# PAWS Management Administration Guide

**First Published:** June 14, 2012

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

Text Part Number: OL-27270-01

© 2012 Cisco Systems, Inc. All rights reserved.

# CONTENTS


CHAPTER 1 **Introduction to PAWS Management** 1

Functional overview of PAWS Management 1

CHAPTER 2 **PAWS Management installation** 3

System requirements for installation 3

Important considerations 4

Frequently Asked Questions about the installation 4

Preinstallation tasks 6

Begin installation 13

Install PAWS-M 14

Post-installation tasks 15

Reset administrator and security passwords 16

CHAPTER 3 **PAWS Management service management** 17

Services 17

Alarms 21

Traces 23

CHAPTER 4 **Backup and restore** 27

Backed Up and Restored Data for PAWS Management 28

System requirements 28

Access the Disaster Recovery System 29

Master Agent duties and activation 29

Local Agent 30

Manage backup devices 30

Create backup schedules 31

Enable, disable, and delete schedules 32

Start a manual backup 32

Check backup status 33
Display backup files 33
Restore PAWS Management from a backup file 34
View the restore status 35
Error messages 35

CHAPTER 5 PAWS Management administrative interface basics 39
PAWS Management administrative interface overview 39
Browser support 40
Login and logout 42
Online help 42
Interface version 42
Accessibility 43
Access icons 43
Access buttons 43

CHAPTER 6 PAWS Management configuration 45
Configuration checklist for PAWS Management 46
Upgrade and application task management using PAWS Management 46
Limitations and restrictions 46
Best practices 47
Server configuration 47
Add a server 47
Import servers 48
To upload the .csv import file: 48
To import the servers: 48
Manage servers 48
Configure server groups 49
Add a server group 49
Manage server groups 49
Configure file servers 50
Add a file server 50
Manage file servers 50
Unified Communications (UC) Applications Synchronization 51
Tasks 51

Create a new install or upgrade task 51
Create a switch version task 52
Create a restart system task 53
Task list 53
Generate reports 54
Download a report 54

CHAPTER 7 Command line interface for PAWS Management 55
Start CLI session 55
CLI basics 56
Complete CLI commands 56
Obtain Help for commands 57
End CLI sessions 58
CLI command properties 58
Generic commands 58
help 58
quit 59
Delete commands 59
delete account 59
delete dns 59
delete dscp 60
delete ipsec policy_group 61
delete ipsec policy_name 61
delete process 62
delete smtp 62
File commands 63
file check 63
file delete* 63
file delete 63
file delete tftp 64
file delete dir tftp 65
file dump* 66
file dump 66
file dump sftpdetails 66
file fragmentation sdi* 67

file fragmentation sdi 67
file fragmentation sdi file 67
file fragmentation sdi all 68
file fragmentation sdl* 68
file fragmentation sdl 68
file fragmentation sdl file 69
file fragmentation sdl all 69
file get* 70
file get 70
file get salog 71
file list* 72
file list 72
file list salog 73
file search* 74
file search 74
file tail* 75
file tail activelog 75
file view* 76
file view 76
file view system-management-log 77
Set commands 77
set account* 77
set account enable 77
set account name 78
set accountlocking* 78
set accountlocking 78
set accountlocking count 79
set accountlocking unlocktime 80
set cli* 80
set cli pagination 80
set cli session timeout 81
set commandcount 81
set csr gen 82
set date 82
set dscp* 83

set dscp defaults 83
set dscp 84
set dscp marking 84
set ipsec* 85
set ipsec policy_group 85
set ipsec policy_name 86
set logging 86
set network* 87
set network cluster publisher 87
set network dhcp eth0 87
set network dns 88
set network dns options 89
set network domain 89
set network failover 90
set network gateway 91
set network hostname 91
set network ip eth0 92
set network ipv6 dhcp 93
set network ipv6 gateway 94
set network ipv6 service 95
set network ipv6 static_address 95
set network max_ip_conntrack 96
set network mtu 97
set network nic eth0 97
set network pmtud 98
set network restore 99
set network status eth0 100
set password* 101
set password age 101
set password change-at-login 102
set password complexity character 102
set password complexity character difference 103
set password complexity character max-repeat 104
set password expiry maximum-age 105
set password expiry minimum-age 106

set password expiry user maximum-age 106
set password expiry user minimum-age 107
set password history 108
set password inactivity 109
set password user admin 109
set password user security 110
set session maxlimit 111
set smtp 111
set timezone 112
set trace* 112
set trace disable 112
set trace enable 113
set web-security 114
set webapp session timeout 115
set workingdir 116
Show commands 116
show account 116
show accountlocking 117
show cert* 117
show cert list 117
show cert own 118
show cert trust 118
show cli* 119
show cli pagination 119
show cli session timeout 119
show csr* 119
show csr list 119
show csr own 120
show date 121
show diskusage 121
show dscp* 122
show dscp all 122
show dscp defaults 122
show dscp marking 123
show dscp status 124

show environment 124
show hardware 125
show ipsec* 125
show ipsec information 125
show ipsec policy_group 126
show ipsec policy_name 126
show ipsec status 127
show logins 127
show memory 127
show myself 128
show network* 128
show network all 128
show network cluster 129
show network dhcp eth0 129
show network eth0 130
show network failover 130
show network ip_conntrack 131
show network ipprefs 131
show network ipprefs 131
show network ipv6 132
show network max_ip_conntrack 133
show network route 133
show network status 134
show open* 134
show open files* 134
show open files all 134
show open files process 135
show open files regexp 135
show open ports* 136
show open ports all 136
show open ports process 136
show open ports regexp 136
show packages 137
show password* 137
show password 137

show password change-at-login 138
show password expiry* 138
show password expiry 138
show password expiry user 139
show password expiry user list 139
show perf* 140
show perf counterhelp 140
show perf list categories 140
show perf list classes 141
show perf list counters 141
show perf list instances 142
show perf query class 142
show perf query counter 143
show perf query instance 143
show perf query path 144
show process* 145
show process list 145
show process load 145
show process name 146
show process open-fd 147
show process pid 147
show process search 148
show process user 148
show process using-most cpu 149
show process using-most memory 149
show registry 150
show risdb* 150
show risdb list 150
show risdb query 151
show session maxlimit 152
show smtp 152
show stats io 152
show status 153
show tech* 154
show tech activesql 154

show tech all 154
show tech network all 155
show tech network hosts 155
show tech network interfaces 156
show tech network resolv 156
show tech network routes 157
show tech network sockets 158
show tech runtime 158
show tech system 159
show timezone 160
show timezone config 160
show timezone list 160
show trace 161
show ups status 161
show version* 162
show version active 162
show version inactive 162
show web-security 163
show webapp session timeout 163
show workingdir 163
Unset commands 164
unset ipsec* 164
unset ipsec policy_group 164
unset ipsec policy_name 164
unset network* 165
unset network dns options 165
unset network domain 165
unset network ipv6 static_address 166
Utils commands 166
utils auditd 166
utils core* 167
utils core analyze 167
utils core list 168
utils create report 168
utils diagnose 169

utils disaster_recovery* 170
utils disaster_recovery backup local 170
utils disaster_recovery cancel_backup 170
utils disaster_recovery device add local 171
utils disaster_recovery device add network 171
utils disaster_recovery device delete 172
utils disaster_recovery device list 173
utils disaster_recovery history 173
utils disaster_recovery restore local 174
utils disaster_recovery restore network 174
utils disaster_recovery schedule add 175
utils disaster_recovery schedule 175
utils disaster_recovery schedule list 176
utils disaster_recovery show_backupfiles 177
utils disaster_recovery show_registration 177
utils disaster_recovery status 178
utils firewall* 178
utils firewall ipv4 debug 178
utils firewall ipv4 179
utils firewall ipv4 list 179
utils firewall ipv4 status 180
utils firewall ipv6 debug 180
utils firewall ipv6 181
utils firewall ipv6 list 182
utils firewall ipv6 status 182
utils import config 182
Execute utils import config in Vmware deployment 183
utils iostat 183
utils iothrottle 184
utils ldap config 184
utils network* 185
utils network arp delete 185
utils network arp set 185
utils network arp list 186
utils network capture 187

utils network connectivity 188
utils network host 188
utils network ipv6 host 189
utils network ipv6 traceroute 189
utils network ipv6 ping 190
utils network ping 191
utils network traceroute 191
utils ntp* 192
utils ntp config 192
utils ntp restart 192
utils ntp server list 192
utils ntp start 193
utils ntp status 193
utils os* 194
utils os kerneldump 194
utils os kerneldump ssh 194
utils os secure 195
utils remote_account* 196
utils remote_account create 196
utils remote_account disable 196
utils remote_account enable 196
utils remote_account status 197
utils service* 197
utils service 197
utils service list 199
utils snmp* 199
utils snmp config 1/2c community-string 199
utils snmp config 1/2c inform 200
utils snmp config 1/2c trap 200
utils snmp config 3 inform 201
utils snmp config mib2 202
utils snmp config 3 trap 202
utils snmp config 3 user 203
utils snmp get 204
utils snmp hardware-agents 204

utils snmp test 205
utils snmp walk 206
utils system* 207
utils system restart 207
utils system shutdown 207
utils system switch-version 208
utils system boot 208
utils system upgrade 208

CHAPTER 8 Troubleshooting PAWS Management 211
SNMP setup 211
SNMP configuration checklist 211
SNMP users 213
SNMP trap notification destinations 215
SNMP inform notification destination 216
MIB2 system group 218
SNMP Management Information Base (MIB) 219
Troubleshooting installation 221
Manage network errors during installation 222
Examine log files 222
Troubleshooting PAWS-M components 222
Troubleshoot PAWS-M services 223
Failed COP file install or UC application server upgrade 223
Common PAWS-M errors 224
PAWS-M Log files 224
Troubleshoot PAWS-M administrative interface 225
Alarm management 225
Trace management 227

CHAPTER 1

# Introduction to PAWS Management

Platform Administrative Web Services Interface Management (PAWS-M) is an administrative platform for enterprise customers who want to perform and control the upgrades of their servers in a unified interface. PAWS-M allows you to:

- configure your server inventory for the system
- schedule and monitor upgrades of one or more servers across one or more clusters
- schedule system restarts for one of more servers
- switch versions between the active and inactive versions, for one or more servers


- Functional overview of PAWS Management, page 1

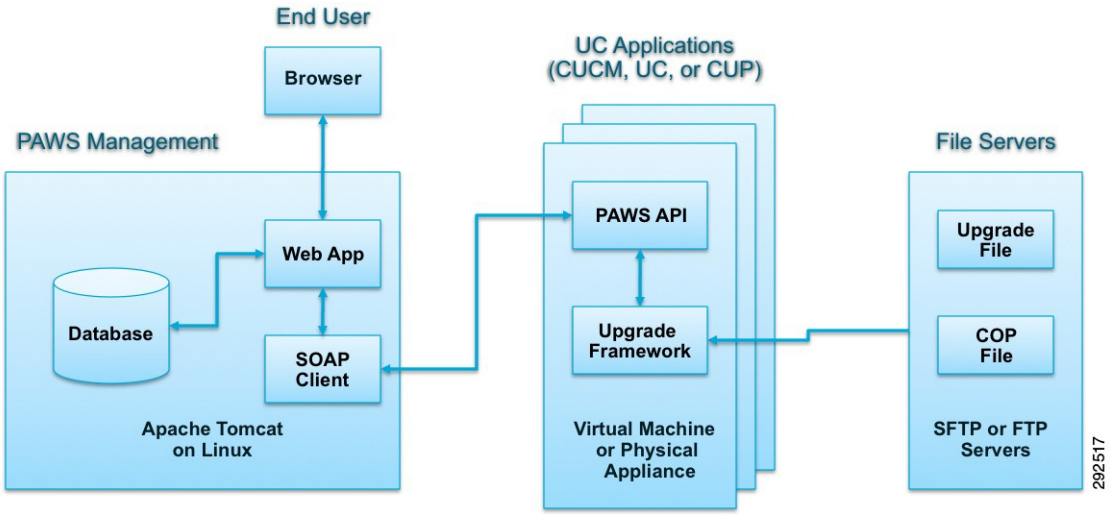

## Functional overview of PAWS Management

Using PAWS-M, you can control upgrades, restarts, and switch versions for Cisco Unified Communications Manager and Cisco Unity Connection servers, provided they are Release 8.6(1) or higher. PAWS-M can control upgrades for Cisco Unified Presence (CUP) servers provided they are release 9.0(2) or higher.

Using PAWS-M, the user can create an inventory of servers, and organize the servers into groups, to control upgrades, switch versions, and restarts of their application servers using one unified interface.

Figure 1 provides a high-level view of the Cisco PAWS-M architecture.

***Figure 1: PAWS-M architecture***




The user accesses PAWS-M through an administration GUI interface. Once an operation task has been scheduled (such as upgrade or restart), the PAWS-M platform sends a SOAP message to the UC Application servers (CUCM, or UC) to initiate the desired operation (upgrade, switch version, or restart). File Servers supply the Upgrade and COP files for the Application Server upgrades.

CHAPTER 2

# PAWS Management installation


- System requirements for installation, page 3
- Important considerations, page 4
- Frequently Asked Questions about the installation, page 4
- Preinstallation tasks, page 6
- Begin installation, page 13
- Install PAWS-M, page 14
- Post-installation tasks, page 15
- Reset administrator and security passwords, page 16


## System requirements for installation

As defined in the OVA used for the installation, the following are the server requirements for the Cisco PAWS-M platform.

***Table 1: PAWS-M Installation Server Requirements***

| Requirement | Notes |
|---|---|
| Product | PAWS Management |
| Version | 9.0(1) |
| CPU | 2 vCPUs |
| Memory | 8 GB (RAM) |
| Hard Drive | 80 GB (one) |

# Important considerations

Before you proceed with the installation, consider the following requirements and recommendations:

- Be aware that when you install on an existing server, the hard drive gets formatted and all existing data on the drive gets overwritten.
- Configure Cisco PAWS-M by using static IP addressing to ensure that the Cisco PAWS-M obtains a fixed IP address.
- You must enable Domain Network Server (DNS) and configure NTP during installation.
- Do not attempt to perform any configuration tasks during the installation.
- Do not install any Cisco-verified applications until you complete the installation.
- Carefully read the information that follows before you proceed with the installation.

# Frequently Asked Questions about the installation

The following section contains commonly asked questions and responses. Review this section carefully before you begin the installation. The section includes the following topics:

### How Much Time Does the Installation Require?

The entire PAWS-M installation process, excluding pre- and post-installation tasks, takes 20 to 30 minutes.

### What Usernames and Passwords Do I Need to Specify?

**Note** The system checks your passwords for strength. For guidelines on creating a strong passwords, see the "What Is a Strong Password?" section.

During the installation, you must specify the following usernames and passwords:

- Administrator account username and password
- Security password

You use the Administrator account username and password to log in to the following areas:

- PAWS-M GUI interface
- Command Line Interface

To specify the Administrator account username and password, follow these guidelines:

- Administrator account username—The Administrator account username must start with an alphabetic character and can contain alphanumeric characters, hyphens, and underscores.
- Administrator account password—The Administrator account password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores.

You can change the Administrator account password or add a new Administrator account by using the command line interface. For more information, see the “Command Line Interface for Cisco PAWS-M" section.

For the security password, the password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores.

### What is a Strong Password?

The Installation wizard checks to ensure that you enter a strong password. To create a strong password, follow these recommendations:

- Mix uppercase and lowercase letters.
- Mix letters and numbers.
- Include hyphens and underscores.
- Remember that longer passwords are stronger and more secure than shorter ones.

Avoid the following types of passwords:

- Do not use recognizable words, such as proper names and dictionary words, even when combined with numbers.
- Do not invert recognizable words.
- Do not use word or number patterns, such as aaabbb, qwerty, zyxwvuts, 123321, and so on.
- Do not use recognizable words from other languages.
- Do not use personal information of any kind, including birthdays, postal codes, names of children or pets, and so on.

### What Is the Cisco Unified Communications Answer File Generator?

Cisco Unified Communications Answer File Generator, a web application, generates answer files for unattended installations of Cisco PAWS-M. Individual answer files get copied to the root directory of a floppy disk and are used in addition to the Cisco PAWS-M DVD during the installation process.

The web application provides:

- Syntactical validation of data entries
- Online help and documentation
- Support for fresh installations (but does not support upgrades)

You can access the Cisco Unified Communications Answer File Generator at the following URL:

http://www.cisco.com/web/cuc_afg/index.html

The Cisco Unified Communications Answer File Generator supports Internet Explorer version 6.0 or higher and Mozilla version 1.5 or later.

Cisco requires that you use virtual floppy image (.flp) that is compatible with Linux 2.4. Cisco recommends that you use virtual floppy that is preformatted to be compatible with Linux 2.4 for the configuration file. These virtual floppies use a W95 FAT32 format.

### Which SFTP Servers Does Cisco Support?

SFTP servers are used for backups and restores, upgrades, and troubleshooting. Cisco allows you to use any SFTP server product but recommends SFTP products that have been certified with Cisco through the Cisco Technology Developer Partner program (CTDP). CTDP partners, such as GlobalSCAPE, certify their products with specified versions of Cisco Unified Communications Manager. For information on which vendors have certified their products with your version of Cisco Unified Communications Manager, see the following URL:

http://marketplace.cisco.com/catalog

For information on using GlobalSCAPE with supported Cisco Unified Communications versions, see the following URL:

http://www.globalscape.com/gsftps/cisco.aspx

Cisco uses the following servers for internal testing. You may use one of the servers, but you must contact the vendor for support:

- Open SSH (refer to http://sshwindows.sourceforge.net/)
- Cygwin (refer to http://www.cygwin.com/ )
- Titan (refer to http://www.titanftp.com/)

**Note** For issues with third-party products that have not been certified through the CTDP process, contact the third-party vendor for support.

### Can I Install Other Software on the Server?

You must perform all software installations and upgrades by using the CLI. The system can upload and process only software that Cisco approved. You cannot install or use unapproved third-party software applications.

# Preinstallation tasks

The following table contains a list of preinstallation tasks that you need to perform to ensure that you can successfully install Cisco PAWS-M.

***Table 2: Preinstallation Tasks***

| | Task |
|---|---|
| **Step 1** | Read this entire document to familiarize yourself with the installation procedure. |
| **Step 2** | Verify that all servers on which you plan to install Cisco PAWS-M are properly registered in DNS. |
| **Step 3** | Record the configuration settings for each server that you plan to install. |

### Allow network traffic

This section describes the minimum required ports that need to be configured to support PAWS-M server. The following table provides a summary of the ports that need to be configured on a corporate firewall. The port configurations shown in this table are based on default settings. If you change the default settings, you need to update these configurations.

If you have other servers/ports required on your network, you need to allow for that traffic.

***Table 3: Corporate firewall configuration***

| Direction | Source | Destination | Protocol | Port | Description |
|---|---|---|---|---|---|
| Outbound | PAWS-M | IP address of the ftp server | TCP | 21 | FTP access to PAWS-M server for uploading licenses/software, upgrade, and CLI access |
| Outbound | PAWS-M | IP address of the sftp server | TCP | 22 | SFTP access to PAWS-M server for uploading licenses/software, upgrade, and CLI access |
| Inbound | Internal network or any management workstation | PAWS-M server DMZ IP address | HTTP | 80 | HTTP access to non-secured GUI and web APIs (e.g. login page) |
| Inbound | Internal network or any management workstation | PAWS-M server DMZ IP address | HTTPS | 443 | HTTPS access to secured GUI and web APIs |
| Inbound | UC application servers | PAWS-M server DMZ IP address | HTTPS | 6060 | Asynchronous SOAP messages from application servers |
| Inbound | Internal network or any management workstation | PAWS-M server DMZ IP address | HTTPS | 8443 | HTTP alternate |
| Inbound | Internal network or any management workstation | PAWS-M server DMZ IP address | HTTP | 8080 | HTTP alternate |

### Additional Information

Preinstallation tasks

### Create virtual machines

Cisco provides a VM template for you to download and transfer to your virtual host. Use this template to create the VMs for PAWS-M platform installation.

Before you deploy the template and create VMs, you should have the VM name, VLAN, hostname, and the IP address allocated for each new VM.

Follow these steps to create a VM and to prepare the PAWS-M installation on it:

**Procedure**

| | |
|---|---|
| **Step 1** | Download the PAWS-M VM template for your application. Go to http://docwiki.cisco.com/wiki/Unified_Communications_Virtualization_Downloads_%28including_OVA/OVF_Templates%29 |
| **Step 2** | Download the template to a location on your PC or at a designated URL. |
| **Step 3** | Deploy the template file using vSphere Client. Enter the following information for the new VM:<br>• hostname<br>• datastore—Select datastore<br>• Provisioning type—thick or thin<br>• target VLAN |
| **Step 4** | Make sure that you complete the procedure to create the VM.<br>At this point a new VM is created with the correct amount of RAM, number of CPUs, size and number of disks for the intended application. |

### Set up virtual machine

This section provides information on how to set up a virtual machine.

**Procedure**

| | |
|---|---|
| **Step 1** | Open the Open Virtualization Format (OVF) or OVA Template from **File > Deployed OVF Template...** |
| **Step 2** | Use the Browse option to find the location of the OVA file.<br>**Note** The OVA file can be located on the PC or at an URL address. |
| **Step 3** | Follow the wizard to complete the OVA installation process. |

### Gather information for installation

Use the following table to record the information about PAWS-M. You may not need to obtain all the information; gather only the information that is pertinent to your system and network configuration.

**Note** Because some of the fields are optional, they may not apply to your configuration.

**Caution** You cannot change some of the fields after installation without reinstalling the software, so be sure to enter the values that you want. The last column in the table shows whether you can change a field after installation; if so, the appropriate CLI command is shown.

