege level: 0

Allowed during upgrade: No

utils dbreplication status

This command displays the status of database replication. You should run this command only on the first node (Publisher server) of a cluster.

Command Syntax

utils dbreplication status

utils dbreplication stop

This command stops the automatic setup of database replication.

Command Syntax

utils dbreplication stop

utils dbreplication repair

This command repairs database replication.

Command Syntax

utils dbreplication repair

utils dbreplication reset

This command resets and restarts database replication.

Command Syntax

utils dbreplication reset

utils disaster_recovery backup tape

This command starts a backup job and stores the resulting tar file on tape.

Command Syntax

backup tape *featurelist tapeid*

Parameters

- *featurelist* specifies the list of features to back up, separated by commas.
- *tapeid* represents the ID of an available tape device.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

utils disaster_recovery backup network

This command starts a backup job and stores the resulting tar file on a remote server.

Command Syntax

backup network *featurelist path servername username*

Parameters

- *featurelist* specifies the list of features to back up, separated by commas.
- *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.

Usage Guidelines



Note

The system prompts you to enter the password for the account on the remote server.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

utils disaster_recovery cancel_backup

This command cancels the ongoing backup job.

Command Syntax

utils disaster_recovery cancel_backup

Usage Guidelines

The system prompts you to confirm that you want to cancel the backup job.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

utils disaster_recovery restore tape

This command starts a restore job and takes the backup tar file from tape.

Command Syntax

restore tape *server tarfilename tapeid*

Parameters

- *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.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

utils disaster_recovery restore network

This command starts a restore job and takes the backup tar file from a remote server.

Command Syntax

restore network *restore_server tarfilename path servername username*

Parameters

- *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.

Usage Guidelines**Note**

The system prompts you to enter the password for the account on the remote server.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

utils disaster_recovery show_backupfiles network

This command starts a restore job and takes the backup tar file from a remote server.

Command Syntax

```
utils disaster_recovery show_backupfiles network path servername username
```

Parameters

- *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.

Usage Guidelines



Note

The system prompts you to enter the password for the account on the remote server.

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils disaster_recovery show_backupfiles tape

This command displays information about the backup files that are stored on a tape.

Command Syntax

```
utils disaster_recovery show_backupfiles tape tapeid
```

Parameters

- *tapeid* represents the ID of an available tape device.

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils disaster_recovery show_registration

This command displays the registered features and components on the specified server.

Command Syntax

```
utils disaster_recovery show_registration hostname
```

Parameters

- *hostname* specifies the server for which you want to display registration information.

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils disaster_recovery show_tapeid

This command displays a list of tape device IDs.

Command Syntax

utils disaster_recovery show_tapeid

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils disaster_recovery status

This command displays the status of the current backup or restore job.

Command Syntax

utils disaster_recovery status *operation*

Parameters

- *operation* specifies the name of the ongoing operation: **backup** or **restore**.

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils fior

This command allows you to monitor the I/O on the server. The File I/O Reporting service provides a kernel based daemon for collecting file I/O per process.

Command Syntax

utils fior

disable

enable

list

start

status

stop

top

Options

- **disable**—Prevents the file I/O reporting service from starting automatically when the machine boots. This command does not stop the service without a reboot. Use the **stop** option to stop the service immediately.
- **enable**—Enables the file I/O reporting service to start automatically when the machine boots. This command does not start the service without a reboot. Use the **start** option to start the service immediately.
- **list**—This command displays a list of file I/O events, in chronological order, from oldest to newest.
- **start**—Starts a previously stopped file I/O reporting service. The service remains in a started state until it is manually stopped or the machine is rebooted.
- **status**—Displays the status of the file I/O reporting service.
- **stop**—Stops the file I/O reporting service. The service remains in a stopped state until it is manually started or the machine is rebooted.
- **top**—Displays a list of top processes that create file I/O. This list can be sorted by the total number of bytes read, the total number of bytes written, the rate of bytes read, or the rate of bytes written.

utils iothrottle enable

This command enables I/O throttling enhancements. When enabled, I/O throttling enhancements lower the impact of upgrades on an active system.

Command Syntax

```
utils iothrottle enable
```

utils iothrottle disable

This command disables I/O throttling enhancements. This could adversely affect the system during upgrades.

Command Syntax

```
utils iothrottle disable
```

utils iothrottle status

This command displays the status of I/O throttling enhancements.