***Table 4: Server configuration data***

| Parameter | Description | Can Entry Be Changed After Installation? |
|---|---|---|
| **Administrator ID** | This field specifies the Administrator account user ID that you use for secure shell access to the CLI on PAWS-M. | No, you cannot change the entry after installation.<br>**Note** After installation, you can create additional Administrator accounts, but you cannot change the original Administrator account user ID. |
| **Administrator Password** | This field specifies the password for the Administrator account, which you use for secure shell access to the CLI.<br>You also use this password with the adminsftp user. You use the adminsftp user to access local backup files, upload server licenses, and so on.<br>Ensure the password is at least six characters long; the password can contain alphanumeric characters, hyphens, and underscores. | Yes, you can change the entry after installation by using the following CLI command:<br>CLI > **set password admin** |
| **Country** | From the list, choose the appropriate country for your installation. | Yes, you can change the entry after installation by using the following CLI command:<br>CLI > **set web-security** |
| **DHCP** | Cisco requires that you choose **No** to the DHCP option. After you choose **No**, enter a hostname, IP address, IP mask, and gateway. | No, you should not change the entry after installation. |

| Parameter | Description | Can Entry Be Changed After Installation? |
|---|---|---|
| **DNS Enable** | A DNS server resolves a hostname into an IP address or an IP address into a hostname.<br>PAWS-M requires that you use a DNS server. Choose **Yes** to enable DNS. | No, you should not change the entry after installation. |
| **DNS Primary** | Enter the IP address of the DNS server that you want to specify as the primary DNS server. Enter the IP address in dotted decimal format as ddd.ddd.ddd.ddd. | Yes, you can change the entry after installation by using the following CLI command:<br>CLI > **set network dns**<br>To view DNS and network information, use the following CLI command:<br>CLI > **network eth0 detail** |
| **DNS Secondary (optional)** | Enter the IP address of the DNS server that you want to specify as the optional secondary DNS server. | Yes, you can change the entry after installation by using the following CLI command:<br>CLI > **set network dns** |
| **Gateway Address** | Enter the IP address of the network gateway.<br>If you do not have a gateway, you must still set this field to 255.255.255.255. Not having a gateway may limit you to being able to communicate only with devices on your subnet. | Yes, you can change the entry after installation by using the following CLI command:<br>CLI > **set network gateway** |
| **Hostname** | Enter a hostname that is unique to your server.<br>The hostname can comprise up to 64 characters and can contain alphanumeric characters and hyphens. The first character cannot be a hyphen. | Yes, you can change the entry after installation.<br>CLI > **set network hostname** |

| Parameter | Description | Can Entry Be Changed After Installation? |
|---|---|---|
| **IP Address** | Enter the IP address of your server. | Yes, you can change the entry after installation.<br>CLI > set network ip eth0<br>**Note** If you have network fault tolerance enabled, you must disable it before you change the IP address by entering **set network failover dis**. Then, re-enable network fault tolerance after you change the IP address by entering **set network failover ena**. |
| **IP Mask** | Enter the IP subnet mask of this machine. | Yes, you can change the entry after installation by using the following CLI command:<br>CLI > **set network ip eth0** |
| **Location** | Enter the location of the server.<br>You can enter any location that is meaningful within your organization. Examples include the state or the city where the server is located. | Yes, you can change the entry after installation by using the following CLI command:<br>CLI > **set web-security** |
| **MTU Size** | The maximum transmission unit (MTU) represents the largest packet, in bytes, that this host will transmit on the network.<br>Enter the MTU size in bytes for your network. If you are unsure of the MTU setting for your network, use the default value.<br>Default specifies 1500 bytes. | Yes, you can change the entry after installation by using the following CLI command:<br>CLI > **set network mtu** |
| **NIC Duplex** | Choose the duplex mode for the network interface card (NIC), either Full or Half.<br>**Note** This parameter appears only when you choose not to use Automatic Negotiation. | Yes, you can change the entry after installation by using the following CLI command:<br>CLI > **set network nic** |

| Parameter | Description | Can Entry Be Changed After Installation? |
|---|---|---|
| **NIC Speed** | Choose the speed for the NIC, 1 Gigabits per second or higher.<br>**Note** This parameter appears only when you choose not to use Automatic Negotiation. | Yes, you can change the entry after installation by using the following CLI command:<br>CLI > **set network nic** |
| **NTP Server** | Enter the hostname or IP address of one or more Network Time Protocol (NTP) servers with which you want to synchronize.<br>You can enter up to five NTP servers.<br>**Note** To avoid potential compatibility, accuracy, and network jitter problems, the external NTP servers that you specify for the primary node can be NTP v4 (version 4). If you are using IPv6 addressing, external NTP servers must be NTP v4. | Yes, you can change the entry after installation Yes, you can change the entry after installation<br>CLI > **utils ntp server** |
| **Organization** | Enter the name of your organization.<br>**Tip** You can use this field to enter multiple organizational units. To enter more than one organizational unit name, separate the entries with a comma. For entries that already contain a comma, enter a backslash before the comma that is included as part of the entry. | Yes, you can change the entry after installation by using the following CLI command:<br>CLI > **set web-security** |
| **Security Password** | The password must contain at least six alphanumeric characters. The password can contain hyphens and underscores, but it must start with an alphanumeric character.<br>**Note** Save this password. | Yes, you can change the entry after installation by using the following CLI command:<br>CLI > **set password security** |

| Parameter | Description | Can Entry Be Changed After Installation? |
|---|---|---|
| **State** | Enter the state that the server is located. | Yes, you can change the entry after installation by using the following CLI command:<br>CLI > **set web-security** |
| **Time Zone** | This field specifies the local time zone and offset from Greenwich Mean Time (GMT).<br>Choose the time zone that most closely matches the location of your machine. | Yes, you can change the entry after installation by using the following CLI command:<br>CLI > **set timezone**<br>To view the current time zone configuration, use the following CLI command:<br>CLI > **show timezone config** |
| **Unit** | Enter your unit. | Yes, you can change the entry after installation by using the following CLI command:<br>CLI > **set password admin** |

# Begin installation

This section describes how to install PAWS-M. You install the operating system and PAWS-M by running one installation program.

For information on how to navigate within the installation wizard, refer to the following table.

***Table 5: Installation Wizard Navigation***

| To Do This | Press This |
|---|---|
| Move to the next field | **Tab** |
| Move to the previous field | **Alt-Tab** |
| Choose an option | Space bar or **Enter** |
| Scroll up or down in a list | **Up Arrow** or **Down Arrow** key |
| Go to the previous window | Space bar or Enter to choose Back (when available) |
| Get help information for a window | Space bar or Enter to choose Help (when available) |

# Install PAWS-M

This section provides information on how to install PAWS-M.

### Procedure

**Step 1** Insert the CD into the client machine running vSphere client. Edit the settings of the virtual machine's CD/DVD drive to use the client drive.

**Step 2** Reboot and start the virtual machine.

**Note** An installation screen appears to start the installation of the PAWS-M.

**Step 3** Follow the wizard installation as shown in the following table

| Sequence | Wizard Task | Remarks |
|---|---|---|
| **Step 1** | Media Check Screen | Click **Yes** if media has not been verified previously. If the media has been verified, you may click No to skip the media check. |
| **Step 2** | Product Deployment Selection | Click **OK**. |
| **Step 3** | Override Previous Installation | Select **Yes** or **No**. |
| **Note** For the DNS option, if the virtual machine cannot reach the DNS and the hostname of the PAWS-M server is not resolvable using that DNS server then the installation gives an error and does not proceed. | | |
| **Step 4** | Platform Installation Wizard | Select **Proceed**. |
| **Step 5** | Basic Installation | Select **Continue**. |
| **Step 6** | Timezone Configuration | Select the time zone from the drop-down list, and click **OK**. |
| **Step 7** | Auto Negotiation Configuration | Select **Continue**. |
| **Step 8** | MTU Configuration | Select **No** for no change, or **Yes** to enter new values. |
| **Note** The virtual machine must be able to reach the gateway that is entered for the static configuration, or else the installation gives an error and does not proceed.<br>**Note** For the DNS option, if the virtual machine cannot reach the DNS and the hostname of the PAWS-M server is not resolvable using that DNS server then the installation gives an error and does not proceed. | | |
| **Step 9** | DHCP Configuration | The IP address is hardcoded. Select **Yes** for no change. Select **No** for DHCP. |

| Sequence | Wizard Task | Remarks |
|---|---|---|
| **Step 10** | Static Network Configuration | Fill the fields Host Name, IP Address, IP Mask, Gateway Address. Click **OK**. |
| **Step 11** | DNS Client Configuration | If you select **Yes** to DNS client configuration, perform Step 12. If you select **No**, perform Step 13. |
| **Step 12** | DNS Client Configuration | Select **Primary DNS**, **Secondary DNS**, or **Domain**. |
| **Step 13** | Administrator Login Configuration | Fill the fields Administrator ID, Password, and Confirm Password. Click **OK.** |
| **Step 14** | Certificate Information | Enter the appropriate information in each field. Click **OK.** |
| **Step 15** | Network Time Protocol Client Configuration | Enter the appropriate information in each field. Click **OK.** |
| **Step 16** | Security Configuration | Fill the fields Security Password and Confirm Password. Click **OK.** |
| **Step 17** | Platform Configuration Confirmation | Click OK to start the installation. |

**Step 4** When the installation process is complete, you get prompted to log in by using the Administrator account and password.

**Step 5** Complete the post-installation tasks in the Post-installation tasks.

# Post-installation tasks

### Procedure

**Step 1** Configure the backup settings. Remember to back up your Cisco PAWS-M data daily.

**Step 2** Verify that you have a valid Network Time Protocol (NTP). To perform this check, log into the Cisco PAWS-M command line interface and enter **utils ntp status**.

### Related Topics

Backup and restore, on page 27
Services, on page 17

# Reset administrator and security passwords

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

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

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

### Procedure

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

- Username: pwrecovery
- Password: pwreset
  The Welcome to platform password reset window appears.

**Step 2** Press any key to continue.

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

**Step 4** Press any key to continue.
The system tests to ensure that you have removed the CD or DVD from the disk drive.

**Step 5** Insert a valid CD or DVD into the disk drive.
**Note** For this test, you must use a data CD, not a music CD. The system tests to ensure that you have inserted the disk.

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

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

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

**Step 8** Reenter the new password.
The password must contain at least six characters. The system checks the new password for strength. If the password does not pass the strength check, you get prompted to enter a new password.

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

CHAPTER 3

# PAWS Management service management

The Cisco PAWS-M platform contains network services and servlets that the system requires to function. Since these services are required for basic functionality, they do not require activation. However, you may need to stop and start (or restart) these services for troubleshooting purposes.

Alarms provide information on runtime status and the state of the system, so you can troubleshoot problems that are associated with your system. After viewing the alarm information, you can run a trace on the service. The trace files can help you further troubleshoot issues with your system.

This section contains information on services and describes how to troubleshoot issues using alarms and traces:


- Services, page 17
- Alarms, page 21
- Traces, page 23


## Services

After the installation of the Cisco PAWS-M platform, most services start automatically. You can configure services by setting service parameters for each service. If necessary, for example, for troubleshooting purposes, you may need to stop and start (or restart) a service. You can perform these task by using the command line interface (CLI) on the Cisco PAWS-M platform.

### Cisco PAWS-M Platform Manager Service

The Cisco Platform Manager Service supports the PAWS-M application interface. This service must be active for the PAWS-M application to work correctly. It is active by default.

### Performance and Monitoring Services

This section describes the Performance and Monitoring Services.

#### Cisco Log Partition Monitoring Tool

The Cisco Log Partition Monitoring Tool service supports the Log Partition Monitoring feature, which monitors the disk usage of the log partition on the Cisco PAWS-M platform by using configured thresholds and a polling interval.

**Cisco RIS Data Collector**

The Real-Time Information Server (RIS) maintains real-time information, such as critical alarms generated.

**Cisco AMC Service**

This service, Alert Manager and Collector service, allows you to retrieve real-time information that exists on the server.

**Cisco Audit Event Service**

The Cisco Audit Event Service monitors and logs any configuration change to the Cisco PAWS-M platform by a user or as a result of the user action.

**SOAP -Log Collection APIs Service**

The Cisco SOAP-Log Collection APIs service allows you to collect log files and to schedule collection of log files on a remote SFTP server. Examples of log files that you can collect include syslog, core dump files, Cisco application trace files, and so on.

**SOAP -Performance Monitoring APIs Service**

The Cisco SOAP Performance Monitoring APIs service allows you to use performance monitoring counters for various applications through SOAP APIs; for example, you can monitor memory information per service, CPU usage, and so on.

### Backup and Restore Services

This section describes the Backup and Restore Services.

**Cisco DRF Master**

The Cisco DRF Master Agent service supports the DRF Master Agent, which works with the CLI to schedule backups, perform restorations, view dependencies, check status of jobs, and cancel jobs, if necessary. The Cisco DRF Master Agent also provides the storage medium for the backup and restoration process.

**Cisco DRF Local**

The Cisco DRF Local service supports the Cisco DRF Local Agent, which acts as the workhorse for the DRF Master Agent. Components register with the Cisco DRF Local Agent to use the disaster recovery framework. The Cisco DRF Local Agent executes commands that it receives from the Cisco DRF Master Agent. Cisco DRF Local Agent sends the status, logs, and command results to the Cisco DRF Master Agent.

### System Services

This section describes the System Services.

**Cisco CDP**

Cisco CDP advertises the voice application to other network management applications, so the network management application can perform network management tasks for the voice application.

**Cisco Trace Collection Servlet**

The Cisco Trace Collection Servlet, along with the Cisco Trace Collection Service, supports trace collection and allows users to view traces. If you stop this service, you cannot collect or view traces on the Cisco PAWS-M platform.

For SysLog Viewer and trace and log collection, the Cisco Trace Collection Servlet and the Cisco Trace Collection Service must run on the server.

**Cisco Trace Collection Service**

The Cisco Trace Collection Service, along with the Cisco Trace Collection Servlet, supports trace collection and allows users to view traces. If you stop this service, you cannot collect or view traces on the Cisco PAWS-M platform.

For SysLog Viewer and trace and log collection, the Cisco Trace Collection Servlet and the Cisco Trace Collection Service must run on the server.

**Tip** If necessary, Cisco recommends that, to reduce the initialization time, you restart the Cisco Trace Collection Service before restarting Cisco Trace Collection Servlet.

### Platform Services

This section describes the Platform Services.

**Cisco Tomcat**

The Cisco Tomcat service supports the web server.

**Cisco Tomcat Stats Servlet**

The Cisco Tomcat Stats servlet collects the Tomcat statistics.

**Platform Administrative Web Service**

**Important** This service should *not* be activated on the PAWS-M server

The Platform Administrative Web service is a SOAP API that can be activated on CUCM, CUP and UC systems, to allow the PAWS-M server to upgrade the system.

**SNMP Master Agent**

This service, which acts as the agent protocol engine, provides authentication, authorization, access control, and privacy functions that relate to SNMP requests.

**Tip** After you complete SNMP configuration in the CLI, you must restart the SNMP Master Agent service.

**MIB2 Agent**

This service provides SNMP access to variables, which are defined in RFC 1213, that read and write variables; for example, system and interfaces.

**Host Resources Agent**

This service provides SNMP access to host information, such as storage resources, process tables, and installed software base. This service implements the HOST-RESOURCES-MIB.

**System Application Agent**

This service provides SNMP access to the applications that are installed and executing on the system. This implements the SYSAPPL-MIB.

**Cisco CDP Agent**

This service uses the Cisco Discovery Protocol to provide SNMP access to network connectivity information on the Cisco PAWS-M platform. This service implements the CISCO-CDP-MIB.

**Cisco Syslog Agent**

This service supports gathering of syslog messages that various components generate. This service implements the CISCO-SYSLOG-MIB.

**Cisco Certificate Expiry Monitor**

This service periodically checks the expiration status of certificates that the system generates and sends notification when a certificate gets close to its expiration date.

### Working with Services

To start, stop, activate, or restart services or to configure service parameters for services on the Cisco PAWS-M platform, you must use the command line interface (CLI). You can start, stop, activate, or refresh only one service at a time. Be aware that when a service is stopping, you cannot start it until after the service is stopped. Likewise, when a service is starting, you cannot stop it until after the service is started.

The following services are activated by default after you install the Cisco PAWS-M platform.

- Cisco AMC Service
- Cisco Audit Event Service
- Cisco CDP
- Cisco CDP Agent
- Cisco Certificate Expiry Monitor
- Cisco DRF Local
- Cisco DRF Master
- Cisco Log Partition Monitoring Tool
- Cisco Platform Manager Service
- Cisco RIS Data Collector
- Cisco Syslog Agent
- Cisco Tomcat
- Cisco Tomcat Stats Servlet
- Cisco Trace Collection Servlet
- Host Resources Agent
- MIB2 Agent
- SNMP Master Agent
- System Application Agent

The following services are stopped by default after you install the Cisco PAWS-M platform.

- Cisco Trace Collection Service
- SOAP -Log Collection APIs
- SOAP -Performance Monitoring APIs

The following services are deactivated by default after you install the Cisco PAWS-M platform.

- Platform Administrative Web Service - this service should not be active on the PAWS-M server, this service should be activated on Application servers (CUCM, CUC, CUP) that will be upgraded, using the PAWS-Management server.

**Caution** Some changes to service parameters may cause system failure. Cisco recommends that you do not make any changes to service parameters unless you fully understand the feature that you are changing or unless the Cisco Technical Assistance Center (TAC) specifies the changes.

The following table shows the commands that you need to work with services on the Cisco PAWS-M platform.

***Table 6: Service CLI Commands***

| Task | Command |
|---|---|
| Display a list of services and service status | utils service list |
| Activate a service | utils service activate *servicename* |
| Stop a service | utils service stop *servicename* |
| Start a service | utils service start *servicename* |
| Restart a service | utils service restart *servicename* |

# Alarms

Alarms provide information on runtime status and the state of the system, so you can troubleshoot problems that are associated with your system; for example, to identify issues with the Disaster Recovery System. Alarm information, which includes an explanation and recommended action, also includes the application name, machine name, and so on, to help you perform troubleshooting.

You configure the alarm interface to send alarm information to multiple locations, and each location can have its own alarm event level (from debug to emergency). Alarms can go to the Syslog Viewer (local syslog), Syslog file (remote syslog), SNMP traps, or to all destinations.

When a service issues an alarm, the alarm interface sends the alarm information to the locations that you configure (and that are specified in the routing list in the alarm definition). The system can either forward the alarm information, as is the case with SNMP traps, or the system can write the alarm information to its final destination (such as a log file).

As soon as you enter the CLI command, the system will prompt you for the required parameters. Enter the values to see the output.

This table shows the commands that you need to work with alarms on the Cisco PAWS-M platform.

*Table 7: Alarm CLI commands*

| Task | Command |
|---|---|
| Display the alarm configuration for a specific service/list of all services | **show alarm**<br>Required Parameter:<br>*servicename*: Name of the service. It can contain multiple words.<br>Example:<br>Enter the *servicename* as all to show the alarm configurations of all the services.<br>Enter the *servicename* as Cisco Tomcat to show the alarm configuration of Cisco Tomcat service. |
| Enable/Disable alarms for a particular destination | **set alarm** *status*<br>Required Parameters:<br>*status*: Enable or disable.<br>*servicename*: Name of the service. It can contain multiple words.<br>*monitorname*: SDI, SDL, Event_Log, or Sys_Log. |
| Enable alarms for a remote Syslog server | **set alarm remotesyslogserver**<br>Required Parameters:<br>*servicename*: Name of the service. It can contain multiple words.<br>*servername*: Name of the remote syslog server. |

| Task | Command |
|---|---|
| Set the event level for an alarm | **set alarm severity**<br>Required Parameters:<br>*servicename*: Name of the service. It can contain multiple words.<br>*monitorname*: SDI, SDL, Event_Log, or Sys_Log.<br>*severity* equals one of the following:<br>• Emergency: This level designates the system as unusable.<br>• Alert: This level indicates that immediate action is needed.<br>• Critical: The system detects a critical condition.<br>• Error: This level signifies that an error condition exists.<br>• Warning: This level indicates that a warning condition is detected.<br>• Notice: This level designates a normal but significant condition.<br>• Informational: This level designates information messages only.<br>• Debug: This level designates detailed event information that Cisco TAC engineers use for debugging. |
| Set alarm configuration to default values<br>**Tip** This option is available only for service names beginning with Cisco. | **set alarm default**<br>Required Parameters:<br>*servicename*: Name of the service. It can contain multiple words. |

# Traces

Traces assist you in troubleshooting issues with your application. You use the CLI to specify the level of information that you want traced as well the type of information that you want to be included in each trace file. You can configure trace parameters for any service on the PAWS-M platform.

After you have configured information that you want to include in the trace files for the various services, you can collect and view trace files through trace and log collection. To do this, configure trace using the **set trace** CLI command.

You can configure the level of information that you want traced (debug level), what information you want to trace (trace fields), and information about the trace files (such as number of files per service, size of file, and time that the data is stored in the trace files).

### Configuring Trace

You use the command line interface (CLI) to enable and disable tracing as well as to configure trace settings for specific services on the PAWS-M platform. As soon as you enter the CLI command, the system prompts you for the required parameters. For more information regarding trace collection, see the Traces.

The following table shows the commands required to work with traces on the PAWS-M platform:

| Task | Command |
|---|---|
| Display the trace configuration for a specified service | show trace<br>Required Parameter:<br>servicename—Name of the service. It can contain multiple words.<br>Example:<br>Enter the servicename as all to show the trace configurations of all the services.<br>Enter the servicename as Cisco AMC Service to show the trace configuration of Cisco AMC service. |
| Display the trace levels available for a specified service | show tracelevels<br>Required Parameter:<br>servicename—Name of the service. It can contain multiple words. |
| Enable/Disable trace for a specified service | set trace status<br>Required Parameters:<br>status— enable or disable<br>servicename—Name of the service. It can contain multiple words. |
| Specify the debug trace level settings for a specified service | set trace tracelevel<br>Required Parameters:<br>tracelevel—Use show tracelevels CLI command to find the trace levels for a given servicename.<br>servicename—Name of the service. It can contain multiple words. |

| Task | Command |
|---|---|
| Specify the maximum size of a trace files for a specific service from 1 to 10 megabytes. | set trace maxfilesize<br>Required Parameters:<br>servicename—Name of the service. It can contain multiple words.<br>size—Maximum size of the trace files from 1 to 10 megabytes. |
| Specify the maximum number of trace files per service.<br>The system automatically appends a sequence number to the file name to indicate which file it is; for example, cus299.txt. When the last file in the sequence is full, the trace data begins writing over the first file. | set trace maxnumfiles<br>Required Parameters:<br>servicename—Name of the service. It can contain multiple words.<br>filecount—Number of trace files from 1 to 10000. |
| Set the usercategories flag to the value provided, for a specified service.<br>**Tip** This option is available only for service names beginning with Cisco. | set trace usercategories<br>Required Parameters:<br>flagnumber—Hexadecimal value from 0 to 7FFF. 7FFF means all the flags are enabled.<br>servicename—Name of the service. It can contain multiple words. |
| Set trace configuration to default values for a specified service.<br>**Tip** This option is available only for service names beginning with Cisco. | set trace default<br>Required Parameters:<br>servicename—Name of the service. It can contain multiple words. |

### Collecting Traces (Logs)

You can collect trace files by performing any of the following tasks:

- To view the trace files directly from the CLI, enter the following the CLI commands:
  - file list
  - file view
  - file search
- To bundle the various trace files and send them to the local SFTP directory, enter the CLI command file get. Then, use a SFTP client to obtain the .tar files and send to the team that troubleshoots.

CHAPTER 4

# Backup and restore

The Disaster Recovery System (DRS), which you invoke from the command line interface (CLI) on the Cisco PAWS-M platform, provides data backup and restore capabilities for the Cisco PAWS-M. The Disaster Recovery System allows you to perform regularly scheduled automatic or user-invoked data backups. The Disaster Recovery System includes the following capabilities:

- A command line interface for performing backup and restore tasks.
- A distributed system architecture for performing backup and restore functions.
- Scheduled backups.

The Disaster Recovery System contains two key functions, Master Agent (MA) and Local Agent (LA). The Master Agent coordinates backup and restore activity with Local Agents.

This chapter contains information on the following topics:


- Backed Up and Restored Data for PAWS Management, on page 28
- System requirements, on page 28
- Access the Disaster Recovery System, on page 29
- Master Agent duties and activation, on page 29
- Local Agent, on page 30
- Manage backup devices, on page 30
- Create backup schedules, on page 31
- Enable, disable, and delete schedules, on page 32
- Start a manual backup, on page 32
- Check backup status, on page 33
- Display backup files, on page 33
- Restore PAWS Management from a backup file, on page 34
- View the restore status, on page 35
- Error messages, on page 35

- Backed Up and Restored Data for PAWS Management, page 28
- System requirements, page 28
- Access the Disaster Recovery System, page 29
- Master Agent duties and activation, page 29
- Local Agent, page 30
- Manage backup devices, page 30
- Create backup schedules, page 31
- Enable, disable, and delete schedules, page 32
- Start a manual backup, page 32
- Check backup status, page 33
- Display backup files, page 33
- Restore PAWS Management from a backup file, page 34
- View the restore status, page 35
- Error messages, page 35


# Backed Up and Restored Data for PAWS Management

The Disaster Recovery System backs up and restores all configuration for Cisco PAWS-M. In addition, DRS restores its own settings (backup device settings and schedule settings) as part of the backup/restore process. DRS backs up and restores drfDevice.xml and drfSchedule.xml files. When the server is restored with these files, you do not need to reconfigure the DRS backup device and schedule.

# System requirements

**Tip** Schedule backups during periods when you expect less network traffic.

**Note** While a backup or restore is running, the command line interface may block you from running some commands, including commands that support upgrades.

Archive backups to a local drive or remote SFTP server. The Disaster Recovery System does not support tape drives for backup and restore on the Cisco PAWS-M platform. You must choose a local device if you do not have outgoing SFTP access to the Cisco PAWS-M platform. If you store backup files to a local device, DRS stores the backup files in the /common/adminsftp/backup directory. You must manually move local backup files from the Cisco PAWS-M platform by opening an SFTP client and connecting to the Cisco PAWS-M platform by using the adminsftp user and the administrator password that you set up during installation.

To back up data to a remote device on the network or to move a local backup to another location, you must have an SFTP server that is configured. Cisco allows you to use any SFTP server product but recommends

SFTP products that have been certified with Cisco through the Cisco Technology Developer Partner program (CTDP). CTDP partners, such as GlobalSCAPE, certify their products with specified versions. For information on which vendors have certified their products with your version, refer to the following URL:

http://marketplace.cisco.com/catalog

For information on using GlobalSCAPE with supported Cisco Unified Communications versions, refer to the following URL:

http://www.globalscape.com/gsftps/cisco.aspx

Cisco uses the following servers for internal testing. You may use one of the servers, but you must contact the vendor for support:

- Open SSH (refer to http://sshwindows.sourceforge.net/)
- Cygwin (refer to http://www.cygwin.com/)
- Titan (refer to http://www.titanftp.com/)

**Note** For issues with third-party products that have not been certified through the CTDP process, contact the third-party vendor for support.

# Access the Disaster Recovery System

To access the Disaster Recovery System, start an SSH session and log in to the CLI on the Cisco PAWS-M platform. To log in to the CLI, you must enter the administrator username and password (from the Cisco PAWS-M installation, unless you changed it after installation).

# Master Agent duties and activation

The system automatically activates the Master Agent on the Cisco PAWS-M platform. The Master Agent performs the following duties:

- The Master Agent stores systemwide component registration information.
- The Master Agent maintains a complete set of scheduled tasks in an XML file. The Master Agent updates this file when it receives updates of schedules from the user interface. The Master Agent sends executable tasks to the applicable Local Agents, as scheduled. (Local Agents execute immediate-backup tasks without delay.)
- You access the Master Agent through Disaster Recovery System to perform activities such as configuring backup devices, scheduling backups by adding new backup schedules, viewing or updating an existing schedule, displaying status of executed schedules, and performing system restoration.
- The Master Agent stores backup data on a local directory or a remote network location.

# Local Agent

The server has a Local Agent to perform backup and restore functions. The Local Agent runs backup and restore scripts on the server.

# Manage backup devices

Before using the Disaster Recovery System, you must configure the locations where you want the backup files to be stored. You can create local or network backup devices. If you create a local backup device, Disaster Recovery System stores the backup files in the a preconfigured directory on the Cisco PAWS-M platform. You must manually move local backup files from the Cisco PAWS-M platform by opening an SFTP client and connecting to the Cisco PAWS-M platform by using the adminsftp user and the administrator password that you set up during Cisco PAWS-M installation.

**Note** The system automatically deletes local backup files that are more than one week old. When you perform a backup. a warning message displays that indicates that local backup files get deleted after one week.

You can estimate the size of the .tar file that the backup creates by entering **utils disaster_recovery estimate_tar_size**.

You can configure up to 10 backup devices. Perform the following steps to configure backup devices.

### Procedure

**Step 1** To access the Disaster Recovery System, start an SSH session and log in to the CLI on the Cisco PAWS-M platform.
The CLI admin prompt displays.

**Step 2** To create a local device, enter **utils disaster_recovery device add local** *device_name number of backups*
*device_name* equals the name of the backup device. The backup device name may contain only alphanumeric characters, spaces ( ), hyphens (-) and underscores (_). Do not use any other characters. By default, DRS stores backup files for local devices in the /common/adminsftp/backup directory.

*number of backups* equals the number of backups that are retained for the backup server. When the backup reaches the limit, the oldest backup files on the backup server are deleted and the new backup files are added.

**Step 3** To create a network device so that you can store backup files on a network drive that is accessed through an SFTP connection, enter **utils disaster_recovery device add network** *device_name path server_name username number_of_backups*
where

*device_name* equals the name of the backup device. The backup device name may contain only alphanumeric characters, spaces ( ), hyphens (-) and underscores (_). Do not use any other characters.

*path* equals the path name for the directory where you want to store the backup file

*server_name* equals the name or IP address of the network server

*username* equals a valid username for an account on the remote system

*number_of_backups* equals the number of backups allowed for this device

**Note** You must have access to an SFTP server to configure a network storage location. The SFTP path must exist prior to the backup. The account that is used to access the SFTP server must have write permission for the selected path.

**Note** The DRS Master Agent validates the selected backup device. If the username, password, server name, or directory path is invalid, the command fails.

**Step 4** To display a list of backup devices, enter **utils disaster_recovery device list**.
The device name, device type, and device path for each backup device displays.

**Step 5** To delete a backup device, enter **utils disaster_recovery device delete** *device_name*,
where *device_name* equals the name of the device that you want to delete.

**Note** You cannot delete a backup device that is configured as the backup device in a backup schedule. You must first delete the schedule which uses this device name, and then delete this device.

# Create backup schedules

You can create up to 10 backup schedules. Each backup schedule has its own set of properties, including a schedule for automatic backups, the set of features to back up, and a storage location.

**Caution** Schedule backups during off-peak hours to avoid call-processing interruptions and impact to service.

To view a history of backups, enter **utils disaster_recovery history Backup**. The results of all backups display.

Perform the following steps to create backup schedules:

### Procedure

**Step 1** To access the Disaster Recovery System, start an SSH session and log in to the CLI on the Cisco PAWS-M platform.
The CLI admin prompt displays.

**Step 2** Enter **utils disaster_recovery schedule add** *schedulename devicename featurelist datetime frequency* where

*schedulename* equals the name of the schedule

*devicename* equals the location where Disaster Recovery System stores the backup files

*featurelist* equals EPM

*datetime* specifies the time and date when Disaster Recovery System performs the backup. The format is yyyy/mm/dd-hh:mm. Enter the time based on a 24-hour clock.

*frequency* equals how often Disaster Recovery System performs the backup. Options are once, daily, weekly, and monthly.

**Step 3** To enable a schedule, enter **utils disaster_recovery schedule enable** *schedulename*.
The next backup occurs automatically at the time that you set.

### Related Topics

Enable, disable, and delete schedules, on page 32

# Enable, disable, and delete schedules

Follow this procedure to enable, disable, or delete backup schedules.

### Procedure

**Step 1** To access the Disaster Recovery System, start an SSH session and log in to the CLI on the Cisco PAWS-M platform.
The CLI admin prompt displays.

**Step 2** To view the list of backup schedules, enter **utils disaster_recovery schedule list**.
The CLI displays the device name and status for each schedule. The device name specifies where Disaster Recovery System stores the backup files.

**Step 3** Perform one of the following steps:

- To enable a schedule, enter **utils disaster_recovery schedule enable** *schedulename*.
- To disable a schedule, enter **utils disaster_recovery schedule disable** *schedulename*.
- To delete a schedule, enter **utils disaster_recovery schedule delete** *schedulename*.

The schedules can be enabled, disabled, or deleted only one at a time.

# Start a manual backup

Follow this procedure to start a manual backup.

### Procedure

**Step 1** To access the Disaster Recovery System, start an SSH session and log in to the CLI on the Cisco PAWS-M platform.
The CLI admin prompt displays.

**Step 2** Enter **utils disaster_recovery backup** *type featurelist device_name*
where

*type* equals the location of the backup, either local or network

*featurelist* equals PAWS-M

*device_name* equals the name of the backup device

**Step 3** To view the status of the current backup, enter **utils disaster_recovery status backup**.

**Step 4** To cancel the current backup, enter **utils disaster_recovery cancel_backup yes**.

# Check backup status

You can check the status of the current backup job and cancel the current backup job. Perform the following steps to check the status of the current backup job.

**Caution** Be aware that if the backup to the remote server is not completed within 20 hours, the backup session times out. You will then need to begin a fresh backup.

**Note** Successful backups display a status of successful. To view a history of backups, enter utils disaster_recovery history Backup. The results of all backups display.

### Procedure

**Step 1** To access the Disaster Recovery System, start an SSH session and log in to the CLI on the Cisco PAWS-M platform.
The CLI admin prompt displays.

**Step 2** To view the status of the current backup, **enter utils disaster_recovery status backup**.

**Step 3** 3To cancel the current backup, enter **utils disaster_recovery cancel_backup yes**.
**Note** The backup cancels after the current component completes its backup operation.

# Display backup files

Using the following procedures, you can see the list of backup files that are stored to the local or network drives.

### Procedure

**Step 1** To access the Disaster Recovery System, start an SSH session and log in to the CLI on the Cisco PAWS-M platform.
The CLI admin prompt displays.

**Step 2** To view backup files, do one of the following:

- To view the list of backup files in the local directory (/common/adminsftp/backup), enter **utils disaster_recovery show_backupfiles device-name**.

- To view the list of backup files on a network drive, enter **utils disaster_recovery show_backupfiles network** *path servername userid*.

where

*path* equals the path name for the directory where the backup file is stored

*servername* equals the name or IP address of the network server

*userid* equals a valid user ID for an account on the remote system

# Restore PAWS Management from a backup file

You can restore the data for Cisco PAWS-M from a backup file in a network directory or in a local directory. Use one of the following procedures to restore the data for Cisco PAWS-M.

**Caution** Before you restore Cisco PAWS-M platform, ensure that the Cisco PAWS-M version that is installed on the platform matches the version of the backup file that you want to restore. The Disaster Recovery System supports only matching versions of Cisco PAWS-M for restore. Essentially, the product version needs to match, end-to-end, for the Disaster Recovery System to run a successful restore. Disaster Recovery System adheres to strict version checking and allows restore only between matching versions of Cisco PAWS-M.

**Caution** After you choose the server to which you want the data restored, any existing data on that server gets overwritten.

### Procedure

**Step 1** Copy the backup file to the Cisco PAWS-M platform by opening an SFTP client, and connecting to the Cisco PAWS-M platform by using the adminsftp user and the administrator password that you set up during installation. To do that, navigate to the backup directory by entering cd backup, and copy the backup file to the /common/adminsftp/restore directory.

**Step 2** Access the Disaster Recovery System by starting an SSH session and logging in to the CLI on the Cisco PAWS-M platform.
The CLI admin prompt displays.

**Step 3** Enter **utils disaster_recovery restore local** *restore_server tarfilename device_name*
where

*restore_server* equals the hostname of the server to be restored

*tarfilename* equals the name of the backup file to be restored without extension; for example, 2008-01-21-18-25-03

*device_name* equals the name of the backup device

**Step 4** Your data gets restored on the server that you chose. To view the status of the restore, enter **utils disaster_recovery status restore**.

**Step 5** Restart the Cisco PAWS-M platform.

# View the restore status

To check the status of the current restore job, perform the following steps:

### Procedure

**Step 1** To access the Disaster Recovery System, start an SSH session and log in to the CLI on the Cisco PAWS-M platform.
The CLI admin prompt displays.

**Step 2** To view information about the current restore job, enter **utils disaster_recovery status restore**. The status shows the restore percentage, log file location, timestamp, feature name, platform name, component name, and component status.

# Error messages

The Disaster Recovery System (DRS) issues alarms for various errors that can occur during a backup or restore procedure. Table 3 provides a list of Cisco DRS alarms.

| Alarm Name | Description | Explanation |
|---|---|---|
| DRFBackupDeviceError | DRF backup process has problems accessing device. | DRS backup process encountered errors while it was accessing device. |
| DRFBackupFailure | Cisco DRF Backup process failed. | DRS backup process encountered errors. |
| DRFBackupInProgress | New backup cannot start while another backup is still running. | DRS cannot start new backup while another backup is still running. |
| DRFInternalProcessFailure | DRF internal process encountered an error. | DRS internal process encountered an error. |
| DRFLA2MAFailure | DRF Local Agent cannot connect to Master Agent. | DRS Local Agent cannot connect to Master Agent. |
| DRFLocalAgentStartFailure | DRF Local Agent does not start. | DRS Local Agent may be down. |

| Alarm Name | Description | Explanation |
|---|---|---|
| DRFLocalDeviceError | DRF has problems accessing local device. | DRS encountered errors while it was accessing local device. |
| DRFMA2LAFailure | DRF Master Agent does not connect to Local Agent. | DRS Master Agent cannot connect to Local Agent. |
| DRFMABackupComponentFailure | DRF cannot back up at least one component. | DRS requested a component to back up its data; however, an error occurred during the backup process, and the component did not get backed up. |
| DRFMABackupNodeDisconnect | The node that is being backed up disconnected from the Master Agent prior to being fully backed up. | While the DRS Master Agent was running a backup operation, the Cisco PAWS-M platform disconnected before the backup operation completed. |
| DRFMARestoreComponentFailure | DRF cannot restore at least one component. | DRS requested a component to restore its data; however, an error occurred during the restore process, and the component did not get restored. |
| DRFMARestoreNodeDisconnect | The node that is being restored disconnected from the Master Agent prior to being fully restored. | While the DRS Master Agent was running a restore operation on the Cisco PAWS-M platform, the platform disconnected before the restore operation completed. |
| DRFMasterAgentStartFailure | DRF Master Agent did not start. | DRS Master Agent may be down. |
| DRFNoRegisteredComponent | No registered components are available, so backup failed. | DRS backup failed because no registered components are available. |
| DRFNoRegisteredFeature | No feature got selected for backup. | No feature got selected for backup. |
| DRFRestoreDeviceError | DRF restore process has problems accessing device. | DRS restore process cannot read from device. |
| DRFRestoreFailure | DRF restore process failed. | DRS restore process encountered errors. |
| DRFSftpFailure | DRF SFTP operation has errors. | Errors exist in DRS SFTP operation. |

| Alarm Name | Description | Explanation |
|---|---|---|
| DRFSecurityViolation | DRF system detected a malicious pattern that can result in a security violation. | The DRF Network Message contains a malicious pattern that can result in a security violation like code injection or directory traversal. DRF Network Message has been blocked. |
| DRFTruststoreMissing | The IPsec trust store is missing on the node. | The IPsec trust store is missing on the node. DRF Local Agent cannot connect to Master Agent. |
| DRFUnknownClient | DRF Master Agent on the platform received a client connection request from an unknown server. The request has been rejected. | The DRF Master Agent on the platform received a client connection request from an unknown server. The request has been rejected. |

CHAPTER 5

# PAWS Management administrative interface basics

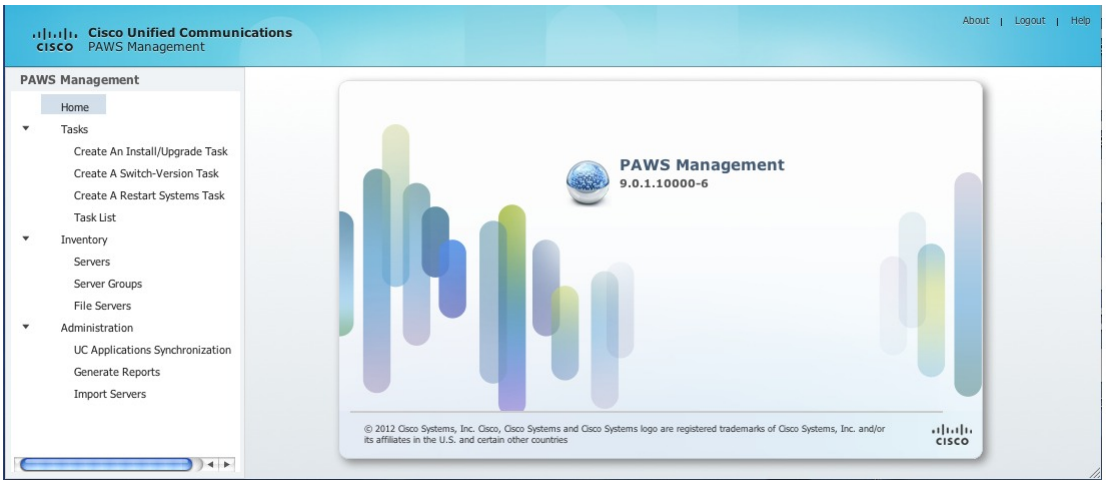

- PAWS Management administrative interface overview, page 39
- Browser support, page 40
- Login and logout, page 42
- Online help, page 42
- Interface version, page 42
- Accessibility, page 43


## PAWS Management administrative interface overview

The PAWS-M administrative interface allows you to start upgrades for Cisco Unified Presence, Cisco Unified Communications Manager, and Cisco Unity Connection. It allows you to configure the server inventory for the system as well as select, schedule, and monitor upgrades of one or more servers across one or more clusters. In the PAWS-M administrative interface, you can also create groups of servers to help manage multiple clients

and applications. From the administrative interface, you can schedule restarts for servers and schedule tasks for switching to the active version (active partition).

***Figure 2: PAWS-M administrative interface***




# Browser support

From any user PC in your network, you can browse into a server that is running the Cisco PAWS-M administrative interface and log in with administrative privileges.

**Tip** The Cisco PAWS-M administrative interface does not support the buttons in your browser. Do not use the browser buttons (for example, the Back button) when you perform configuration tasks.

### Chrome

This table outlines the compatibility of Chrome versions by operating system for Cisco PAWS-M.

***Table 8: Compatibility of Chrome versions by operating system***

| Version | Windows OS - Windows XP | Windows OS - Win 7 (32 and 64 bit) | Apple OS | Linux OS | Google Chrome OS |
|---|---|---|---|---|---|
| Chrome 13 | Supported | Supported | Supported | Not supported | Not supported |
| Chrome 14 | Supported | Supported | Supported | Not supported | Not supported |
| Chrome 15 | Supported | Supported | Supported | Not supported | Not supported |
| Chrome 16 | Supported | Supported | Supported | Not supported | Not supported |

### Firefox

This table outlines the compatibility of Firefox versions by operating system for Cisco PAWS-M.

*Table 9: Compatibility of Firefox versions by operating system*

| Version | Windows OS - Windows XP | Windows OS - Win 7 (32 and 64 bit) | Apple OS | Linux OS | Google Chrome OS |
|---|---|---|---|---|---|
| Firefox 4.0 | Supported | Supported | Supported | Not supported | Not supported |
| Firefox 5.0 | Supported | Supported | Supported | Not supported | Not supported |
| Firefox 6.0 | Supported | Supported | Supported | Not supported | Not supported |
| Firefox 7.0 | Supported | Supported | Supported | Not supported | Not supported |

### Internet Explorer

This table outlines the compatibility of Internet Explorer versions by operating system for Cisco PAWS-M.

*Table 10: Compatibility of Internet Explorer versions by operating system*

| Version | Windows OS - Windows XP | Windows OS - Win 7 (32 and 64 bit) | Apple OS | Linux OS | Google Chrome OS |
|---|---|---|---|---|---|
| IE 8 | Supported | Supported | Not supported | Not supported | Not supported |
| IE 9* | Not supported | Supported | Not supported | Not supported | Not supported |

### Opera

Opera is not supported with Cisco PAWS-M.

### Safari

This table outlines the compatibility of Safari versions by operating system for Cisco PAWS-M.

*Table 11: Compatibility of Internet Explorer versions by operating system*

| Version | Windows OS - Windows XP | Windows OS - Win 7 (32 and 64 bit) | Apple OS | Linux OS | Google Chrome OS |
|---|---|---|---|---|---|
| Safari 5 | Not supported | Not supported | Supported | Not supported | Not supported |
| Safari 5.1 | Not supported | Not supported | Supported | Not supported | Not supported |

# Login and logout

**Note** Simultaneous login by a large number of administrators can cause performance issues with the interface, so try to limit the number of administrators that are logged in simultaneously.

**Note** For security purposes, the Cisco PAWS-M administrative interface logs you out after 30 minutes of inactivity, and you must log back in.

Use this procedure to log in to the Cisco PAWS-M administrative interface:

### Procedure

**Step 1** To log in, start your preferred operating system browser.
In the address bar of the web browser, enter this case-sensitive URL:

https://<name of Cisco PAWS-M platform> where <name of the Cisco PAWS-M platform> equals the name or IP address that you specified for the Cisco PAWS-M platform during installation.

**Step 2** At the main Cisco PAWS-M login page, enter the username and password that you specified during Cisco PAWS-M installation or changed after the installation.

**Step 3** Click **Login**.

a) To log out, click **Logout** in the upper right corner of the Cisco PAWS-M administrative interface. The page displays with the login fields.

# Online help

Each page in the Cisco PAWS-M administrative interface provides online help for the settings on that page. To access the online help for the page, click the **Help** option in the upper right corner of the page.

The online help does not provide all of the information that is available in this guide. Review this guide before you perform configuration tasks in the Cisco PAWS-M administrative interface.

# Interface version

To identify the version of the Cisco PAWS-M administrative interface, click **About** in the upper right corner of the page or click **Home** in the administrative interface. To close the About page, click **x**.

# Accessibility

The Cisco PAWS-M administrative interface provides functionality that allows you to access buttons on the page without using a mouse. You can perform the following procedures from any point on the page, so you do not have to scroll or tab through various fields.

## Access icons

Many of the pages in the Cisco PAWS-M administrative interface include icons that display at the top of the page; for example, an icon for filter or last updated. To access these icons, perform this procedure:

### Procedure

**Step 1** Press **Alt**, press **1**; then, press **Tab**. The cursor will highlight the first icon from the left. To move to the next icon, press **Tab** again.

**Step 2** Press **Enter**. The system performs the function of the icon; for example, Filter.

## Access buttons

Many of the pages in the Cisco PAWS-M administrative interface have buttons that display; for example, a button for Save. To access these buttons, perform this procedure:

### Procedure

**Step 1** Press **Alt**, press **2**, and then press **Tab**. The cursor highlights the first button from the left. To move to the next button, press **Tab** again.

**Step 2** Press **Enter**. The function of the button gets performed; for example, Save.

CHAPTER 6

# PAWS Management configuration


- Configuration checklist for PAWS Management, page 46
- Upgrade and application task management using PAWS Management , page 46
- Limitations and restrictions, page 46
- Best practices, page 47
- Server configuration, page 47
- Add a server, page 47
- Import servers, page 48
- Manage servers, page 48
- Configure server groups , page 49
- Add a server group, page 49
- Manage server groups, page 49
- Configure file servers, page 50
- Add a file server, page 50
- Manage file servers, page 50
- Unified Communications (UC) Applications Synchronization, page 51
- Tasks, page 51
- Create a new install or upgrade task, page 51
- Create a switch version task, page 52
- Create a restart system task, page 53
- Task list, page 53
- Generate reports, page 54

# Configuration checklist for PAWS Management

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | If you have not already done so, install the PAWS-M platform. | Install PAWS-M, on page 14 |
| **Step 2** | If you have not already done so, activate the Platform SOAP Services or Platform Administrative Web Service on any of the Cisco Unified Presence, Cisco Unified Communications Manager, or Cisco Unity Connection servers you want PAWS-M to access. This can be done by CLI or the application interface. For more information on activating this service, review the documentation for the specific application. | Refer to the component documentation for information on how to activate this service. |
| **Step 3** | Configure servers. Select **Inventory > Servers** then select Add Server to populate the server inventory on PAWS-M. | Server configuration, on page 47<br>**Note** You can add servers either by importing them or entering each server individually. For more information see the "Import Servers" section or the "Add a Server" section. |
| **Step 4** | Configure server groups. Add the servers you want into your server inventory before creating server groups. **Select Inventory > Server Groups**, then **Add Server Group** to create server groups. | Configure server groups , on page 49 |
| **Step 5** | Configure file server. Select **Inventory > File Servers**, then **Add File Server**. | Configure file servers, on page 50 |
| **Step 6** | Create tasks. Select the appropriate task you want to create and enter the appropriate details. | Tasks, on page 51 |

# Upgrade and application task management using PAWS Management

# Limitations and restrictions

The following list describes the current limitations for PAWS-M.