Command Syntax

```
utils iothrottle status
```

utils netdump client

This command configures the netdump client.

Command Syntax**utils netdump client**

start *ip-address-of-netdump-server*

status

stop

Parameters

- **start** starts the netdump client.
- **status** displays the status of the netdump 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.

Usage Guidelines

In the event of a kernel panic crash, the netdump client sends diagnostic information about the crash to a netdump server.

Requirements

Command privilege level: 0

Allowed during upgrade: No

utils netdump server

This command configures the netdump server.

Command Syntax**utils netdump server**

add-client *ip-address-of-netdump-client*

delete-client *ip-address-of-netdump-client*

list-clients

start

status

stop

Parameters

- **add-client** adds a netdump client.
- **delete-client** deletes a netdump client.
- **list-clients** lists the clients that are registered with this netdump server.
- **start** starts the netdump server.
- **status** displays the status of the netdump server.
- **stop** stops the netdump server.
- *ip-address-of-netdump-client* specifies the IP address of a netdump client.

Usage Guidelines

In the event of a kernel panic crash, a netdump-enabled client system sends diagnostic information about the crash to the netdump server.

netdump diagnostic information gets stored in the following location on the netdump server: *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.

Requirements

Command privilege level: 0

Allowed during upgrade: No

utils network arp

This command lists, sets, or deletes Address Resolution Protocol (ARP) table entries.

Command Syntax

utils network arp

list [*host host*] [**page**] [**numeric**]

set {*host*} {*address*}

delete *host*

Parameters

- **list** lists the contents of the address resolution protocol table.
- **set** sets an entry in the address resolution protocol table.
- **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

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils network capture eth0

This command captures IP packets on the specified Ethernet interface.

Command Syntax

utils network capture eth0 [*page*] [*numeric*] [*file fname*] [*count num*] [*size bytes*] [*src addr*] [*dest addr*] [*port num*]

Parameters

- **eth0** specifies Ethernet interface 0.

Options

- **page**—Displays the output one page at a time
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
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
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
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

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils network host

This command resolves a host name to an address or an address to a host name.

Command Syntax

utils network host *hostname* [**server** *server-name*] [**page**] [**detail**] [**srv**]

Parameters

- *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.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils network ping

This command allows you to ping another server.

Command Syntax

utils network ping *destination* [*count*]

Parameters

- *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.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils network tracert

This command traces IP packets that are sent to a remote destination.

Command Syntax

utils network tracert *destination*

Parameters

- *destination* represents the hostname or IP address of the server to which you want to send a trace.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils ntp

This command displays the NTP status or configuration.

Command Syntax

utils ntp {*status* | *config*}

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils remote_account

This command allows you to enable, disable, create, and check the status of a remote account.

Command Syntax**utils remote_account**

status

enable

disable

create *username life*

Parameters

- *username* specifies the name of the remote account. The username can contain only lowercase characters and must be more than six-characters long.
- *life* specifies the life of the account in days. After the specified number of day, the account expires.

Usage Guidelines

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. You can have only one remote account that is enabled at a time.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Example

```
utils remote_account status
```

utils reset_ui_administrator_name

This command resets the Cisco Unified Communications Operating System Administration administrator account name.

Command Syntax

```
utils reset_ui_administrator_name
```

utils reset_ui_administrator_password

This command resets the Cisco Unified Communications Operating System Administration password.

Command Syntax**utils reset_ui_administrator_password**

utils service list

This command retrieves a list of all services and their status.

Command Syntax**utils service list** [page]**Options**

- **page**—Displays the output one page at a time

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils service

This command stops, starts, or restarts a service.

Command Syntax**utils service****start** *service-name***stop** *service-name***restart** *service-name***auto-restart** {**enable** | **disable** | **show**} *service-name***Parameters**

- *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 Serviceability
- **enable** enables auto-restart.
- **disable** disables auto-restart
- **show** shows the auto-restart status

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils sftp handshake

This command exchanges SFTP SSH keys to all members of the cluster.

Command Syntax

utils sftp handshake

utils snmp test

This command tests the SNMP host by sending sample alarms to local syslog, remote syslog, and SNMP trap.

Command Syntax

utils snmp test

Requirements

Command privilege level: 0

Allowed during upgrade: No

utils soap realservice test

This command executes a number of test cases on the remote server.

Command Syntax

utils soap realservice test *remote-ip remote-https-user remote-https-password*

Parameters

- *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.