- PAWS-M is not a diagnostic tool. An error message does appear on the task list page if a task fails; however, you should use your usual set of tools and procedures to diagnose and correct the problem.
- The SOAP services do not replace the existing OS Administration and CLI upgrade processes. You can still upgrade your servers using the application GUIs, or CLI commands. PAWS-M is just another way to upgrade, restart, or switch versions on the application servers.

# Best practices

The following are recommendations for configuring your systems as suggested by Cisco development and testing teams.

- Use the Add a server, on page 47 or Import servers, on page 48 functionality to populate the servers in your system if possible.
- Use your standard pre- and post- upgrading procedures when performing this action. PAWS-M simplifies this process for you.
- Create groups with multiple servers that you perform similar tasks on.
- Use the sequencing feature in a task when you want a second group of servers to wait until the first group is done before performing that task.

# Server configuration

Use the Server page to add, edit, delete, and manage servers.

**Note** Use the Quick View button to the right of the IP address to see detailed server information.

# Add a server

### Procedure

**Step 1** Click the **Add Server** button.

**Step 2** In the Add Server window complete the following fields:

a) In the Hostname/IP Address field enter a valid hostname or IP address for the server that you want to add.

b) Enter the current OS Admin username defined on the server in the **OS Admin Username** field.

**Note** The username must be no more than 50 characters and begin with an alphanumeric character.

c) Enter the current OS Admin password defined on the server in the **OS Admin Password** field.

**Note** The password must be between 4 and 32 characters.

d) Click **Next**.

e) Enter a description of the customer for the server in the **Customer** field.

f) If a publisher field appears, choose the FQDN of the first node for this server. If your Cisco Unified Communications Manager is version 8.6(2) or higher, this field is be auto-populated.
g) Check the role that will be associated with the server from the **Server Roles** checklist.
**Note** Server roles are labels to help users identify a server. Setting a server role does not activate any services. Mislabeling a server with not cause any service outages.

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

# Import servers

Use the Import Servers feature located in **Administration > Import Servers** to import multiple servers from a .csv file. Each line of an import file defines a single Unified Communications server with six comma separated values: IP address, OS Administrator username, OS Administrator password, Customer name, server roles and FQDN of the first node. For 8.6(2) or higher servers, you do not need to add FQDN of the first node.

## To upload the .csv import file:

### Procedure

**Step 1** SFTP to the Platform Manager server using the adminsftp account and the OS Administration password with any SFTP client.
**Step 2** Change directories to the import directory, and upload the import file.

## To import the servers:

### Procedure

**Step 1** Follow the steps in the Import servers, on page 48 procedure.
**Step 2** Select the import file that you uploaded from the **Import File** drop-down list box.
**Step 3** Check the **Overwrite a server if it already exists** check box if you want to overwrite existing server information that is in the import file.
**Step 4** Click **Start Import**.
**Note** Import files must be uploaded to the /common/adminsftp/import directory using SFTP before they can be imported. An import file will be removed automatically after it has been imported.

# Manage servers

You can perform a variety of actions on the Server page including filter, view, delete, and edit.

Use the Show drop-down or Filter button to filter the server display. You can view content using Quick Filter, Advanced Filter, or All selection from the drop-down list box. The Set Default Filter button defines what the Show menu will be when you load the page.

An Action column appears on the page for each server. The following table lists the options available in this column:

***Table 12: Actions on the Server page***

| Action | Detail |
|---|---|
| Delete | Click **Delete** to delete a single server. Delete multiple servers by checking the check box next to each server that you want to delete and click the **Delete** button. |
| Edit | Click **Edit** to edit a server. |

# Configure server groups

Use the Server Groups page to add, delete, and manage server groups.

# Add a server group

### Procedure

**Step 1** Click the **Add Server Group** button.

**Step 2** In the **Add Server Group** window complete the following fields:

a) In the **Server Group Details** section, enter a name for the group and select a product type from the drop-down list. When you select a product type, only servers with the specified type are available to be added to the group.

b) In the **Add Servers to the Group** section, check the check box next to the available servers that you want to include in the group and click the right arrow to select the servers.

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

# Manage server groups

You can perform a variety of actions on the Server Group page including filter, view, delete, and edit.

Use the Show drop-down or Filter button to filter the server display. You can view content using Quick Filter, Advanced Filter, or All selection from the drop-down list box. The Set Default Filter button defines what the Show menu will be when you load the page.

An Action column appears on the page for each server group. The following table lists the options available in the this column:

| Action | Detail |
|---|---|
| View | Click **View** under the Actions column to view details about a specific server group. |
| Delete | Click **Delete** to delete a single server group. Delete multiple server groups by checking the check box next to each server group that you want to delete and click the **Delete** button. |
| Edit | Click **Edit** to edit a server group. |

# Configure file servers

Use the File Servers page to add, edit, delete, and manage FTP/SFTP file servers.

# Add a file server

To add a file server, complete the following steps.

### Procedure

**Step 1** Click **Add File Server** button.

**Step 2** Enter the following information in the **Add File Server** window:

a) Enter the file server name in the **File Server** field.
   **Note** The file server ID must contain no special characters. It may contain spaces, hyphens and underscores.
b) Enter the hostname or IP address of the new file server in the **Hostname/IP Address** field.
c) Enter the path to the files on the file server in the **Directory** field.
d) Enter the **Username** and **Password** required to access the file server.
e) Select either **SFTP** or **FTP** server type.
   **Note** You can use the **Show Files** button to view all of the files in the specified directory.

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

# Manage file servers

You can perform a variety of actions on the server group page including filter, view, delete, and edit. Use the **Show** drop-down or **Filter** button to filter the server display. You can view content using **Quick Filter**,

**Advanced Filter**, or **All** selection from the drop-down list box. The **Set Default Filter** button defines what the Show menu will be when you load the page.

An Action column appears on the page for each server group. The following table lists the options available in the this column:

***Table 13: Actions on File Servers Page***

| Action | Detail |
|---|---|
| Test | Click **Test** under the actions column to test that this File server can be reached successfully from the PAWS-M server. |
| Delete | Click **Delete** to delete a single file server. Delete multiple file servers by checking the check box next to each file server that you want to delete and click the **Delete** button. |
| Show Files | Click to view all of the files. You can also browse a file server by checking the check box next to the file server in the list display and clicking the **Show** option. |
| Edit | Click **Edit** to edit a file server. |

# Unified Communications (UC) Applications Synchronization

Use the UC Applications Synchronization page to keep Platform Manager up to date with OS changes such as active version and installed options made on the UC applications in the server inventory. Synchronize data for all servers immediately by clicking the **Sync Now** button. To schedule recurring syncs, indicate a start time and frequency and click **Save**. The lower half of the page shows the result of the latest server synchronization.

# Tasks

Tasks are used to upgrade, switch versions, or restart groups of servers. You can create various tasks to perform on server groups. The following sections describes how to create various tasks.

- Create a new install or upgrade task, on page 51
- Create a switch version task, on page 52
- Create a restart system task, on page 53

# Create a new install or upgrade task

Use the Upgrade Install Wizard to create and manage installation and upgrade tasks.

**Note** Server groups containing both publisher and subscriber servers cannot be used for upgrade tasks.

Create a new installation or upgrade task to automatically run on one or more server groups at scheduled times.

### Procedure

**Step 1** Enter a task name and click **Next**.

**Step 2** Select one or more of server groups from the list of available groups in the left pane and click the arrow buttons to move them to the **Selected Server Groups** list.

**Step 3** Click **Next**.

**Step 4** Select a file server from the drop-down list and click the **Show Files** button. **Hostname**, **Directory**, **Type** and **User Name** populate automatically.

**Note** The upgrade wizard only shows files that are valid for every server added to the task.

**Step 5** Click the **Show Files** button to retrieve a list of patches or COP files that can be used to upgrade.

**Step 6** Select the valid file that you want to apply to your server group upgrade and click **Next**.

**Step 7** Check the **Automatically switch to the new version after a successful upgrade** check box if you want to automatically switch to the upgraded partition.

**Step 8** Use the **Sequence the Server Groups** section to set the date, time and sequence for the upgrade tasks to be executed on the servers. Each server group can start at a specific time or after another server group.

**Step 9** Click **Next**.

**Note** If you are performing a refresh upgrade, do not select the **Automatically switch to the new version** option.

**Step 10** Use the **Review and Schedule the Task** section to verify the details of the task you created.

**Step 11** Click **Finish** to schedule the task.
If you are performing a refresh upgrade, do not click the **Reboot** button while the task is running.

# Create a switch version task

Use the Switch Version Task Wizard to create and manage switch version tasks.

Create a switch version task to automatically switch one or more server groups to the upgraded version at scheduled times.

### Procedure

**Step 1** Enter a name for the task in the **Task Name** box and click **Next**.

**Step 2** Select one or more of server groups from the list of available groups in the left pane and click the arrow buttons to move them to the **Selected Server Groups** list.

**Step 3** Click **Next**.

**Step 4** Select the installed version that you want to switch to by selecting the radio button for either **Inactive Version** or **Specific Version**. If you select **Specific Version** you must specify a build number. If the inactive version installed does not match the build number specified, the switch will not occur.

**Step 5** Click **Next**.

**Step 6** Use the **Sequence the Server Groups** section to set the date, time and sequence for the switch version tasks to be executed on the servers. Each server group can start at a specific time or after another server group.

**Step 7** Click **Next**.

**Step 8** Use the **Review and Schedule the Task** section to verify the details of the task you created.

**Step 9** Click **Finish** to schedule the task.

# Create a restart system task

Use the Restart System Task Wizard to create and manage restart system tasks.

Create a restart system task to automatically restart one or more server groups to at scheduled times.

### Procedure

**Step 1** Enter a name for the task in the **Task Name** box and click **Next**.

**Step 2** Select one or more of server groups from the list of available groups in the left pane and click the arrow buttons to move them to the **Selected Server Groups** list.

**Step 3** Click **Next**.

**Step 4** Use the **Sequence the Server Groups** section to set the date, time and sequence for the switch version tasks to be executed on the servers. Each server group can start at a specific time or after another server group.

**Step 5** Click **Next**.

**Step 6** Use the **Review and Schedule the Task** section to verify the details of the task you created.

**Step 7** Click **Finish** to schedule the task.

# Task list

The Tasks window displays a list of tasks created with the following methods:

- Install/Upgrade Task Wizard

- Switch-Version Task Wizard
- Restart System Task Wizard
- Tasks created using clone a task

Under the **Actions** column, you can cancel tasks, view details of a task, view history of a task, delete a task and clone a task. **Cancel** is only available for tasks that have not been run.

Use the **Clone** option to duplicate a task that was previously scheduled or run. Each cloned task starts the appropriate wizard depending on whether it was originally an **Install/Upgrade**, **Switch-Version**, or **Restart** task. Cloned tasks start the task wizard and default to the previously used task data. You can also edit the task data and run the task again. Using a cloned task, you can repeat a task while re-using the task parameters.

Use the **Show** drop-down or Filter button to filter the task display. You can view content using Quick Filter, Advanced Filter or All selection from the drop-down list. The **Set Default Filter** button defines what the show menu will be when you load the page.

# Generate reports

Use the Generate Reports feature to generate reports that detail the current state of the server inventory.

### Procedure

**Step 1** Enter a unique name for your report in the **Report File** field.

**Step 2** Click the Generate Report button. Reports are created on the server in the /common/adminsftp/log directory.

# Download a report

To download a report:

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | SFTP to the Platform Manager server using the **adminsftp** account and the **OS Administration password** with any SFTP client. | |
| **Step 2** | Navigate to the log directory, and download the report. | |

CHAPTER 7

# Command line interface for PAWS Management

This chapter describes the command line interface (CLI) commands that are available for the Cisco PAWS Management platform.


- Start CLI session, page 55
- CLI basics, page 56
- Generic commands, page 58
- Delete commands, page 59
- File commands, page 63
- Set commands, page 77
- Show commands, page 116
- Unset commands, page 164
- Utils commands, page 166


# Start CLI session

You can access the PAWS-M 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 also access the Cisco PAWS-M CLI from the virtual console of the virtual machine it is installed on. Use this method if a problem exists with the IP address.

Perform the following steps to start a CLI session:

### 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.

### Procedure

**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 hostname 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 sections contains basic tips for using the command line interface.

Complete CLI commands, on page 56

Obtain Help for commands, on page 57

End CLI sessions, on page 58

CLI command properties, on page 58

# Complete CLI commands

To complete commands, use **Tab**:

- Enter the start of a command and press **Tab** to complete the command. For example, if you enter **set** and press **Tab**, **set** is 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 asterix (*) 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.

# Obtain Help for commands

You can obtain two types 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

- To get detailed help, at the CLI prompt, enter
  **help** *command*

  Where command specifies the command name or the command and parameter. See the example below.

**Note** If you enter the help command without specifying the name of a particular command as the optional parameter, the system provides information about the CLI system.

**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
```

- To query only command syntax, at the CLI prompt, enter
  *command?*

  Where command represents the command name or the command and parameter. See the example below.

**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.

**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]
```

# End CLI sessions

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.

The following sections list and describe the CLI commands that are available for PAWS-M.

# CLI command properties

### Command Privilege Level

Each CLI command has a "Command Privilege Level" setting. The CLI has privilege levels 0 (lowest) through 4 (highest). Each Level, that is, the collection of commands such as "show," and each command has a privilege associated with it. A user will only be able to execute a command if the account they are using has sufficient privilege. The original Admin account, created during install, has the highest privilege level (4). This is the only account with this privilege level. When other accounts are created in the CLI using the CLI command set account, the account is assigned a privilege level. A new account can only have a privilege level of 0 or 1. Privilege levels 2 and 3 are currently unassigned and reserved for future use.

### Allowed during Upgrade

Each CLI command has an "Allow during upgrade?" setting. This setting controls whether the command can be run while an L2 upgrade is taking place. During an L2 upgrade, an administrator can log into the system and try to execute CLI commands. Since the CLI parser can figure out if an L2 is in progress, it can refuse to run any commands that are not permitted during an upgrade.

# Generic commands

# help

**help** *command*

**Syntax Description**

| Parameters | Description |
|---|---|
| *command* | Specifies the command for which help is required. |

### Requirements

Command privilege level: 0

Allowed during upgrade: Unknown

## quit

**quit**

**Requirements**

Command privilege level: 0

Allowed during upgrade: Unknown

# Delete commands

## delete account

This command allows you to delete an administrator account.

**delete account** *account-name*

**Syntax Description**

| Parameters | Description |
|---|---|
| *account-name* | Specifies the name of an administrator account. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## delete dns

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

**delete dns** *addr*

**Syntax Description**

| Parameters | Description |
|---|---|
| *addr* | Represents the IP address of the DNS server that you want to delete. |

**Command Modes** Administrator (admin:)

**Usage Guidelines** After you execute this command, the system asks whether you want to continue.

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

### Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

# delete dscp

This command deletes a DSCP port tag.

**delete dscp** *port-tag*

**Syntax Description**

| Parameters | Description |
|---|---|
| *port-tag* | Represents a DSCP port tag, which is a string that is mapped to a TCP or UDP port to identify the application that uses the port. This value is for the portTag field displayed when you use the command **show dscp defaults**. The set of port tags is predefined. |

**Command Modes** Administrator (admin:)

**Usage Guidelines** After you delete an enabled port tag, DSCP marking on that port tag stops. You can recreate a deleted port tag when you use the set dscp marking command; enter the name of the port tag that you previously deleted.

**Tip** Use the command **show dscp defaults** to list the configured port tags.

### Requirements

Applies to: Unified CM, Cisco Unity Connection

# delete ipsec policy_group

This command deletes all policies within the specified group or all groups.

**delete ipsec policy_group** {*group*| **all**}

**Syntax Description**

| Parameters | Description |
|---|---|
| *group* | Represents a specific group name. |
| **all** | Deletes all groups. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, Cisco Unity Connection

# delete ipsec policy_name

This command deletes an Ipsec policy with given policy name.

**delete ipsec policy_name** {*policy_name*| **all**}

**Syntax Description**

| Parameters | Description |
|---|---|
| *policy_name* | Represents the policy name. |
| **all** | Deletes policies within all policy names. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, Cisco Unity Connection

# delete process

This command allows you to delete a particular process.

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

**Syntax Description**

| Parameters | Description |
|---|---|
| *process-id* | Represents the process ID number. |
| **force** | Causes the process to stop. |
| **terminate** | Causes the operating system to terminate the process. |
| **crash** | Crashes the process and produces a crash dump. |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

Use the **force** option only if the command alone does not delete the process; use the **terminate** option only if **force** does not delete the process.

### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

# delete smtp

This command allows you to delete the SMTP host.

**delete smtp**

**Command Modes**

Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

# File commands

## file check

This command checks the /usr directory tree to see whether files or directories have been added, removed, or changed in size since the last fresh installation or upgrade and shows the results.

**file check** [ *detection-size-kb* ]

**Syntax Description**

| Parameters | Description |
|---|---|
| *detection-size-kb* | Specifies the minimum file size change that is required for the command to display the file as changed.<br>Default value: 100 KB. |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

The command notifies you about a possible impact to system performance and asks you whether you want to continue. The display includes both deleted and new files.

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

**Requirements**

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## file delete*

### file delete

This command deletes a log on the active or inactive side.

**file delete** {**activelog**| **inactivelog**| **install**} *file-spec* **[detail] [noconfirm]**

**Syntax Description**

| Parameters | Description |
|---|---|
| **activelog** | Specifies a log on the active side. |
| **inactivelog** | Specifies a log on the inactive side. |
| **install** | Specifies an installation log. |
| *file-spec* | Specifies the path and filename of the log or logs to delete. |
| **detail** | Shows a listing of deleted files with the date and time. |
| **noconfirm** | Deletes files without asking you to confirm each deletion. |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

You get prompted for confirmation after you enter the command. You cannot delete directories or files that are in use.

**Caution** You cannot recover a deleted file, but you may be able to with The Disaster Recovery System.

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

### file delete tftp

This command deletes a TFTP file.

**file delete tftp** *file-spec* **[detail] [noconfirm]**

**Syntax Description**

| Parameters | Description |
|---|---|
| *file-spec* | Represents the TFTP file name. |
| **detail** | Shows a listing of deleted files with the date and time. |

| Parameters | Description |
|---|---|
| **noconfirm** | Deletes files without asking you to confirm each deletion. |

**Command Modes** Administrator (admin:)

**Usage Guidelines** You get prompted for confirmation after you enter the command. You cannot delete directories or files that are in use.

**Caution** You cannot recover a deleted file, but you may be able to with The Disaster Recovery System.

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to:Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

### *file delete dir tftp*

This command deletes the TFTP directory.

**file delete dir tftp** *dir-name* **[detail]**

**Syntax Description**

| Parameters | Description |
|---|---|
| *dir-name* | Specifies the TFTP directory to delete. |
| **detail** | Shows a listing of deleted files with the date and time. |

**Command Modes** Administrator (admin:)

**Usage Guidelines** You get prompted for confirmation after you enter the command. You cannot delete directories or files that are in use.

**Caution** You cannot recover a deleted file, but you may be able to with The Disaster Recovery System.

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

# file dump*

## file dump

This command dumps the contents of a log, a page at a time.

**file dump** {**activelog| inactivelog| install**} *file-spec* **[hex] [recent]** [**regexp** *expression*]

**Syntax Description**

| Parameters | Description |
|---|---|
| **activelog** | Specifies a log on the active side. |
| **inactivelog** | Specifies a log on the inactive side. |
| **install** | Specifies an installation log. |
| *file-spec* | Represents the log file to dump. |
| **hex** | Shows output in hexadecimal. |
| **recent** | Dumps the most recently changed file in the directory. |
| **regexp** *expression* | Displays only the lines in the file that match the regular expression *expression*. |

**Command Modes**

Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

### Example

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

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

## file dump sftpdetails

This command specifies the list of files that can be dumped in the SFTP context and allows you to choose which file to dump.

**file dump sftpdetails**

**Command Modes** Administrator (admin:)

**Usage Guidelines** Enter **a** to dump all SFTP-related files. Enter **q** to exit this command.

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, Cisco Unity Connection

## file fragmentation sdi*

### file fragmentation sdi

This command shows file fragmentation information about SDI log files.

**file fragmentation sdi most** {**fragmented**| **recent**} [ *number* ]

**Syntax Description**

| Parameters | Description |
|---|---|
| **most fragmented** | Represents the most fragmented log files. |
| **most recent** | Represents the most recent logs files. |
| *number* | Represents the number of files to list. |

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

*file fragmentation sdi file*

This command shows file fragmentation information about an SDI log file.

**file fragmentation sdi file** *filename* **[verbose]**

**Syntax Description**

| Parameters | Description |
|---|---|
| *filename* | Represents the SDI log file name. |
| **verbose** | Shows more detailed information on the screen. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level:1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

*file fragmentation sdi all*

This command shows file fragmentation information about all SDI log files in the directory.

**file fragmentation sdi all** *filename*

**Syntax Description**

| Parameters | Description |
|---|---|
| *filename* | Specifies the SDI log file name for which you want to show all fragmentation details. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## file fragmentation sdl*

### file fragmentation sdl

This command shows file fragmentation information about the most fragmented SDL log files.

**file fragmentation sdl most** {**fragmented**| **recent**} [ *number* ]

**Syntax Description**

| Parameters | Description |
|---|---|
| **most fragmented** | Represents the most fragmented log files. |
| **most recent** | Represents the most recent log files. |
| *number* | Represents the number of files to list. |

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection.

### *file fragmentation sdl file*

This command displays file fragmentation information about an SDL log file.

**file fragmentation sdl file** *filename* **[verbose]**

**Syntax Description**

| Parameters | Description |
|---|---|
| *filename* | Represents the file name of the SDL log file. |
| **verbose** | Shows more detailed information on the screen. |

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection.

### *file fragmentation sdl all*

This command shows file fragmentation information about all SDL log files in the directory.

**file fragmentation sdl all** *filename*

**Syntax Description**

| Parameters | Description |
|---|---|
| *filename* | Represents the file name for which you want to show all fragmentation details. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection.

## file get*

### file get

This command sends a log to another system by using SFTP.

**file get** {**activelog| inactivelog| install**} *file-spec* [*reltime*| *abstime*] [**match** *regex*] **[recurs] [compress]**

**Syntax Description**

| Parameters | Description |
|---|---|
| **activelog** | Specifies a log on the active side. |
| **inactivelog** | Specifies a log on the inactive side. |
| **install** | Specifies an installation log. |
| *file-spec* | Specifies the name of the file to transfer. |
| *reltime* | The relative time period, specified in minutes \| hours \| days \| weeks \| months \| time value |
| *abstime* | The absolute time period, specified as hh:mm:MM/DD/YY hh:mm:MM/DD/YY |
| **match** *regex* | Match a particular string in the filename, specified as *regex*. |

| Parameters | Description |
|---|---|
| **recurs** | Get all files, including subdirectories. |
| **compress** | Transfer files as compressed file. |

**Command Modes**

Administrator (admin:)

**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

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

**Example**

This example gets all files in the activelog operating system directory that match the string "plat."

```
admin: file get activelog platform match plat
```

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

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

### *file get salog*

This command sends the partBsalog or salog directory to another system by using SFTP.

**file get** {**partBsalog| salog**} *file-spec* [*reltime*| *abstime*] [**match** *regex*] **[recurs] [compress]**

**Syntax Description**

| Parameters | Description |
|---|---|
| **partBsalog** | Specifies the partBsalog directory. |
| **salog** | Specifies the salog directory. |
| *file-spec* | Specifies the name of the file to transfer. |
| *reltime* | The relative time period, specified in minutes \| hours \| days \| weeks \| months \| time value |
| *abstime* | The absolute time period, specified as hh:mm:MM/DD/YY hh:mm:MM/DD/YY |

| Parameters | Description |
|---|---|
| **match** *regex* | Match a particular string in the filename, specified as *regex*. |
| **recurs** | Get all files, including subdirectories. |
| **compress** | Transfer files as compressed file. |

**Command Modes**

Administrator (admin:)

**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

Applies to: Unified CM, Cisco Unity Connection

## file list*

### file list

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

**file list** {**activelog**| **inactivelog**| **install**} *file-spec* [**page**| **detail**| **reverse**] [**date**| **size**]

**Syntax Description**

| Parameters | Description |
|---|---|
| **activelog** | Specifies a log on the active side. |
| **inactivelog** | Specifies a log on the inactive side. |
| **install** | Specifies an installation log. |
| *file-spec* | Specifies the name of the log file . |
| **page** | Shows the output one screen at a time. |
| **detail** | Shows a detailed listing with date and time. |

| Parameters | Description |
|---|---|
| **reverse** | Reverses the sort direction. |
| **date** | Sorts files by date. |
| **size** | Sorts files by size. |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

**Example: Log files with details**

This example lists operating system log files with details.

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

**Example: Directories in the platform/drf directory**

This example shows directories in the platform/drf directory.

```
admin: file list activelog platform/drf
```

**Example: Platform files by size**

This example shows Platform files in a specified directory by size.

```
admin: file list activelog platform/drf size
```

### *file list salog*

This command lists the partBsalog or salog directory.

**file list** {**partBsalog**| **salog**} *file-spec* [**page**| **detail**| **reverse**] [**date**| **size**]

**Syntax Description**

| Parameters | Description |
|---|---|
| **partBsalog** | Specifies the partBsalog log directory. |
| **salog** | Specifies the salog log directory. |
| *file-spec* | Specifies the path to the file or files to list. |

| Parameters | Description |
|---|---|
| **page** | Shows the output one screen at a time. |
| **detail** | Shows a detailed listing with date and time. |
| **reverse** | Reverses the sort direction. |
| **date** | Sorts files by date. |
| **size** | Sorts files by size. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to:Unified CM, Cisco Unity Connection

## file search*

### file search

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

**file search** {**activelog**| **inactivelog**| **install**} *file-spec* [*reltime*| *abstime*] **[ignorecase]**

**Syntax Description**

| Parameters | Description |
|---|---|
| **activelog** | Specifies a log on the active side. |
| **inactivelog** | Specifies a log on the inactive side. |
| **install** | Specifies an installation log. |
| *file-spec* | Specifies the name of the file to search. |
| *reltime* | The relative time period, specified in minutes \| hours \| days \| weeks \| months \| time value |

| Parameters | Description |
|---|---|
| *abstime* | The absolute time period, specified as hh:mm:MM/DD/YY hh:mm:MM/DD/YY |
| **ignorecase** | Ignores case in a search. |

**Command Modes** Administrator (admin:)

**Usage Guidelines** Write the search term in the form of a regular expression, which is a special text string to describe 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

## file tail*

### file tail activelog

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

**file tail** {**activelog**| **inactivelog**| **install**} *filespec* **[hex]** [ *lines* ] [**regexp** *expression*]

**Syntax Description**

| Parameters | Description |
|---|---|
| **activelog** | Specifies a log on the active side. |
| **inactivelog** | Specifies a log on the inactive side. |
| **install** | Specifies an installation log. |
| *filespec* | Specifies the path to the file. You can use the wildcard character, *, for filename as long as it resolves to one file. |
| **hex** | Show the listing in hexadecimal. |
| *lines* | Specifies the number of lines to display. |
| **regexp** *expression* | Tails log files that match *expression* |

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

### Example

This example tails the operating system CLI log file.

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

## file view*

### file view

This command shows the contents of log files.

**file view** {**activelog**| **inactivelog**| **install**} *file-spec*

**Syntax Description**

| Parameters | Description |
|---|---|
| **activelog** | Specifies a log file on the active side. |
| **inactivelog** | Specifies a log file on the inactive side. |
| **install** | Specifies an installation log file. |
| *file-spec* | Specifies the path to the file to view. You can use the wildcard character, *, as long as it resolves to one file. |

**Command Modes** Administrator (admin:)

**Usage Guidelin**

**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

Applies to: Unified CM, Unified CM with IM and Presence, Cisco Unity Connection

#### Example

This example shows a particular CDR log on the active side.

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

*file view system-management-log*

This command shows the contents of the Integrated Management Logs (IML).

**file view system-management-log**

**Command Modes** Administrator (admin:)

**Usage Guidelin**

**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

Applies to: Unified CM, Cisco Unity Connection

# Set commands

## set account*

### set account enable

This command enables the OS user account that was disabled because of password inactivity.

**set account enable** *user-id*

**Syntax Description**

| Parameters | Description |
|---|---|
| *user-id* | Specifies the user ID of the account that was disabled. |

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

### set account name

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

**set account name** *name*

**Syntax Description**

| Parameters | Description |
|---|---|
| *name* | Represents the username for the new account. |

**Command Modes** Administrator (admin:)

**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

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## set accountlocking*

### set accountlocking

This command enables or disables account locking for the current administration accounts.

**set accountlocking** {**enable**| **disable**}

**Syntax Description**

| Parameters | Description |
|---|---|
| **enable** | Enable account locking. |

| Parameters | Description |
|---|---|
| **disable** | Disable account locking. |

**Command Modes** Administrator (admin:)

**Usage Guidelin**

**Note** After you run this command with **enable**, the system automatically enables account lockout notification after the system enables the audit logging function.

**Requirements**

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## set accountlocking count

This command sets the global consecutive failed sign-in attempt count that triggers locking a user account.

**set accountlocking count** *attempts*

**Syntax Description**

| Parameters | Description |
|---|---|
| *attempts* | Represents the number of consecutive sign-in attempts before the system locks the account.<br>Value Range: 2-5<br>Default value: 3 |

**Command Modes** Administrator (admin:)

**Usage Guidelines** To change the global value for consecutive failed sign-in attempts before the system locks a user account, execute this command.

**Note** This command is only valid when account locking is enabled. If account locking is disabled, the system does not remember the account locking value and uses the default value, 3, after you enable account locking.

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

### set accountlocking unlocktime

This command configures the unlock time for the current Unified CM admin accounts

**set accountlocking unlocktime** *seconds*

**Syntax Description**

| Parameters | Description |
|---|---|
| *seconds* | Specifies the unlock time in seconds.<br>Valid values: greater than 300 seconds, but less than 3600 seconds (60 minutes). |

**Command Modes**

Administrator (admin:)

**Requirements**

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## set cli*

### set cli pagination

For the current CLI session, this command turns automatic pagination On or Off.

**set cli pagination** {**on**| **off**}

**Syntax Description**

| Parameters | Description |
|---|---|
| **on** | Turns pagination on. |
| **off** | Turns pagination off. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

```
admin:set cli pagination off
Automatic pagination is turned off
```

## set cli session timeout

This command sets the time, in minutes, after which an active CLI session times out and disconnects.

**set cli session timeout** *minutes*

**Syntax Description**

| Parameters | Description |
|---|---|
| *minutes* | Specifies the time, in minutes, that can elapse before an active CLI session times out and disconnects.<br>• Value range: 5-99999 minutes<br>• Default value: 30 minutes |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

Be aware that the new session timeout value becomes effective immediately for a new CLI session; however, active sessions retain their original timeout value. Also the show cli session timeout command reflects the new value, even if the current session does not use that value.

**Note** This setting gets preserved through a software upgrade and does not get reset to the default value.

### Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

# set commandcount

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

**set commandcount** {**enable**| **disable**}

**Syntax Description**

| Parameters | Description |
|---|---|
| **enable** | Turns on command count. |
| **disable** | Turns off command count. |

**Command Modes**

Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

# set csr gen

This command regenerates the certificate for the specified unit.

**set csr gen** *name*

**Syntax Description**

| Parameters | Description |
|---|---|
| *name* | Specifies the unit on which the certificate is generated. |

**Command Modes**

Administrator (admin:)

### Requirements

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

### Example

```
admin:set csr gen tomcat
Successfully regenerated certificate for tomcat.
Please restart services related to tomcat for the new certificate to become active.
```

# set date

This command changes the time and date on the server.

**set date** *HH:mm:ss:MM/DD/YY*

**Syntax Description**

| Parameters | Description |
|---|---|
| *HH:mm:ss* | Represents the time format (24 hours format). |
| *MM/DD/YY* | Represents the date format.<br>**Note** Date format MM/DD/YYYY is also accepted. |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

If the server is configured to synchronize with external NTP servers, this command requires the user to remove all of those NTP servers.

**Requirements**

Applies to: Unified CM and Cisco Unity Connection.

**Set date and time to 2:10:33 pm April 13th 2012 example**

```
admin:set date 14:10:33:04/13/12
```

# set dscp*

## set dscp defaults

This command sets the factory default DSCP settings for all of the port tags.

**set dscp defaults**

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

All non-default DSCP settings get removed after you run this command.

You can use the command show dscp defaults to see the factory default DSCP settings.

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

## set dscp

This command enables or disables DSCP marking on outgoing TCP or UDP packets. You can enable or disable DSCP on a single port tag, or on all port tags at once.

**set dscp** {**enable**| **disable**}{**all**| *port_tag*}

**Syntax Description**

| Parameters | Description |
|---|---|
| **all** | Disables all DSCP port tags. |
| *port_tag* | Represents a DSCP port tag, which is a string that is mapped to a TCP or UDP port to identify the application that uses the port. This value is for the portTag field displayed when you use the command **show dscp defaults**. The set of port tags is predefined. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

## set dscp marking

This command sets DSCP markings on port tags by using well-known DSCP classes and numeric values.

**set dscp marking** *port_tag value*

**Syntax Description**

| Parameters | Description |
|---|---|
| *port_tag* | Represents a DSCP port tag, which is a string that is mapped to a TCP or UDP port to identify the application that uses the port. This value is for the portTag field displayed when you use the command **show dscp defaults**. The set of port tags is predefined. |
| *value* | A DSCP value. You can enter the name of a well-known DSCP class or a numeric value in decimal or hexadecimal format. Precede hexadecimal values with 0x or 0X. |

**Command Modes**

Administrator (admin:)

**Usage Guidelines** The valid class names as defined by DSCP are:

- Class Selector: values CS0, CS1, CS2, CS3, CS5, CS6, CS7

  The class selector (CS) values correspond to IP Precedence values and are fully compatible with IP Precedence.

- Expedited Forwarding: value EF

  EF PHB is ideally suited for applications such as VoIP that require low bandwidth, guaranteed bandwidth, low delay, and low jitter.

- Best Effort: value BE

  Also called default PHB, this value essentially specifies that a packet be marked with 0x00, which gets the traditional best-effort service from the network router.

- Assured Forwarding: values AF11, AF12, AF13, AF21, AF22, AF23, AF41, AF42, AF43

  There are four types of Assured Forwarding classes, each of which has three drop precedence values. These precedence values define the order in which a packet is dropped (if needed) due to network congestion. For example, packets in AF13 class are dropped before packets in the AF12 class.

### Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

# set ipsec*

## set ipsec policy_group

This command enables ipsec policies with the specified policy group name.

**set ipsec policy_group** {**ALL**| *group*}

**Syntax Description**

| Parameters | Description |
|---|---|
| **ALL** | Enables all ipsec policy groups. |
| *group* | Specifies the name of a particular ipsec policy group to enable. |

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM and Cisco Unity Connection.

## set ipsec policy_name

This command enables the specified ipsec policy.

**set ipsec policy_name** {**ALL**| *policy_name*}

**Syntax Description**

| Parameters | Description |
|---|---|
| **ALL** | Enables all ipsec policies. |
| *policy_name* | Specifies the name of a particular ipsec policy to enable. |

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM and Cisco Unity Connection.

# set logging

This command allows you to enable or disable CLI Admin logs.

**set logging** {**enable| disable**}

**Syntax Description**

| Parameters | Description |
|---|---|
| **enable** | Turns on logging. |
| **disable** | Turns off logging. |

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

# set network*

## set network cluster publisher

This command sets the network cluster publisher hostname and IP address.

**set network cluster publisher** {**hostname| ip**} *name*

**Syntax Description**

| Parameters | Description |
|---|---|
| **hostname** | Specifies the hostname of the network cluster. |
| **ip** | Specifies the ip address of the network cluster. |
| *name* | Hostname or IP address to assign to the network cluster publisher. |

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

## set network dhcp eth0

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

**set network dhcp eth0** {**enable| disable** } {*node_ip*| *net_mask*| *gateway_ip* }

**Syntax Description**

| Parameters | Description |
|---|---|
| **eth0** | Specifies Ethernet interface 0. |

| Parameters | Description |
|---|---|
| **enable** | This enables DHCP. |
| **disable** | This disables DHCP. |
| **disable** | This disables DHCP. |
| *node_ip* | Represents the static IP address for the server. |
| *net_mask* | Represents the subnet mask for the server. |
| *gateway_ip* | Represents the IP address of the default gateway. |

**Command Modes** Administrator (admin:)

**Usage Guidelin**

**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

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

## set network dns

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

**set network dns** {**primary**| **secondary**} *addr*

**Syntax Description**

| Parameters | Description |
|---|---|
| **primary** | |
| **secondary** | |
| *addr* | Represents the IP address of the primary or secondary DNS server. |

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

## set network dns options

This command sets DNS options.

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

### Syntax Description

| Parameters | Description |
|---|---|
| **timeout** | Sets the DNS timeout. |
| **attempts** | Sets the number of times to attempt a DNS request. |
| **rotate** | Causes the system to rotate among the configured DNS servers and distribute the load. |
| *seconds* | Specifies the DNS timeout period in seconds. |
| *number* | Specifies the number of attempts. |

### Command Modes

Administrator (admin:)

### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

## set network domain

This command sets the domain name for the system.

**Note** Changing the domain name triggers an automatic regeneration of all Cisco Unified Communications Manager certificates, including any third party signed certificates that have been uploaded. After the server reboots automatically, phones running in secure (mixed) mode cannot connect to the server until after the CTL client updates the new CTL file to the phones.

**set network domain** [ *domain-name* ]

**Syntax Description**

| Parameters | Description |
|---|---|
| *domain_name* | Represents the system domain that you want to assign. |

**Command Modes**

Administrator (admin:)

**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.

If you use the **set network domain** *domain-name* command to change the domain name, you must manually regenerate all of your security certificates in Cisco Unified Operating System Administration. The list of certificates depends on your software release but may include cup.pem, cup-xmpp.pem, cup-xmpp-s2s.pem, tomcat, ipsec and so on. Note that you must restart the tomcat service after the tomcat cert is regenerated and you can only restart this service using the CLI. For more information about regenerating security certificates, see the *Cisco Unified Communications Operating System Administration Guide* (on Cisco.com).

After you regenerate your security certificates, you must reboot all the servers in the cluster. This will ensure that database replication keeps working correctly. After the servers have rebooted, confirm that there are no issues reported on the Cisco Unified Reporting report for Database Replication. After you reboot the server, we recommend that you manually delete old certificates that have become disassociated by the domain name change. For every ICSA peer that exists on the local node, you must either update the ICSA entry for the peer node with the new FQDN hostname, or delete that entry and add a new ICSA peer entry with the new FQDN hostname.

#### Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

## set network failover

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

**set network failover** {**ena**| **dis**}

**Syntax Description**

| Parameters | Description |
|---|---|
| **ena** | Enables Network Fault Tolerance. |
| **dis** | Disables Network Fault Tolerance. |

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

## set network gateway

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

**set network gateway** *addr*

**Syntax Description**

| Parameters | Description |
|---|---|
| *addr* | Represents the IP address of the network gateway that you want to assign. |

**Command Modes** Administrator (admin:)

**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

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

## set network hostname

This commands sets the network host name and then causes a restart of the system.

**set network hostname** *hostname*

**Syntax Description**

| Parameters | Description |
|---|---|
| *hostname* | Represents the new network hostname of the system.<br>**Note** The host name must follow the rules for ARPANET host names. It must start with an alphabetic character, end with an alphanumeric character, and consist of alphanumeric characters and hyphens. The host name can have a maximum length of 63 characters. |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

For information about renaming the host name of a Cisco Unity Connection server, see topics related to renaming Cisco Unity Connection servers in the *Reconfiguration and Upgrade Guide for Cisco Unity Connection* at http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html.

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

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

### Example

```
admin:set network hostname myname
W A R N I N G
This will cause the system to restart - Do you want to continue ?
Enter "yes" to continue and restart or any other key to abort
yes
executing...
Broadcast message from root (Thu Jun 21 13:00:21 2012):
The system is going down for restart NOW!
```

## set network ip eth0

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

**set network ip eth0** *addr mask gw*

**Syntax Description**

| Parameters | Description |
|---|---|
| **eth0** | Specifies Ethernet interface 0. |

| Parameters | Description |
|---|---|
| *addr* | Represents the IP address that you want to assign. |
| *mask* | Represents the IP mask that you want to assign. |
| *gw* | Represents the IP default gw that you want to assign. |

**Command Modes**

Administrator (admin:)

**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

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

## set network ipv6 dhcp

This command sets the DHCPv6 client on the server and enables IPv6 support. For changes to take effect, you must restart the server.

**set network ipv6 dhcp** {**enable**| **disable**} **[reboot]**

**Syntax Description**

| Parameters | Description |
|---|---|
| **dhcp** | Sets the DHCPv6 client on the server. By default, the server does not restart after you enable the DHCPv6 client. For your changes to take effect, you must restart the server by either entering the reboot parameter or manually restarting the server. |
| **enable** | Enables IPv6 support. |
| **disable** | Disables IPv6 support. |
| **reboot** | (Optional) Causes the server to automatically restart after you enter the command. |

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM and Cisco Unity Connection.

**Note** IPv6 is not supported in Cisco Unified Communications Manager Business Edition 5000.

## set network ipv6 gateway

This command sets the IPv6 gateway for the server. For changes to take effect, you must restart the server.

**set network ipv6 gateway** *addr* **[reboot]**

**Syntax Description**

| Parameters | Description |
|---|---|
| **gateway** | Sets the IPv6 gateway for the server. By default, the server does not restart after you set the IPv6 gateway for the server. For your changes to take effect, you must restart the server by either entering the reboot parameter or manually restarting the server. |
| *addr* | The IPv6 gateway address. |
| **reboot** | (Optional) Causes the server to automatically restart after you enter the command. |

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM and Cisco Unity Connection.

**Note** IPv6 is not supported in Cisco Unified Communications Manager Business Edition 5000.

## set network ipv6 service

This command enables or disables the IPv6 service on the server. For changes to take effect, you must restart the server.

**set network ipv6 service** {**enable**| **disable**} **[reboot]**

**Syntax Description**

| Parameters | Description |
|---|---|
| **service** | Sets the IPv6 service on the server. By default, the server does not restart after you enable or disable the IPv6 service on the server. For your changes to take effect, you must restart the server by either entering the reboot parameter or manually restarting the server. |
| *enable* | Enables IPv6 service on the server. |
| *disable* | Disables IPv6 service on the server. |
| **reboot** | (Optional) Causes the server to automatically restart after you enter the command. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM and Cisco Unity Connection.

**Note** IPv6 is not supported in Cisco Unified Communications Manager Business Edition 5000.

## set network ipv6 static_address

This command assigns the static IPv6 address to the server. For changes to take effect, you must restart the server.

**Note** IPv6 is not supported in Cisco Unified Communications Manager Business Edition 5000.

**set network ipv6 static_address** *addr mask* **[reboot]**

**Syntax Description**

| Parameters | Description |
|---|---|
| **static_address** | Assigns a static IPv6 address to the server. By default, the server does not restart after you assign the static IPv6 address. For your changes to take effect, you must restart the server by either entering the reboot parameter or manually restarting the server. |
| *addr* | Specifies the static IPv6 address you assign to the server. |
| *mask* | Specifies the IPv6 network mask (0-128). |
| **reboot** | (Optional) Causes the server to automatically restart after you enter the command. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM and Cisco Unity Connection.

## set network max_ip_conntrack

This command sets the ip_conntrack_max value.

**set network max_ip_conntrack** *ip_conntrack_max value*

**Syntax Description**

| Parameters | Description |
|---|---|
| *ip_conntrack_max value* | Specifies the value for ip_conntrack_max.<br>**Note** The value of ip_conntrack_max cannot be less than 65536. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

### Example

```
admin:set network max_ip_conntrack 65536
```

## set network mtu

This command sets the maximum MTU value.

**set network mtu** *mtu_max*

**Syntax Description**

| Parameters | Description |
|---|---|
| *mtu_max* | Specifies the maximum MTU value. The system default MTU value equals 1500. |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

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

**Caution** If you continue, the system loses network connectivity temporarily.

### Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

### Example

```
admin:set network mtu 576      W A R N I N G
This will cause the system to temporarily lose network connectivity
     Do you want to continue ?
Enter "yes" to continue or any other key to abort
yes
executing...
```

## set network nic eth0

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

**set network nic eth0** {**auto** | {**en**| **dis**}} {**speed**| {**10**| **100**}} {**duplex half**| {**half**| **full**}}

**Syntax Description**

| Parameters | Description |
|---|---|
| **eth0** | Specifies Ethernet interface 0. |

| Parameters | Description |
|---|---|
| **auto** | Specifies whether auto negotiation gets enabled or disabled. |
| **speed** | Specifies whether the speed of the Ethernet connection: 10 or 100 Mb/s. |
| **duplex** | Specifies half-duplex or full-duplex. |

**Command Modes** Administrator (admin:)

**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

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

## set network pmtud

This command enables and disables Path MTU Discovery.

**set network pmtud** {**enable**| **disable**}

**Syntax Description**

| Parameters | Description |
|---|---|
| **enable** | Enables Path MTU Discovery. |
| **disable** | Disables Path MTU Discovery. |

**Command Modes** Administrator (admin:)

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

**Caution** If you continue, the system loses network connectivity temporarily.

### Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

### Example

```
admin:set network pmtud enable      W A R N I N G
This will cause the system to temporarily lose network connectivity
     Do you want to continue ?
Enter "yes" to continue or any other key to abort
yes
executing...
```

## set network restore

This command configures the specified Ethernet port to use a specified static IP address.

**set network restore eth0** *ip-address network-mask gateway*

**Syntax Description**

| Parameters | Description |
|---|---|
| **eth0** | Specifies Ethernet interface 0. |
| *ip-address* | Represents the IP address of the primary or secondary DNS server, or the network gateway that you want to assign. If you continue, this command causes a temporary loss of network connectivity. If you change the IP address for the primary DNS server, you must also restart the Cisco Tomcat service. For more information, see the **utils service** command. We also recommend that you restart all nodes whenever any IP address gets changed. |
| *network-mask* | Represents the subnet mask for the server. |
| *gateway* | Specifies the IP address of the default gateway. |
| *ip-address* | Represents the IP address of the primary or secondary DNS server, or the network gateway that you want to assign. If you continue, this command causes a temporary loss of network connectivity. If you change the IP address for the primary DNS server, you must also restart the Cisco Tomcat service. For more information, see the **utils service** command. We also recommend that you restart all nodes whenever any IP address gets changed. |

| Parameters | Description |
|---|---|
| *ip-address* | Represents the IP address of the primary or secondary DNS server, or the network gateway that you want to assign. If you continue, this command causes a temporary loss of network connectivity. If you change the IP address for the primary DNS server, you must also restart the Cisco Tomcat service. For more information, see the **utils service** command. We also recommend that you restart all nodes whenever any IP address gets changed. |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

**Caution** Only use this command option if you cannot restore network connectivity through any other set network commands. This command deletes all previous network settings for the specified network interface, including Network Fault Tolerance. After you run this command, you must restore your previous network configuration manually.