Requirements

Command privilege level: 0

Allowed during upgrade: No

utils system

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 Syntax

utils system {restart | shutdown | switch-version}

Usage Guidelines

The **utils system shutdown** command provides 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.

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils system upgrade

This command allows you to upgrade the server.

Command Syntax

utils system upgrade

cancel

get {local | remote} filename

list {local | remote} path

start

Parameters

- **cancel** cancels the active upgrade.
- **get** gets an upgrade file from which to upgrade.
- **local** specifies that the upgrade files are on a local drive.
- **remote** specifies that the upgrade files are on a remote system.
- *filename* specifies the name of the upgrade file.
- *path* specifies the path to the upgrade file(s).
- **list** lists the available upgrade files.
- **start** starts an upgrade with the upgrade file that is obtained with the **get** parameter.

Usage Guidelines

To upgrade the system, follow these major steps:

1. Use the **utils system upgrade list** command to display a list of the .iso upgrade files available on the local disk or remote server from which you plan to upgrade.
2. Use the **utils system upgrade get** command to get the upgrade file that you want to use.
3. Use the **utils system upgrade start** command to start upgrading from the upgrade file you got.



INDEX

A

administrator password [2-2](#)

B

browser requirements [1-1](#)

C

certificates

deleting [6-2](#)

displaying [6-2](#)

downloading [6-2](#)

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

expiration monitor fields (table) [6-7](#)

managing [6-1](#)

monitoring expiration dates [6-7](#)

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

uploading [6-3](#)

Certificate Trust List

See CTL

CLI

basics [A-2](#)

commands

completing [A-2](#)

described (table) [A-3](#)

getting help [A-2](#)

ending session [A-3](#)

overview [A-1](#)

starting a session [A-1](#)

cluster nodes

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

procedure [3-1](#)

Command Line Interface

See CLI

configuration

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

CTL

downloading [6-2](#)

managing [6-1](#)

uploading [6-3](#)

D

dial plan installation [7-5](#)

E

error messages

descriptions (table) [7-7](#)

Ethernet settings [4-1](#)

H

hardware, status

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

procedure [3-2](#)

I

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

installed software

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

procedure [3-3](#)

installing

dial plan [7-5](#)locales [7-6](#)

Internet Explorer

set security options [6-1](#)

IPSec

changing policy [6-10](#)displaying policy [6-10](#)management [6-8](#)policy fields (table) [6-9](#)setting up new policy [6-8](#)

L

locales

files [7-7](#)installation [7-6](#)

installer

error messages (table) [7-7](#)installing [7-6](#)

logging in

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

M

menu

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

messages, error

N

network status

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

nodes, cluster

fields (table) [3-1](#)procedure [3-1](#)NTP server settings [4-3](#)

O

operating system

administrator password [2-2](#)browser requirements [1-1](#)configuration [1-2, 3-1](#)

hardware status

fields (table) [3-2](#)procedure [3-2](#)introduction [1-1](#)logging in [2-1](#)network status fields (table) [3-3](#)overview [1-1](#)restart [5-1](#)security [1-3](#)services [1-3](#)settings [1-2, 4-1](#)software upgrades [1-3](#)status [1-2, 3-1](#)

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

R

remote support

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

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

S

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

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

settings
 Ethernet
 fields (table) [4-2](#)
 procedure [4-1](#)
 IP [4-1](#)
 menu [1-2](#)
 NTP servers [4-3](#)
 overview [4-1](#)
 publisher [4-2](#)
 SMTP [4-3](#)
 time [4-4](#)

show, menu [1-2](#)

shutdown, operating system [5-2](#)

SMTP settings [4-3](#)

software
 installation [7-1](#)
 installed
 fields (table) [3-4](#)
 procedure [3-3](#)
 upgrades [1-3](#)
 from local source [7-2](#)
 from remote source [7-3](#)

 overview [7-1](#)
 procedure [7-1](#)

status
 hardware
 fields (table) [3-2](#)
 procedure [3-2](#)
 network
 fields (table) [3-3](#)
 procedure [3-2](#)
 operating system [1-2, 3-1](#)
 system
 fields (table) [3-4](#)
 procedure [3-4](#)

supported products [7-8](#)

system
 restart [5-1](#)
 shutdown [5-2](#)
 status
 fields (table) [3-4](#)
 procedure [3-4](#)

T

TFTP server, installing files [7-8](#)

time settings [4-4](#)

V

version, restart [5-1](#)