**Caution** The server temporarily loses network connectivity after you run this command.

#### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

#### Example

```
admin:set network restore eth0   10.94.150.108   255.255.255.0   10.94.150.1
```

## set network status eth0

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

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

**Syntax Description**

| Parameters | Description |
|---|---|
| **eth0** | Specifies Ethernet interface 0. |
| **up** | Sets the status of Ethernet interface 0 to up. |
| **down** | Sets the status of Ethernet interface 0 to down. |

**Command Modes** Administrator (admin:)

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

**Caution** If you continue, the system loses network connectivity temporarily.

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

# set password*

## set password age

This command modifies the value for password age, in days, for Cisco Unified Communications Operating System accounts.

**set password age** {**maximum**| **minimum**} *days*

**Syntax Description**

| Parameters | Description |
|---|---|
| **maximum** | Specifies the maximum age. |
| **minimum** | Specifies the minimum age. |
| *days* | Specifies the maximum password age and must be greater-than or equal-to 90 days. |

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

## set password change-at-login

Use this command to force new or existing users to change their password when they sign in to the system the next time.

**set password change-at-login** {**disable| enable**} *userid*

**Syntax Description**

| Parameters | Description |
|---|---|
| **disable** | This does not force users to change their password. |
| **enable** | This forces users to change their password when they sign in to the system the next time. |
| *userid* | Specifies the affected user account. |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

By default, this command is enabled for new users, so users have to change their password the first time they sign in to the system.

### Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: IM and Presence service on Unified CM only.

## set password complexity character

Use this command to enable or disable password complexity rules for the type of characters in a password.

**Note** After you enable password complexity, this command also enables password history if it has not already been enabled (for more information, see the **set password history** command). If you had not previously enabled password history, the password history number parameter value gets set to 10. If you previously enabled password history with a value of less than 10, the value gets reset to 10 after you execute this command. If you previously enabled password history with a value of 10 or greater, the value remains unchanged after you execute this command.

**set password complexity character** {**disable| enable**} *num-char*

**Syntax Description**

| Parameters | Description |
|---|---|
| **disable** | This turns off password complexity for character types. |
| **enable** | This turns on password complexity for character types.<br>**Note** When you disable password complexity, you also turn off **password character difference**, **password character max-repeat**, and **password history**. |
| *num-char* | This specifies the number of characters required from each of the four character sets: lowercase, uppercase, numbers, and special characters.<br>• Value range: 0-8<br>• Default value: 1 |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

When you enable password complexity, you must follow these guidelines when you assign a password:

- It must have at least the current setting, num-chars, of lower-case character.
- It must have at least the current setting, num-chars, of uppercase characters.
- It must have at least the current setting, num-chars, of digit characters.
- It must have at least the current setting, num-chars, of special characters.
- You cannot use adjacent characters on the keyboard; for example, qwerty.
- You cannot reuse any of the previous passwords that match the passwords retained by password history.
- By default, the admin user password can be changed only once in a 24-hour day.

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

**Related Topics**

REUSE COMMAND

## set password complexity character difference

This command specifies the number of characters that the character sequence in a new password must differ from the character sequence in the old password.

**set password complexity character difference** *num-char*

**Syntax Description**

| Parameters | Description |
|---|---|
| *num-char* | This specifies the number of characters that the character sequence in a new password must differ from the character sequence in the old password.<br>• Value range: 0-31 |

**Command Modes** Administrator (admin:)

**Usage Guidelines** Enter 0 to indicate no difference.

**Note** The maximum password length is 31 characters.

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

## set password complexity character max-repeat

This command specifies the number of times you can consecutively repeat a single character in a new password.

**set password complexity character max-repeat** *max-repeat*

**Syntax Description**

| Parameters | Description |
|---|---|
| *max-repeat* | This specifies the number of times you can consecutively repeat a single character in a new password.<br>• Value range: 0 – 10<br>Default value: 0 |

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

## set password expiry maximum-age

This command enables or disables the password expiry maximum age settings for Cisco Unified Operating System Administrator accounts.

**set password expiry maximum-age** {**enable**| **disable**}

### Syntax Description

| Parameters | Description |
|---|---|
| **enable** | Turns on password expiry maximum age settings for Cisco Unified Operating System administrator accounts. The set password expiry enable command sets the value of **maximum password age** to 3650 days (10 yrs) for Cisco Unified Operating System Administrator accounts. |
| **disable** | Turns off password expiry maximum age settings for Cisco Unified Operating System administrator accounts. The set password expiry disable command results in Cisco Unified Operating System Administrator accounts never expiring. |

### Command Modes

Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

### Example

```
admin:set password expiry maximum-age disable
Operation Successful.
```

## set password expiry minimum-age

This command enables or disables the password expiry minimum age settings for Cisco Unified Operating System Administrator accounts.

**set password expiry minimum-age** {**enable| disable**}

**Syntax Description**

| Parameters | Description |
|---|---|
| **enable** | Turns on password expiry minimum age settings for Cisco Unified Operating System administrator accounts. The set password expiry enable command sets the value of minimum password age to one day (24 hrs) for Cisco Unified Operating System Administrator accounts. |
| **disable** | Turns off password expiry minimum age settings for Cisco Unified Operating System administrator accounts. This means that passwords for administrator accounts can be changed at any interval. |

**Command Modes**

Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

### Example

```
admin:set password expiry minimum-age disable
Operation Successful.
```

## set password expiry user maximum-age

This command disables the maximum age password expiry for a particular Cisco Unified Operating System Administrator account.

**set password expiry user maximum-age** {**enable| disable**}*userid*

**Syntax Description**

| Parameters | Description |
|---|---|
| **enable** | Turns on the maximum age password expiry settings for a particular Cisco Unified Operating System administrator account. The set password expiry user enable command sets the value of maximum password age to 3650 days (10 yrs) for the Cisco Unified Operating System Administrator account. |
| **disable** | Turns off the maximum age password expiry settings for a particular Cisco Unified Operating System administrator account. The set password expiry user disable command results in that Cisco Unified Operating System Administrator account never expiring. |
| *userid* | Specifies a particular Cisco Unified Operating System Administrator account. |

**Command Modes**

Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

### Example

```
admin:set password expiry user maximum-age enable
Operation Successful.
```

## set password expiry user minimum-age

This command enables or disables the maximum age password expiry for a particular Cisco Unified Operating System Administrator account.

**set password expiry user minimum-age** {**enable**| **disable**} *userid*

**Syntax Description**

| Parameters | Description |
|---|---|
| **enable** | Turns on the minimum age password expiry settings for a particular Cisco Unified Operating System administrator account. |
| **disable** | Turns off the minimum age password expiry settings for a particular Cisco Unified Operating System administrator account. |

| Parameters | Description |
|---|---|
| *userid* | Specifies a particular Cisco Unified Operating System Administrator account. |

**Command Modes**

Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

### Example

```
admin:set password expiry user minimum-age disable
Operation Successful.
```

## set password history

This command modifies the number of passwords that get maintained in the history for OS admin accounts. New passwords matching remembered passwords get rejected.

**set password history** *number*

**Syntax Description**

| Parameters | Description |
|---|---|
| *number* | Specifies the mandatory number of passwords to maintain in history. |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

- To disable, enter 0.
- Default specifies 10.
- Upper limit specifies 20.

### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

## set password inactivity

**set password inactivity** {**enable| disable| period**} *days*

**Syntax Description**

| Parameters | Description |
|---|---|
| **enable** | Enable the password inactivity globally and update individual OS users according to the setting. |
| **disable** | Disable the password inactivity globally and update individual OS users according to the setting. |
| **period** | Configure the password inactivity period globally and update individual OS users according to the setting. |
| *days* | Specify the number of days of inactivity after a password has expired before the account gets disabled. Valid range is 1 - 99. |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

- To enable password inactivity globally, execute the set password inactivity enable command. This command enables the password inactivity globally and updates individual OS users according to the setting.
- To disable password inactivity globally, execute the set password inactivity disable command. This command disables the password inactivity globally and updates individual OS users according to the setting.

  A user whose account is disabled must contact the system administrator to use the system again.
- To configure the password inactivity period execute the set password inactivity period days command. This command configures the password inactivity globally and updates individual OS users according to the setting.

### Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

## set password user admin

This command allows you to change the administrator password.

**set password user admin**

**Command Modes** Administrator (admin:)

**Usage Guidelines** The systems prompts you for the old and new passwords.

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

#### Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

## set password user security

This command allows you to change the security password.

**set password user security**

**Command Modes** Administrator (admin:)

**Usage Guidelines** The systems prompts you for the old and new passwords.

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

Servers in a cluster use the security password to authenticate communication between servers. You must reset the cluster after you change the security password.

1. Change the security password on the publisher server (first node) and then reboot the server (node).
2. Change the security password on all the subsequent servers and nodes to the same password that you created on the first node and restart subsequent nodes, including application servers, to propagate the password change.

**Note** Cisco recommends that you restart each server after the password is changed on that server.

**Note** Failure to reboot the servers (nodes) causes system service problems and problems with the Cisco Unified Communications Manager Administration windows on the subscriber servers.

### Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

# set session maxlimit

This command sets the upper limit for concurrent sessions.

**set session maxlimit** [ *value* ]

### Syntax Description

| Parameters | Description |
|---|---|
| **maxlimit** | This command sets the upper limit for concurrent sessions. Acceptable values are 1 - 100.<br>If no upper limit is entered, the default value of 10 is assigned to sshd_config param. |
| *value* | Acceptable values are 1 - 100. |

### Command Modes

Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

# set smtp

This command sets the SMTP server hostname.

**set smtp** *hostname*

### Syntax Description

| Parameters | Description |
|---|---|
| *hostname* | Represents the SMTP server name. |

### Command Modes

Administrator (admin:)

### Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

# set timezone

This command lets you change the system time zone.

**set timezone** *zone*

**Syntax Description**

| Parameters | Description |
|---|---|
| *zone* | Specifies the new timezone. Enter the appropriate string or zone index id to uniquely identify the timezone. To view a list of valid time zones, use the CLI command: **show timezone list**. |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

Enter characters to uniquely identify the new time zone. Be aware that the timezone name is case-sensitive.

**Caution** You must restart the system after you change the timezone.

### Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

### Example setting time zone to Pacific time

```
admin:set timezone Pac
```

# set trace*

## set trace disable

This command unsets trace activity for the specified task.

**set trace disable** *tname*

**Syntax Description**

| Parameters | Description |
|---|---|
| **disable** | Unsets the task trace settings. |
| *tname* | Represents the task for which you want to disable traces. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

## set trace enable

This command sets trace activity for the specified task.

**set trace enable** {**Arbitrary| Detailed| Entry_exit| Error| Significant| Special| State_Transition**} *tname*

**Syntax Description**

| Parameters | Description |
|---|---|
| **Arbitrary** | Sets task trace settings to the arbitrary level. |
| **Detailed** | Sets task trace settings to the detailed level. |
| **Entry_exit** | Sets task trace settings to the entry_exit level. |
| **Error** | Sets task trace settings to the error level. |
| **Significant** | Sets task trace settings to the significant level. |
| **Special** | Sets task trace settings to the special level. |
| **State_transition** | Sets task trace settings to the state transition level. |
| *tname* | Represents the task for which you want to disable traces. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

# set web-security

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

**set web-security** *orgunit orgname locality state* [ *alternatehostname* ] [ *alternatehostname* ]

## Syntax Description

| Parameters | Description |
|---|---|
| *orgunit* | Represents the organizational unit (OU) name.<br>You can use this command to enter multiple organizational units. To enter more than one organizational unit name, separate the entries with a comma. For entries that already contain a comma, enter a backslash before the comma that is included as part of the entry. To enter multiple values for organizational unit, enclose them in quotation marks, as shown in the example for this command. |
| *orgname* | Represents the organizational name. |
| *locality* | Represents the organization location. |
| *state* | Represents the organization state. |
| *country* | (Optional) Represents the organization country. |
| *alternatehostname* | (Optional) Specifies an alternate name for the host when you generate a web-server (Tomcat) certificate.<br>When you set an alternate-host-name parameter with the set web-security command, self-signed certificates for tomcat contain the Subject Alternate Name extension with the alternate-host-name specified. CSR for Cisco Unified Communications Manager contains Subject Alternate Name Extension with the alternate host name included in the CSR. |

## Command Modes

Administrator (admin:)

### Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

### Example

This example shows the web-security command with multiple organizational unit names using comma separators. The certificate has three OU fields:

- OU=accounting
- OU=personnel, CA
- OU=personnel, MA

```
admin:set web-security "accounting,personnel\,CA,personnel\,MA" Cisco Milpitas
CA
```

# set webapp session timeout

This command sets the time, in minutes, that can elapse before a web application, such as Cisco Unified Communications Manager Administration, times out and logs off the user.

For the new webapp session timeout setting to become effective, you must restart the Cisco Tomcat service. Until you restart the Cisco Tomcat service, the **show webapp session timeout** command reflects the new values, but system continues to use and reflect the old values. This command prompts you to restart the service.

**Caution** Restarting the Cisco Tomcat service ends all active sessions and can affect system performance. Cisco recommends that you only execute this command during off-peak traffic hours.

**Note** This setting gets preserved through a software upgrade and does not get reset to the default value.

**set webapp session timeout** *minutes*

## Syntax Description

| Parameters | Description |
|---|---|
| *minutes* | Specifies the time, in minutes, that can elapse before a web application times out and logs off the user.<br>• Value range: 5-99999 minutes<br>• Default value: 30 minutes |

## Command Modes

Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

## set workingdir

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

**set workingdir** {**activelog| inactivelog| tftp**} *directory*

**Syntax Description**

| Parameters | Description |
|---|---|
| **activelog** | Sets the working directory for active logs. Choose a valid sub-directory of activelog. |
| **inactivelog** | Set the working directory for inactive logs. Choose a valid sub-directory of inactivelog. |
| **tftp** | Sets the working directory for TFTP files. |
| *directory* | Represents the current working directory. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 0 for logs, 1 for TFTP

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

# Show commands

## show account

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

**show account**

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 4

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

# show accountlocking

This command displays the current account locking settings.

**show accountlocking**

**Command Modes** Administrator (admin:)

### Requirements

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

### Example

```
admin:show accountlocking
Account Lockout is disabled
```

# show cert*

## show cert list

This command displays certificate trust lists.

**show cert list** {**own**| **trust**}

**Syntax Description**

| Parameters | Description |
|---|---|
| **own** | Specifies owned certificates. |
| **trust** | Specifies trusted certificates. |

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

### Example

```
admin:cert list own
```

## show cert own

This command displays certificate contents.

**show cert own** *filename*

**Syntax Description**

| Parameters | Description |
|---|---|
| **own** | Specifies owned certificates. |
| *filename* | Represents the name of the certificate file. |

**Command Modes**

Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

## show cert trust

This command displays certificate contents.

**show cert trust** *filename*

**Syntax Description**

| Parameters | Description |
|---|---|
| **trust** | Specifies trusted certificates. |
| *filename* | Represents the name of the certificate file. |

**Command Modes**

Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

# show cli*

## show cli pagination

This command displays the status of automatic CLI automatic pagination.

**show cli pagination**

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

### Example

```
admin:show cli pagination
Automatic Pagination : Off.
```

## show cli session timeout

This command displays the CLI session timeout value, which is the amount of time, in minutes, that can elapse before a CLI session times out and disconnects.

**show cli session timeout**

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

# show csr*

## show csr list

This command displays Certificate Sign Request contents and certificate trust lists.

**show csr list** {**own** | **trust**}

**Syntax Description**

| Parameters | Description |
|---|---|
| **own** | Shows a list of owned Certificate Sign Requests. |
| **trust** | Shows a list of trusted Certificate Sign Requests. |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

The certificate name can be obtained by using the **show cert list own** command.

#### Requirements

Command privilege level:

Allowed during upgrade:

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

#### Example

```
admin: show csr list own
tomcat/tomcat.csr
Vipr-QuetzalCoatl/Vipr-QuetzalCoatl.csr
.....
.....
.....
```

## show csr own

This command displays Certificate Sign Request (CSR) contents and certificate trust lists.

**show csr own** *name*

**Syntax Description**

| Parameters | Description |
|---|---|
| *name* | The name of the CSR file. |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

The certificate name can be obtained by using the **show cert list own** command.

#### Requirements

Command privilege level:

Allowed during upgrade:

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

### Example

```
admin:show csr own tomcat/tomcat.csr

[
[
-----BEGIN CERTIFICATE SIGN REQUEST-----
MIIDrDCCAxUCBENeUewwDQYJKoZIhvcNAQEEBQAwggEbMTQwMgYDVQQGEytVbmFibGUgdG8gZmlu
ZCBDb3VudHJ5IGluIHBsYXRmb3JtIGRhdGFiYXNlMTIwMAYDVQQIEylVbmFibGUgdG8gZmluZCBT
dGF0ZSBpbiBwbGF0Zm9ybSBkYXRhYmFzZTE1MDMGA1UEBxMsVW5hYmxlIHRvIGZpbmQgTG9jYXRp
b24gaW4gcGxhdGZvcm0gZGF0YWJhc2UxMDAuBgNVBAoTJ1VuYWJsZSB0byBmaW5kIE9yZyBpbiBw
bGF0Zm9ybSBkYXRhYmFzZTExMC8GA1UECxMoVW5hYmxlIHRvIGZpbmQgVW5pdCBpbiBwbGF0Zm9y
bSBkYXRhYmFzZTETMBEGA1UEAxMKYmxkci1jY20zNjAeFw0wNTEwMjUxNTQwMjhaFw0xMDEwMjQx
NTQwMjhaMIIBGzE0MDIGA1UEBhMrVW5hYmxlIHRvIGZpbmQgQ291bnRyeSBpbiBwbGF0Zm9ybSBk
YXRhYmFzZTEyMDAGA1UECBMpVW5hYmxlIHRvIGZpbmQgU3RhdGUgaW4gcGxhdGZvcm0gZGF0YWJh
c2UxNTAzBgNVBAcTLFVuYWJsZSB0byBmaW5kIExvY2F0aW9uIGluIHBsYXRmb3JtIGRhdGFiYXNl
MTAwLgYDVQQKEydVbmFibGUgdG8gZmluZCBPcmcgaW4gcGxhdGZvcm0gZGF0YWJhc2UxMTAvBgNV
BAsTKFVuYWJsZSB0byBmaW5kIFVuaXQgaW4gcGxhdGZvcm0gZGF0YWJhc2UxEzARBgNVBAMTCmJs
ZHItY2NtMzYwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMoZ4eLmk1Q3uEFwmb4iU5nrMbhm
J7bexSnC3PuDGncxT3Au4zpGgMaQRL+mk+dAt8gDZfFKz8uUkUoibcUhvqk4h3FoTEM+6qgFWVMk
gSNUU+1i9MST4m1aq5hCP87GljtPbnCXEsFXaKH+gxBq5eBvmmzmO1D/otXrsfsnmSt1AgMBAAEw
DQYJKoZIhvcNAQEEBQADgYEAKwhDyOoUDiZvlAOJVTNF3VuUqv4nSJlGafB6WFldnh+3yqBWwfGn
```

# show date

This command displays the date and time on the server.

**show date**

## Command Modes

Administrator (admin:)

### Example

```
admin: show date
Sat Jul 17 01:28:57 IST 2010
```

# show diskusage

This command displays disk usage information about specific directories.

**show diskusage activelog** {**activelog**| **common**| **inactivelog**| **install**| **tftp**| **tmp**} **filename** *filename*{**directory**| **sort**}

## Syntax Description

| Parameters | Description |
|---|---|
| **filename** *filename* | Saves the output to a specified file. These files are stored in the platform/cli directory. To view saved files, use the file view activelog command. |

| Parameters | Description |
|---|---|
| **directory** | Displays the directory sizes only. |
| **sort** | Sorts the output on the basis of file size. File sizes display in 1024-byte blocks. |

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection

# show dscp*

## show dscp all

This command displays the current DSCP traffic markings on all the ports. It displays the DSCP markings in decimal and hexidecimal. If the value corresponds to a class then it displays the correct class. If the value does not correspond to a class, then it displays N/A.

**show dscp all**

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified CM and Cisco Unity Connection

## show dscp defaults

This command displays the default factory DSCP settings. These values take effect if the set dscp defaults, on page 83 command is executed.

**show dscp defaults**

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified CM and Cisco Unity Connection

## show dscp marking

This command displays the current DSCP traffic markings for a particular DSCP value.

**show dscp marking** *value*

### Syntax Description

| Parameters | Description |
|---|---|
| *value* | DSCP value. You can enter the name of a well-known DSCP class, or a numeric value in decimal or hexadecimal format. Precede hexadecimal values with 0x or 0X. |

### Command Modes

Administrator (admin:)

### Usage Guidelines

The valid class names as defined by DSCP are:

- Class Selector: values **CSO**, **CS1**, **CS2**, **CS3**, **CS5**, **CS6 CS7**

  The class selector (CS) values correspond to IP Precedence values and are fully compatible with IP Precedence.

- Expedited Forwarding: value **EF**

  EF PHB is ideally suited for applications such as VoIP that require low bandwidth, guaranteed bandwidth, low delay, and low jitter.

- Best Effort: value **BE**

  Also called default PHB, this value essentially specifies that a packet be marked with 0x00, which gets the traditional best-effort service from the network router.

- Assured Forwarding: values **AF11**, **AF12**, **AF13**, **AF21**, **AF22**, **AF23**, **AF41**, **AF42**, **AF43**

  There are four types of Assured Forwarding classes, each of which has three drop precedence values. These precedence values define the order in which a packet is dropped (if needed) due to network congestion. For example, packets in AF13 class are dropped before packets in the AF12 class.

### Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection

## show dscp status

This command displays the current DSCP traffic markings.

**show dscp status** {**enabled**| **disabled**}

**Syntax Description**

| Parameters | Description |
|---|---|
| **enabled** | Filters the output to show only DSCP traffic markings that are enabled. If you do not specify a status, this filter is the default option. |
| **disabled** | Filters the output to show only DSCP traffic markings that are disabled. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection

# show environment

This command displays environmental information for three types of hardware components.

**show environment** {**fans**| **power-supply**| **temperatures**}

**Syntax Description**

| Parameters | Description |
|---|---|
| **fans** | Displays the fan speeds in Rotations per Minute (RPMs), fan-speed thresholds, and status. |
| **power-supply** | Displays the power-supply status only MCS-7845, MCS-7835, MCS-7825H3/H4, and MCS-7816H3 servers (those servers with redundant power supplies or embedded health hardware). |
| **temperatures** | Displays the temperature sensor temporary values, thresholds, and status. |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

The output data from this command varies between IBM and HP server models.

### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection

# show hardware

This command displays hardware-related information about the platform.

**show hardware**

**Command Modes** Administrator (admin:)

**Usage Guidelines** The following information is displayed:

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

### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection

# show ipsec*

## show ipsec information

**show ipsec information** {*policy_group*| *policy_name*}

**Syntax Description**

| Parameters | Description |
|---|---|
| *policy_group* | |
| *policy_name* | |

**Command Modes** Administrator (admin:)

**Usage Guidelines**

**Requirements**

Command privilege level:

Allowed during upgrade:

Applies to: IM and Presence service on Unified CM

**Example title**

```
admin:
```

## show ipsec policy_group

This command displays all the ipsec policy group on the node.

**show ipsec policy_group**

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM and Cisco Unity Connection

## show ipsec policy_name

This command displays the list of ipsec policy names that exist in the specified policy group.

**show ipsec policy_name** *policy_group*

**Syntax Description**

| Parameters | Description |
|---|---|
| *policy_group* | Specifies the policy group name. |

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM and Cisco Unity Connection

### show ipsec status

**show ipsec status**

**Command Modes** Administrator (admin:)

**Usage Guidelines**

**Requirements**

Command privilege level:

Allowed during upgrade:

Applies to: IM and Presence service on Unified CM

## show logins

This command lists recent logins to the server

**show logins** [ *number* ]

**Syntax Description**

| Parameters | Description |
|---|---|
| *number* | Specifies the number of the most recent logins to display. The default is 20. |

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM and Cisco Unity Connection

## show memory

This command displays information about the onboard memory.

**show memory** {**count**| **modules**| **size**}

**Syntax Description**

| Parameters | Description |
|---|---|
| **count** | Displays the number of memory modules on the system. |
| **modules** | Displays detailed information about all the memory modules. |
| **size** | Displays the total amount of physical memory. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection

# show myself

This command displays information about the current account.

**show myself**

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection

# show network*

## show network all

This command shows network information for listening and nonlistening sockets.

**show network all [detail] [page]** [**search** *srchtext*]

**Syntax Description**

| Parameters | Description |
|---|---|
| **detail** | Shows additional information. |
| **page** | Displays information one page at a time. |
| **search** *srchtext* | Searches for *srchtext* in the output. |

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show network cluster

This command lists nodes in the network cluster.

**show network cluster**

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show network dhcp eth0

This command shows DHCP status information.

**show network dhcp eth0**

**Command Modes** Administrator (admin:)

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

### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show network eth0

This command shows network information for ethernet 0.

**show network eth0 [detail]** [**search** *srchtxt*]

**Syntax Description**

| Parameters | Description |
|---|---|
| **detail** | Shows additional information. |
| **search** *srchtxt* | Searches for *srchtxt* in the output. |

**Command Modes** Administrator (admin:)

**Usage Guidelines** The **eth0** parameter displays Ethernet port 0 settings

### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show network failover

This command shows Network Fault Tolerance information.

**show network failover [detail] [page]**

**Syntax Description**

| Parameters | Description |
|---|---|
| **detail** | Shows additional information. |
| **page** | Shows information one page at a time. |

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show network ip_conntrack

This command shows ip_conntrack usage information.

**show network ip_conntrack**

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show network ipprefs

### show network ipprefs

This command shows the list of ports that have been requested to be opened or translated in the firewall.

**show network ipprefs** {**all**| **enabled**| **public**}

**Syntax Description**

| Parameters | Description |
|---|---|
| **all** | Shows all incoming ports that may be used on the product. |
| **enabled** | Shows all incoming ports that are currently opened. |
| **public** | Shows all incoming ports that are currently opened for a remote client. |

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

### Example

```
admin: show network ipprefs public
Application  IPProtocol   PortValue    Type         XlatedPort   Status       Description

------------ ------------ ------------ ------------ ------------ ------------ ------------

sshd         tcp          22           public       -            enabled      sftp and ssh
access
tomcat       tcp          8443         translated   443          enabled      secure web
access
tomcat       tcp          8080         translated   80           enabled      web access

clm          udp          8500         public       -            enabled      cluster
manager
clm          tcp          8500         public       -            enabled      cluster
manager
ntpd         udp          123          public       -            enabled      network time
sync
snmpdm       udp          161          public       -            enabled      SNMP

ccm          tcp          2000         public       -            enabled      SCCP-SIG

ctftp        udp          6969         translated   69           enabled      TFTP access
to CUCM TFTP Server
ctftp        tcp          6970         public       -            enabled      HTTP access
```

## show network ipv6

This command shows IPv6 network routes and network settings.

**show network ipv6** {**route**| **settings**}

### Syntax Description

| Parameters | Description |
|---|---|
| **route** | Shows all IPv6 routes. |
| **settings** | Shows all IPv6 network settings. |

### Command Modes

Administrator (admin:)

**Usage Guidelin**

**Note** IPv6 is not supported in Cisco Unified Communications Manager Business Edition 5000.

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, Cisco Unity Connection

## show network max_ip_conntrack

This command shows max_ip_conntrack information.

**show network max_ip_conntrack**

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show network route

This command shows network routing information.

**show network route [detail]** [**search** *srchtext*]

**Syntax Description**

| Parameters | Description |
|---|---|
| **detail** | Shows additional information. |
| **search** *srchtext* | Searches for the *srchtext* in the output. |

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show network status

This command shows active internet connections.

**show network status [detail] [listen] [process] [all] [nodns][search** *stext*]

**Syntax Description**

| Parameters | Description |
|---|---|
| **detail** | Shows additional information. |
| **listen** | Shows only listening sockets. |
| **process** | Shows the process ID and name of the program to which each socket belongs. |
| **all** | Shows both listening and nonlistening sockets. |
| **nodns** | Shows numerical addresses without any DNS information. |
| **search** *stext* | Searches for the *stext* in the output. |

**Command Modes**

Administrator (admin:)

### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

### Example

This example displays active internet connections.

```
admin: show network status
```

# show open*

## show open files*

### show open files all

This command shows all open files on the system.

**show open files all**

**Command Modes** Administrator (admin:)

**Requirements**

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

### show open files process

The command shows open files that belong to a specified process.

**show open files process** *processID*

**Syntax Description**

| Parameters | Description |
|---|---|
| *processID* | Specifies a process. |

**Command Modes** Administrator (admin:)

**Requirements**

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

### show open files regexp

This command shows open files that match the specified regular expression.

**show open files regexp** *reg_exp*

**Syntax Description**

| Parameters | Description |
|---|---|
| *reg_exp* | Specifies a regular expression. |

**Command Modes** Administrator (admin:)

**Requirements**

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

# show open ports*

## show open ports all

This command shows all open ports on the system.

**show open ports all**

**Command Modes** Administrator (admin:)

### Requirements

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show open ports process

This command displays open ports the belong to a specified process.

**show open ports process** *processID*

**Syntax Description**

| Parameters | Description |
|---|---|
| *processID* | Specifies a process. |

**Command Modes** Administrator (admin:)

### Requirements

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show open ports regexp

This command shows open ports that match the specified regular expression.

**show open ports regexp** *reg_exp*

**Syntax Description**

| Parameters | Description |
|---|---|
| *reg_exp* | Specifies a regular expression. |

**Command Modes** Administrator (admin:)

### Requirements

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

# show packages

This command displays the name and version for installed packages.

**show packages** {**active**| **inactive**} *name* **[page]**

**Syntax Description**

| Parameters | Description |
|---|---|
| **active** | Specifies active packages. |
| **inactive** | Specifies inactive packages. |
| *name* | Specifies the package name. To display all active or inactive packages, use the wildcard character, *. |
| **page** | Shows the output one page at a time |

**Command Modes**

Administrator (admin:)

### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

# show password*

## show password

This command shows information about the configured password.

**show password** {**age**| **history**| **inactivity**}

**Syntax Description**

| Parameters | Description |
|---|---|
| **age** | Shows information about the configured password age parameters |
| **history** | Shows the number of passwords that the history maintains for OS administration accounts. |

| Parameters | Description |
|---|---|
| **inactivity** | Shows the status of the password inactivity for OS accounts. Password inactivity is the number of days of inactivity after a password has expired before the account is disabled. |

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

### show password change-at-login

This command shows whether a user is forced to change passwords after the user signs in to the system the next time.

**show password change-at-login** *userid*

**Syntax Description**

| Parameters | Description |
|---|---|
| *userid* | Specifies the user account that you want to show. |

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show password expiry*

### show password expiry

This command shows the configured password expiration parameters.

**show password expiry** {**maximum-age**| **minimum-age**}

**Syntax Description**

| Parameters | Description |
|---|---|
| **maximum-age** | Shows the maximum number of days for set password expiry. |
| **minimum-age** | Shows the minimum number of days for set password expiry. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

### show password expiry user

This command shows the configured password expiration parameters for the specified user.

**show password expiry user** {**maximum-age**| **minimum-age**} *userid*

**Syntax Description**

| Parameters | Description |
|---|---|
| **maximum-age** | Shows the maximum number of days for set password expiry. |
| **minimum-age** | Shows the minimum number of days for set password expiry. |
| *userid* | Specifies the user account that you want to show. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

### show password expiry user list

This command shows the password maximum age and password minimum age for each CLI user in the system.

**show password expiry user**

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

# show perf*

## show perf counterhelp

This command displays information about the specified perfmon counter.

**show perf counterhelp** *class-name counter-name*

**Syntax Description**

| Parameters | Description |
|---|---|
| *class-name* | Represents the class name that contains the counter. |
| *counter-name* | Represents the counter that you want to view. |

**Command Modes** Administrator (admin:)

**Usage Guidelines** 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

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show perf list categories

This command lists the categories in the perfmon system.

**show perf list categories**

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show perf list classes

This command lists perfmon classes (objects).

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

**Syntax Description**

| Parameters | Description |
|---|---|
| **cat** *category* | Displays perfmon classes for the specified category. |
| **detail** | Displays detailed information. |

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show perf list counters

This command lists perfmon counters for the specified perfmon class.

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

**Syntax Description**

| Parameters | Description |
|---|---|
| *class-name* | Represents the class name that contains the counter. |
| **detail** | Displays detailed information. |

**Command Modes** Administrator (admin:)

**Usage Guidelines** If the class name contains white spaces, enclose the name in double quotation marks.

### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show perf list instances

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

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

**Syntax Description**

| Parameters | Description |
|---|---|
| *class-name* | Represents the class name that contains the counter. |
| **detail** | Displays detailed information. |

**Command Modes** Administrator (admin:)

**Usage Guidelines** If the class name contains white spaces, enclose the name in double quotation marks.

### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show perf query class

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

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

**Syntax Description**

| Parameters | Description |
|---|---|
| *class-name* | Represents the class name that contains the counter. |

**Command Modes** Administrator (admin:)

**Usage Guidelines** If the class name contains white spaces, enclose the name in double quotation marks.

You can specify a maximum of five classes for each command.

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show perf query counter

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

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

**Syntax Description**

| Parameters | Description |
|---|---|
| *class-name* | Represents the class name that contains the counter. |
| *counter-name* | Represents the counter that you want to view. |

**Command Modes** Administrator (admin:)

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

You can specify a maximum of five counters for each command.

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show perf query instance

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

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

**Syntax Description**

| Parameters | Description |
|---|---|
| *class-name* | Represents the class name that contains the counter. |

| Parameters | Description |
|---|---|
| *instance-name* | Specifies the perfmon instance to view. |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

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

You can specify a maximum of five instances for each command.

This command does not apply to singleton perfmon classes.

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show perf query path

This command queries a specified perfmon path.

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

**Syntax Description**

| Parameters | Description |
|---|---|
| *path-spec* | Specifies a perfmon path. |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

For an instance-based perfmon class, you must specify *path-spec* as follows:
*class-name(instance-name)\counter-name*

For a noninstance-based perfmon class (a singleton), you must specify *path-spec* as follows:
*class-name\counter-name*

You can specify a maximum of five paths for each command.

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

### Example

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

# show process*

## show process list

This command displays a list of all the processes and critical information about each process and visually indicates the child-parent relationships between the processes.

**show process list** [**file** *filename*] [**detail**]

**Syntax Description**

| Parameters | Description |
|---|---|
| **file** | Outputs the results to the file that is specified by the filename variable. |
| *filename* | Specifies the filename. |
| **detail** | Displays detailed output. |

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show process load

This command displays the current load on the system.

**show process load** [**cont**] [**clear**] [**noidle**] [**num** *number*] [**thread**] [**cpu** | **memory** | **time**] [**page**]

**Syntax Description**

| Parameters | Description |
|---|---|
| **cont** | Repeats the command continuously. |
| **clear** | Clears the screen before displaying output. |
| **noidle** | Ignores the idle or zombie processes. |

| Parameters | Description |
|---|---|
| **num** *number* | Displays the number of processes that are specified by number. The default number of processes equals 10. Set *number* to all to display all processes. |
| **thread** | Displays threads. |
| **cpu** | Sorts output by CPU usage. This is the default sorting. |
| **memory** | Sorts output by memory usage. |
| **time** | Sorts output by time usage. |
| **page** | Displays the output in pages. |

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show process name

This command displays the details of processes that share the same name and indicates their parent-child relationship.

**show process name** *process* [**file** *filename*]

**Syntax Description**

| Parameters | Description |
|---|---|
| *process* | Specifies the name of a process. |
| **file** *filename* | Outputs the results to the file that is specified by *filename*. |

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show process open-fd

This command lists the open file descriptors for a comma-separated list of process IDs.

**show process open-fd** *process-id* [,*process-id2*]

**Syntax Description**

| Parameters | Description |
|---|---|
| *process-id* | Specifies the process-id. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show process pid

This command shows a specific process number or command name.

**show process pid** *pid* [**file** *filename*]

**Syntax Description**

| Parameters | Description |
|---|---|
| *pid* | Specifies the process ID number of a process. |
| **file** *filename* | Outputs the results to the file that is specified by *filename*. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show process search

This command searches for the pattern that the regular expression regexp specifies in the output of the operating system-specific process listing.

**show process search** *regexp* [**file** *filename*]

**Syntax Description**

| Parameters | Description |
|---|---|
| *regexp* | Represents a regular expression. |
| **file** *filename* | Outputs the results to the file that is specified by *filename*. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show process user

This command retrieves details of processes that share the user name and displays parent-child relationship.

**show process user** *username* [**file** *filename*]

**Syntax Description**

| Parameters | Description |
|---|---|
| *username* | Specifies the username. |
| **file** *filename* | Outputs the results to the file that is specified by *filename*. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show process using-most cpu

This command displays a list of the most CPU-intensive processes.

**show process using-most cpu** [*number*] [**file** *filename*]

**Syntax Description**

| Parameters | Description |
|---|---|
| *number* | Specifies the number of processes to display. The default specifies 5. |
| **file** *filename* | Outputs the results to the file that is specified by *filename*. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show process using-most memory

This command displays a list of the most memory-intensive processes.

**show process using-most memory** [*number*] [**file** *filename*]

**Syntax Description**

| Parameters | Description |
|---|---|
| *number* | Specifies the number of processes to display. The default specifies 5. |
| **file** *filename* | Outputs the results to the file that is specified by *filename*. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

# show registry

This command displays the contents of the registry.

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

**Syntax Description**

| Parameters | Description |
|---|---|
| *system* | Represents the registry system name. |
| *component* | Represents the registry component name. |
| *name* | Represents the name of the parameter to show. |
| **page** | Displays one page at a time. |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

If the name is "page," and you want to display the output one page at a time, use the command **show registry** *system component name* **page page**

To show all components in a system, enter the wildcard character * in the command: **show registry** *system* *

#### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

#### Example

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

```
admin: show registry cm dbl/sdi
```

# show risdb*

## show risdb list

This command displays the tables that are supported in the Realtime Information Service (RIS) database.

**show risdb list** [**file** *filename*]

**Syntax Description**

| Parameters | Description |
|---|---|
| **file** *filename* | Outputs the information to a file. |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

The **file** option saves the information to `platform/cli/filename.txt`. Ensure that the filename does not contain the "." character.

#### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

#### Example

This command displays a list of all RIS database tables.

```
admin: show risdb list
```

## show risdb query

This command displays the contents of the specified RIS tables.

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

**Syntax Description**

| Parameters | Description |
|---|---|
| *table1* | Specifies the name of a table. |
| **file** *filename* | Outputs the information to a file. |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

The file option saves the information to `platform/cli/filename.txt`. Ensure that the filename does not contain the "." character.

#### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

# show session maxlimit

This command shows the upper limit for concurrent SSH sessions.

**show session maxlimit**

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

# show smtp

This command displays the name of the SMTP host.

**show snmp**

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

# show stats io

This command displays the IO statistics.

**show stats io** [**kilo**] [**detail**] [**page**] [**file** *filename*]

**Syntax Description**

| Parameters | Description |
|---|---|
| **kilo** | Displays statistics in kilobytes. |
| **detail** | Displays detailed statistics on every available device on the system and overrides the **kilo** option. |

| Parameters | Description |
|---|---|
| **page** | Displays one page at a time. |
| **file** *filename* | Outputs the information to a file specified by *filename* |

**Command Modes** Administrator (admin:)

**Usage Guidelines** The **file** option saves the information to `platform/cli/filename.txt`. Ensure that the filename does not contain the "." character.

### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

# show status

This command displays basic platform status.

**show status**

**Command Modes** Administrator (admin:)

**Usage Guidelines** This command displays the following basic platform status:

- hostname
- date
- timezone
- locale
- product version
- platform version
- CPU usage
- memory and disk usage

### Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

# show tech*

## show tech activesql

This command displays the active queries to the database taken at one minute intervals as far back as the logs allow.

**show tech activesql**

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show tech all

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

**show tech all** [**page**] [**file** *filename*]

**Syntax Description**

| Parameters | Description |
|---|---|
| **page** | Displays one page at a time. |
| **file** *filename* | Outputs the information to a file. |

**Command Modes** Administrator (admin:)

**Usage Guidelines** The file option saves the information to `platform/cli/filename.txt`. Ensure that the file name does not contain the "." character

### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show tech network all

This command displays all network tech information.

**show tech network all** [**page**] [**search** *text*] [**file** *filename*]

**Syntax Description**

| Parameters | Description |
|---|---|
| **page** | Displays one page at a time. |
| **search** *text* | Searches the output for the string that text specifies. Be aware that the search is case insensitive. |
| **file** *filename* | Outputs the information to a file. |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

The **file** option saves the information to `platform/cli/filename.txt`. Ensure that the file name does not contain the "." character

### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show tech network hosts

This command displays information about hosts configuration.

**show tech network hosts** [**page**] [**search** *text*] [**file** *filename*]

**Syntax Description**

| Parameters | Description |
|---|---|
| **page** | Displays one page at a time. |
| **search** *text* | Searches the output for the string that text specifies. Be aware that the search is case insensitive. |
| **file** *filename* | Outputs the information to a file. |

**Command Modes** Administrator (admin:)

**Usage Guidelines** The **file** option saves the information to `platform/cli/filename.txt`. Ensure that the file name does not contain the "." character

#### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show tech network interfaces

This command displays information about the network interfaces.

**show tech network interfaces** [**page**] [**search** *text*] [**file** *filename*]

**Syntax Description**

| Parameters | Description |
|---|---|
| **page** | Displays one page at a time. |
| **search** *text* | Searches the output for the string that text specifies. Be aware that the search is case insensitive. |
| **file** *filename* | Outputs the information to a file. |

**Command Modes** Administrator (admin:)

**Usage Guidelines** The **file** option saves the information to `platform/cli/filename.txt`. Ensure that the file name does not contain the "." character

#### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show tech network resolv

This command displays information about hostname resolution.

**show tech network resolv** [**page**] [**search** *text*] [**file** *filename*]

**Syntax Description**

| Parameters | Description |
|---|---|
| **page** | Displays one page at a time. |
| **search** *text* | Searches the output for the string that text specifies. Be aware that the search is case insensitive. |
| **file** *filename* | Outputs the information to a file. |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

The **file** option saves the information to `platform/cli/filename.txt`. Ensure that the file name does not contain the "." character

#### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show tech network routes

This command displays information about network routes.

**show tech network routes** [**page**] [**search** *text*] [**file** *filename*]

**Syntax Description**

| Parameters | Description |
|---|---|
| **page** | Displays one page at a time. |
| **search** *text* | Searches the output for the string that text specifies. Be aware that the search is case insensitive. |
| **file** *filename* | Outputs the information to a file. |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

The **file** option saves the information to `platform/cli/filename.txt`. Ensure that the file name does not contain the "." character

### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show tech network sockets

This command displays the list of open sockets.

**show tech network sockets** {**numeric**}

**Syntax Description**

| Parameters | Description |
|---|---|
| **numeric** | Displays the numerical addresses of the ports instead of determining symbolic hosts. This parameter is equivalent to running the Linux shell **numeric [-n]** command. |

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show tech runtime

This command displays CPU usage information at the time the command is run.

**show tech runtime** {**all**| **cpu**| **disk**| **env**| **memory**} **page file** *filename*

**Syntax Description**

| Parameters | Description |
|---|---|
| **all** | Displays all runtime information. |
| **cpu** | Displays CPU usage information at the time the command is run. |
| **disk** | Displays system disk usage information. |
| **env** | Displays environment variables. |
| **memory** | Displays memory usage information. |
| **page** | Displays one page at a time. |

| Parameters | Description |
|---|---|
| **file** *filename* | Outputs the information to a specified file.<br>**Note** This option saves the information to platform/cli/<filename>.txt. Ensure that the file name does not contain the "." character. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection

## show tech system

This command displays all the system information.

**show tech system** {**all**| **bus**| **hardware**| **host**| **kernel modules**| **software**| **tools**} **page file** *filename*

**Syntax Description**

| Parameters | Description |
|---|---|
| **all** | Displays all the system information. |
| **bus** | Displays information about the data buses on the server. |
| **hardware** | Displays information about the server hardware. |
| **host** | Displays information about the server. |
| **kernel modules** | Lists the installed kernel modules. |
| **software** | Displays information about the installed software versions. |
| **tools** | Displays information about the software tools on the server. |
| **page** | Displays one page at a time. |

| Parameters | Description |
|---|---|
| **file** *filename* | Outputs the information to a file. This option saves the information to platform/cli/<filename>.txt. Ensure that the file name does not contain the "." character. |

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

# show timezone

## show timezone config

This command displays the current timezone settings.

**show timezone config**

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show timezone list

This command displays the available timezones.

**show timezone list** [**page**]

**Syntax Description**

| Parameters | Description |
|---|---|
| **page** | Displays the output one page at a time. |

**Command Modes** Administrator (admin:)

**Usage Guidelines** Although the list of available time zones includes **Factory**, Unified CM does not support the **Factory** timezone.

### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

# show trace

This command displays trace information for a particular task.

**show trace** [*task_name*]

**Syntax Description**

| Parameters | Description |
|---|---|
| *task_name* | Represents the name of the task for which you want to display the trace information. |

**Command Modes** Administrator (admin:)

**Usage Guidelines** If you do not enter a parameter, the command returns a list of available tasks.

### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

### Example

```
admin: show trace cdps
```

# show ups status

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

**show ups status**

**Command Modes** Administrator (admin:)

**Usage Guidelines** This command provides full status only for 7835-H2 and 7825-H2 servers.

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

# show version*

## show version active

This command displays the software version on the active partition.

**show version active**

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: o

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## show version inactive

This command displays the software version on the inactive partition

**show version inactive**

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: o

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

# show web-security

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

**show web-security**

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

# show webapp session timeout

This command displays the webapp session timeout value, which is the amount of time, in minutes, that can elapse before a web application times out and logs off the user.

**show webapp session timeout**

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

# show workingdir

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

**show workingdir**

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

# Unset commands

## unset ipsec*

### unset ipsec policy_group

This command disables the ipsec policy on the specified group.

**unset ipsec policy_group** *policy_group*

**Syntax Description**

| Parameters | Description |
|---|---|
| *policy_group* | Specifies the group name. |

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

### unset ipsec policy_name

This command disables the ipsec policy with the specified name.

**unset ipsec policy_name** *policy_name*

**Syntax Description**

| Parameters | Description |
|---|---|
| *policy_name* | Specifies the policy name to disable. |

**Command Modes** Administrator (admin:)

**Usage Guidelines** Enter `ALL` for *policy_name* to disable all policy names.

### Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

# unset network*

## unset network dns options

This command unsets DNS options.

**unset network dns options** [**timeout**] [**attempts**] [**rotate**]

**Syntax Description**

| Parameters | Description |
|---|---|
| **timeout** | Sets the wait time before the system considers a DNS query as failed to the default. |
| **attempts** | Sets the number of DNS attempts to make before the system fails to the default. |
| **rotate** | Sets the method for selecting a nameserver to the default. This affects how loads are distributed across nameservers. |

**Command Modes** Administrator (admin:)

**Usage Guidelines** You are asked to confirm that you want to execute this command.

**Caution** If you continue, the system loses network connectivity temporarily.

### Requirements

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## unset network domain

This command unsets the domain name and restarts the server.

**unset network domain**

**Command Modes** Administrator (admin:)

**Usage Guidelines** You are asked to confirm that you want to execute this command.

#### Requirements

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

#### Example

```
admin: unset network domain
cmdSetIp.domain.name.change.warning
Continue (y/n)?
trying to restart system...
Warning: Restart could take up to 5 minutes...
Shutting down Service Manager. Please wait...
```

### unset network ipv6 static_address

This command unsets the IPV6 static address.

**unset network ipv6 static_address** [*reboot*]

**Syntax Description**

| Parameters | Description |
|---|---|
| *reboot* | Reboots the server after applying the change. |

**Command Modes** Administrator (admin:)

#### Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, Cisco Unity Connection

#### Example

```
admin: admin:unset network ipv6 static_address
    W A R N I N G
The Server must be rebooted for these changes to take effect.
Please make sure that you reboot this server.
IPv6 static address was removed.
```

# Utils commands

## utils auditd

This command starts, stops, and provides the status of the system auditing service.

**utils auditd** {**enable**| **disable**| **status**}

**Syntax Description**

| Parameters | Description |
|---|---|
| **enable** | Enables the collection of audit logs. When enabled, the system monitors and records user actions as well as Linux events such as the creation and removal of users, as well as the editing and deleting of files . |
| **disable** | Disables the collection of audit logs. |
| **status** | Displays the status of audit log collection. Cisco recommends that you retrieve the audit log by using the Real-Time Monitoring Tool, but you can also retrieve it by using the CLI. |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

After the service has been enabled, it monitors and logs activity on the system. Be aware that the system auditing service logs a lot of information. Care must be taken not to overfill the disk.

#### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

# utils core*

## utils core analyze

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

**utils core** {**active**| **inactive**} **analyze** [ *core_filename* ]

**Syntax Description**

| Parameters | Description |
|---|---|
| **active** | Specifies an active version |
| **inactive** | Specifies an inactive version |
| *core_filename* | Specifies the name of the core file from which to generate the stack trace. |

**Command Modes** Administrator (admin:)

**Usage Guidelines** This command creates a file of the same name as the core file, with a .txt extension, in the same directory as the core file. After you execute this command on a core file created by cimserver, an unexpected message displays. This message is a known limitation of the command.

#### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

### utils core list

This command displays all active or inactive core files.

**utils core** {**active**| **inactive**} **list**

**Command Modes** Administrator (admin:)

#### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

## utils create report

This command creates reports about the server in the platform/log directory.

**utils create report** {**csa**| **hardware**| **platform**| **security**}

**Syntax Description**

| Parameters | Description |
|---|---|
| **csa** | Collects all the files required for the Cisco Security Agent (CSA) diagnostics and assembles them into a single CSA diagnostics file. You can retrieve this file using the **file get** command. |
| **hardware** | Creates a system report that contains disk array, remote console, diagnostic, and environmental data. |
| **platform** | Collects the platform configuration files into a TAR file. |

| Parameters | Description |
|---|---|
| **security** | Collects the diagnostic reports and creates a TAR file that you can download for troubleshooting purposes. You can retrieve this file with the **file get** command. |

**Command Modes** Administrator (admin:)

**Usage Guidelines** You are prompted to continue after you enter the command.

After you create a report, use the command **file get activelog platform/log/***filename* command, to get the report. where *filename* specifies the report filename that displays after the command completes.

### Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

# utils diagnose

This command enables you to diagnose and attempt to automatically fix system problems.

**utils diagnose** {**fix| list| module| test| version**} *[module_name]*

**Syntax Description**

| Parameters | Description |
|---|---|
| **fix** | Runs all diagnostic commands and attempts to fix problems. |
| **list** | Lists all available diagnostic commands. |
| **module** | Runs a single diagnostic command or group of commands and attempts to fix problems |
| **test** | Runs all diagnostic commands but does not attempt to fix problems. |
| **version** | Displays the diagnostic framework version. |
| *module_name* | Specifies the name of a diagnostics module. |

**Command Modes** Administrator (admin:)

### Requirements

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection

# utils disaster_recovery*

## utils disaster_recovery backup local

This command invokes the backup and creates the tar file on the local drive.

**utils disaster_recovery backup local** *featurelist device_name*

**Syntax Description**

| Parameters | Description |
|---|---|
| *featurelist* | Comprises a comma-separated feature list to backup. |
| *device_name* | Specifies the name of the backup device to be added. |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

Use **utils disaster_recovery show_registration** to display the list of registered features.

Use **utils disaster_recovery device list** to display the configured device list.

### Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence on Unified CM, Cisco Unity Connection

## utils disaster_recovery cancel_backup

This command cancels the ongoing backup.

**utils disaster_recovery cancel_backup** [ *confirm* ]

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

After you enter the command, you must confirm that you want to cancel the backup. Enter **Y** to cancel the backup or any other key to continue the backup.

### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection

### Example

```
admin: utils disaster_recovery cancel_backup yes
Cancelling backup...
Backup cancelled successfully.
```

## utils disaster_recovery device add local

This command adds a backup local device.

**utils disaster recovery device add local** *device_name Number_of_backups*

**Syntax Description**

| Parameters | Description |
|---|---|
| *device_name* | Name of the backup device to be added. |
| *Number_of_backups* | Number of backups to be stored on the local or the network directory (default value is 2). |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

You get prompted for confirmation after you enter the command. You cannot delete directories or files that are in use.

**Caution** You cannot recover a deleted file, but you may be able to with The Disaster Recovery System.

### Requirements

Command privilege level: 1

Allowed during upgrade: No

### Examples

```
admin:utils disaster_recovery device add local localBackup 3
admin:utils disaster_recovery device add network networkDevice /root
10.77.31.116 root 3

admin:utils disaster_recovery device add tape tapeDevice /dev/nst0
```

## utils disaster_recovery device add network

This command adds the backup network device.

**utils disaster_recovery device add network** *devicename path server_namei/ip_address username* [ *Number_of_backups* ]

**Syntax Description**

| Parameters | Description |
|---|---|
| *devicename* | Specifies the name of the backup device to be added (mandatory). |
| *path* | Specifies the path to retrieve the backup device (mandatory). |
| *server_name/ip_address* | Specifies the hostname or IP address of the server where the backup file is stored (mandatory). |
| *username* | Specifies the userid required to connect to the remote machine (mandatory). |
| [ *Number_of_backups* ] | Specifies the number of backups to store on the Network Directory (default 2). This parameter is optional. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection

**Example**

```
admin: utils disaster_recovery device add network networkDevice /root 10.77.31.116 root 3
```

## utils disaster_recovery device delete

This command deletes the specified device.

**utils disaster_recovery device delete** *device_name*| *

**Syntax Description**

| Parameters | Description |
|---|---|
| *device_name* | Name of the device to be deleted. |
| * | Deletes all existing devices except for the ones associated to a schedule. |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection

## utils disaster_recovery device list

Displays the device name, device type, and device path for all the backup devices.

**utils disaster_recovery device list**

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection

## utils disaster_recovery history

This command displays the history of previous backups and restores.

**utils disaster_recovery history** [ *operation* ]

**Syntax Description**

| Parameters | Description |
|---|---|
| *operation* | Specifies backup or restore. |

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level:

Allowed during upgrade:

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection

**Example**

```
admin: utils disaster_recovery history backup
Tar Filename: Backup Device: Completed On: Result: Backup Type: Features Backed Up:
```

```
2009-10-30-14-53-32.tar TAPE Fri Oct 30 14:55:31 CDT 2009 ERROR MANUAL
2009-12-10-10-30-17.tar TAPE Thu Dec 10 10:35:22 CST 2009 SUCCESS MANUAL CDR_CAR,CCM
```

## utils disaster_recovery restore local

This command invokes the restore and takes the tar file from network drive.

**utils disaster_recovery restore local** *restore_server tarfilename device_name*

**Syntax Description**

| Parameters | Description |
|---|---|
| *restore_server* | represents the hostname of the server to be restored. |
| *tarfilename* | specifies the file that will get restored (without the file extension, for example: 2008-01-21-18-25-03). |
| *device_name* | specifies the name of the backup device to be added. |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

Use **utils disaster_recovery device list** to display the configured device list.

#### Requirements

Command privilege level: 1

Allowed during upgrade: No

#### Example

```
admin:utils disaster_recovery restore local SW075B-CM11 2008-01-21-18-25-03
 localdeviceRestore initiated successfully.Please run 'utils showstatus
restore' command to see the status.
```

## utils disaster_recovery restore network

This command backs up files to a remote server.

**utils disaster_recovery restore network** *restore_server tarfilename devicename*

**Syntax Description**

| Parameters | Description |
|---|---|
| *restore_server* | Specifies the hostname of the remote server that you want to restore. |
| *tarfilename* | Specifies the name of the file to restore. |

| Parameters | Description |
|---|---|
| *devicename* | Specifies the name of the device on which to restore files. |

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection

## utils disaster_recovery schedule add

This command adds the configured schedules.

**utils disaster_recovery schedule add** *schedulename devicename featurelist datetime frequency*

**Syntax Description**

| Parameters | Description |
|---|---|
| *schedulename* | Represents the name of the scheduler (mandatory). |
| *devicename* | Represents the name of the device for which scheduling is done (mandatory). |
| *featurelist* | Represents the comma-separated feature list to back up (mandatory). |
| *datetime* | Represents the date when the scheduler is set (mandatory). Format specified (yyyy/mm/dd-hh:mm) 24-hr clock. |
| *frequency* | Represents the frequency at which the schedule is set to take a backup. Examples: once, daily, weekly and monthly. |

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection

## utils disaster_recovery schedule

This command enables or disables the specified schedule.

**utils disaster_recovery schedule** {**enable**| **disable**} [ *schedulename* ]

**Syntax Description**

| Parameters | Description |
|---|---|
| **enable** | Enables the specified schedule. |
| **disable** | Disables the specified schedule. |
| *schedulename* | Represents the name of the scheduler. |

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level:1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection

### Example

```
admin: utils disaster_recovery schedule enable schedule1
Schedule enabled successfully.
```

## utils disaster_recovery schedule list

Displays the schedules that are configured.

**utils disaster_recovery schedule list**

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection

### Example

```
admin: utils disaster_recovery schedule list
schedule name device name Schedule Status
----------------------------------------
schedule1      device 1     enabled
schedule2      device 2     disabled
```

## utils disaster_recovery show_backupfiles

This command displays information about backup files.

**utils disaster_recovery show_backupfiles** {| } [ ]

**Syntax Description**

| Parameters | Description |
|---|---|
| | |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection

## utils disaster_recovery show_registration

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

**utils disaster_recovery show_registration** *hostname*

**Syntax Description**

| Parameters | Description |
|---|---|
| *hostname* | Specifies the server for which you want to display registration information. |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection

## utils disaster_recovery status

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

**utils disaster_recovery status** *operation*

**Syntax Description**

| Parameters | Description |
|---|---|
| *operation* | Specifies the name of the ongoing operation: backup or restore. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection

# utils firewall*

## utils firewall ipv4 debug

This command turns IPv4 firewall debugging on or off. If you do not enter a time parameter, this command turns on debugging for 5 minutes.

**utils firewall ipv4 debug** {**off**| [ *time* ]}

**Syntax Description**

| Parameters | Description |
|---|---|
| **off** | Turns off the IPv4 firewall debugging. If you do not enter the time parameter, this command disables the firewall for 5 minutes. |
| *time* | (Optional) Sets the duration for which the firewall debugging is to be enabled in the following formats:<br>• Minutes: 0–1440m<br>• Hours: 0–23h<br>• Hours and minutes: 0–23h 0–60m |

**Command Modes**

Administrator (admin:)

### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

## utils firewall ipv4

This commands enables and disables IPv4 firewall.

**utils firewall ipv4** {**enable**| **disable**| *[time]*}

### Syntax Description

| Parameters | Description |
|---|---|
| **enable** | Turns on the IPv4 firewall. |
| **disable** | Turns off the IPv4 firewall. If you do not enter the time parameter, this command disables the firewall for 5 minutes. |
| *time* | (Optional) Sets the duration for which the firewall is to be disabled in the following formats:<br>• Minutes: 0–1440m<br>• Hours: 0–23h<br>• Hours and minutes: 0–23h 0–60m |

### Command Modes

Administrator (admin:)

### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

## utils firewall ipv4 list

This commands displays the current configuration of the IPv4 firewall.

**utils firewall ipv4 list**

### Command Modes

Administrator (admin:)

### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

## utils firewall ipv4 status

This command displays the current status of the IPv4 firewall.

**utils firewall ipv4 status**

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

## utils firewall ipv6 debug

This command turns IPv6 firewall debugging on or off. If you do not enter a time parameter, this command turns on debugging for 5 minutes.

**Note** IPv6 is not supported in Cisco Unified Communications Manager Business Edition 5000.

**utils ipv6 firewall debug** {**off**| [ *time* ]}

**Syntax Description**

| Parameters | Description |
|---|---|
| **off** | Turns off the IPv6 firewall debugging. If you do not enter the time parameter, this command disables the firewall for 5 minutes. |
| *time* | (Optional) Sets the duration for which the firewall debugging is to be enabled in the following formats:<br>• Minutes: 0–1440m<br>• Hours: 0–23h<br>• Hours and minutes: 0–23h 0–60m |

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM and Cisco Unity Connection.

## utils firewall ipv6

This commands enables and disables IPv6 firewall.

**Note** IPv6 is not supported in Cisco Unified Communications Manager Business Edition 5000.

**utils firewall ipv6** {**enable**| **disable**| *[time]*}

**Syntax Description**

| Parameters | Description |
|---|---|
| **enable** | Turns on the IPv6 firewall. |
| **disable** | Turns off the IPv6 firewall. If you do not enter the time parameter, this command disables the firewall for 5 minutes. |
| *time* | (Optional) Sets the duration for which the firewall is to be disabled in the following formats:<br>• Minutes: 0–1440m<br>• Hours: 0–23h<br>• Hours and minutes: 0–23h 0–60m |

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM and Cisco Unity Connection.

## utils firewall ipv6 list

This commands displays the current configuration of the IPv6 firewall.

**Note** IPv6 is not supported in Cisco Unified Communications Manager Business Edition 5000.

**utils firewall ipv6 list**

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM and Cisco Unity Connection.

## utils firewall ipv6 status

This command displays the current status of the IPv6 firewall.

**Note** IPv6 is not supported in Cisco Unified Communications Manager Business Edition 5000.

**utils firewall ipv6 status**

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM and Cisco Unity Connection.

# utils import config

This command takes data from the platformConfig.xml file on the virtual floppy drive and modifies the system to match the configuration file. The system reboots after the command successfully completes.

**utils import config**

**Command Modes** Administrator (admin:)

**Usage Guidelines** This command can be executed on any VMware deployment.

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

### Execute utils import config in Vmware deployment

**Procedure**

# utils iostat

This command displays the iostat output for the given number of iterations and intervals.

**utils iostat** {**interval| iterations| filename**}

**Syntax Description**

| Parameters | Description |
|---|---|
| **interval** | Sets the seconds between two iostat readings. You must set this value if you are using the iteration parameter |
| **iterations** | Sets the number of iostat iterations. You must set this value if you are using the interval parameter. |
| **filename** | Redirects the output to a file. |

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection

# utils iothrottle

This command allows you to manage and monitor IO throttling on the server.

**utils iothrottle** {**enable**| **disable**| **status**}

**Syntax Description**

| Parameters | Description |
|---|---|
| **Enable** | Enables I/0 throttling enhancements which lowers the impact of upgrades on an active system. |
| **Disable** | Disables I/0 throttling enhancements. |
| **Status** | Displays the status of I/0 throttling enhancements. |

**Command Modes** Administrator (admin:)

**Usage Guidelines** Disabling I/0 throttling enhancements can adversely affect the system during upgrades.

# utils ldap config

This command configures the system LDAP authentication.

**utils ldap config** {*fqdn*| *ipaddr*}

**Syntax Description**

| Parameters | Description |
|---|---|
| *fqdn* | Configures the system to use an FQDN for LDAP authentication. |
| *ipaddr* | Configures the system to use an IP address for LDAP authentication |

**Command Modes** Administrator (admin:)

**Usage Guidelines**

- **utils ldap config fqdn**—This command is preferred for LDAP authentication, however, you can only use this command if DNS is configured on the system; if the system is not configured to use DNS, use **utils ldap config ipaddr**.
- **utils ldap config ipaddr**—This command is not preferred and should only be used if the system is not, or can not be, configured to use DNS; if the system is configured to use DNS, use **utils ldap config fqdn**.

### Requirements

Applies to: Unified CM and Cisco Unity Connection

# utils network*

## utils network arp delete

This command deletes an entry in the Address Resolution Protocol table.

**utils network arp delete** *host*

**Syntax Description**

| Parameters | Description |
|---|---|
| *host* | (Optional) Represents the host name or IP address of the host to delete from the table. |

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

### Delete example

```
admin:utils network arp delete myhost
```

## utils network arp set

This command sets an entry in the Address Resolution Protocol table.

**utils network arp set** {*host*} {*addr*}

**Syntax Description**

| Parameters | Description |
|---|---|
| *host* | Represents the host name or IP address of the host to add to the table. |
| *addr* | Represents the hardware address (MAC) of the host to be added in the format: XX:XX:XX:XX:XX:XX |

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

### Set example

```
admin:utils network arp set myhost 11:22:33:44:55:66
```

## utils network arp list

This command lists the contents of the Address Resolution Protocol table.

**utils network arp list host** *hostname* [ *options* ]

**Syntax Description**

| Parameters | Description |
|---|---|
| **host** | |
| *hostname* | |
| *options* | (Optional) page, numeric<br>• Page: Pauses to display the output one page at a time.<br>• Numeric: Shows hosts as dotted IP addresses. |

**Command Modes** Administrator (admin:)

**Usage Guidelines** In the Flags column, C=cached, M=permanent, P=published.

### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

### List example

```
admin:admin: utils network arp listAddress HWtype HWaddress
Flags Mask Iface
sjc21-3f-hsrp.cisco.com ether 00:00:0C:07:AC:71 C
eth0
philly.cisco.com ether 00:D0:B7:85:98:8E C
```

```
eth0
Entries: 2 Skipped: 0 Found: 2
```

## utils network capture

This command captures IP packets on the specified Ethernet interface.

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

### Syntax Description

| Parameters | Description |
|---|---|
| **eth0** | Specifies Ethernet interface 0. |
| *page* | (Optional) Displays the output one page at a time.<br>When you use the page or file options, the complete capture of all requested packets must occur before the command completes. |
| *numeric* | (Optional) Displays hosts as dotted IP addresses. |
| **file** *fname* | (Optional) Outputs the information to a file.<br>The file option saves the information to `platform/cli/fname.cap`. The filename cannot contain the "." character. |
| **count***num* | (Optional) Sets a count of the number of packets to capture.<br>For screen output, the maximum count equals 1000, and, for file output, the maximum count equals 10,000. |
| **size***bytes* | (Optional) Sets the number of bytes of the packet to capture.<br>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* | (Optional) Specifies the source address of the packet as a host name or IPV4 address. |
| **dest***addr* | (Optional) Specifies the destination address of the packet as a host name or IPV4 address. |
| **port***num* | (Optional) Specifies the port number of the packet, either source or destination. |

### Command Modes

Administrator (admin:)

#### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

## utils network connectivity

This command verifies the node network connection to the first node in the cluster. Be aware that this connection is only valid on a subsequent node.

**utils network connectivity** [**reset**] [ *hostname/ip address* ]

**Syntax Description**

| Parameters | Description |
|---|---|
| **connectivity** | This command verifies the node network connection to the first node in the cluster. |
| **reset** | (Optional) Clears previous return codes. |
| *hostname/ip address* | (Optional) Hostname or ip address of cluster node. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

## utils network host

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

**utils network host** *name* [**server**| *serv*] **[page] [detail] [srv]**

**Syntax Description**

| Parameters | Description |
|---|---|
| *name* | Represents the host name or IP address that you want to resolve. |
| *serv* | (Optional) Specifies an alternate domain name server. |
| **[page]** | (Optional) Displays the output one screen at a time. |
| **[detail]** | (Optional) Displays a detailed listing. |
| **[srv]** | (Optional) Displays DNS SRV records. |

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

## utils network ipv6 host

This command does an IPv6 host lookup (or IPv6 address lookup) for the specified host name or IPv6 address.

**Note** IPv6 is not supported in Cisco Unified Communications Manager Business Edition 5000.

**utils network ipv6 host** {*host_name*| *ipv6_address*}

**Syntax Description**

| Parameters | Description |
|---|---|
| *host_name* | Specifies the name of the server. |
| *ipv6_address* | Specifies the IPv6 address of the server. |

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM and Cisco Unity Connection.

## utils network ipv6 traceroute

This command to traces an IPv6 address or hostname.

**Note** IPv6 is not supported in Cisco Unified Communications Manager Business Edition 5000.

**utils network ipv6 traceroute** [*ipv6-address*| *hostname*]

**Syntax Description**

| Parameters | Description |
|---|---|
| *ipv6-address* | Specifies IPv6 address that you want to trace. |
| *hostname* | Specifies the host name that you want to trace. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM and Cisco Unity Connection.

## utils network ipv6 ping

This command allows you to ping an IPv6 address or hostname.

**Note** IPv6 is not supported in Cisco Unified Communications Manager Business Edition 5000.

**utils network ipv6 ping** *destination* [ *count* ]

**Syntax Description**

| Parameters | Description |
|---|---|
| *destination* | Specifies a valid IPv6 address or host name that you want to ping. |
| [ *count* ] | Specifies the number of times to ping the external server. The default count equals 4. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM and Cisco Unity Connection.

## utils network ping

This command allows you to ping another server.

**utils network ping** *destination* [ *count* ]

**Syntax Description**

| Parameters | Description |
|---|---|
| *destination* | Represents the ip address or host name of the server that you want to ping. |
| [ *count* ] | Specifies the number of times to ping the external server. The default count equals 4. |

**Command Modes**

Administrator (admin:)

### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

## utils network traceroute

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

**utils network traceroute** [ *destination* ]

**Syntax Description**

| Parameters | Description |
|---|---|
| *destination* | Represents the hostname or IP address of the server to which you want to send a trace. |

**Command Modes**

Administrator (admin:)

### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection.

# utils ntp*

## utils ntp config

This command displays the current configuration of the NTP client and server.

**Note** To avoid potential compatibility, accuracy, and network jitter problems, the external NTP servers that you specify for the primary node should be NTP v4 (version 4). If you are using IPv6 addressing, external NTP servers must be NTP v4.

**utils ntp config**

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence server on Unified CM, Cisco Unity Connection

## utils ntp restart

This command restarts the NTP service.

**utils ntp restart**

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection

## utils ntp server list

This command lists all NTP servers.

**utils ntp server list**

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: IM and Presence server on Unified CM

## utils ntp start

This command starts the NTP service if it is not already running.

**Note** You can not stop the NTP service from the command line interface. Use this command when the utils ntp status command returns stopped.

**utils ntp start**

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence server on Unified CM, and Cisco Unity Connection

## utils ntp status

This command displays the current status of NTP.

**utils ntp status**

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level:

Allowed during upgrade:

Applies to: IM and Presence service on Unified CM.

# utils os*

## utils os kerneldump

This command configures kerneldump to provide a kernel crash dumping mechanism. The kernel captures the dump to the local disk, in case of a kernel crash.

The MCS-7835-H2 and MCS-7845-H2 models do not support this command.

**Note** The netdump commands have been removed from release 8.6(1) and have been replaced with the kerneldump commands.

**utils os kerneldump** {**enable**| **disable**}

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

If a kernel crash occurs, the capture kernel dumps th core on the local disk of the server. The primary kernel reserves 128MB of physical memory that the capture kernel uses to boot. The kerneldump uses **kexec** command to boot into a capture kernel whenever the kernel crashes.

### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM and Cisco Unity Connection

### Example

```
admin: utils os kerneldump enable
***************WARNING******************
Enabling kerneldump requires system reboot
Would you like to boot the machine (y/n):y
kerneldump enable operation succeeded
System going for a reboot
```

## utils os kerneldump ssh

This command enables, disables, or displays the status of an external SSH server.

**utils os kerneldump ssh** {**enable**| **disable**| **status**}

**Syntax Description**

| Parameters | Description |
|---|---|
| **enable** | Configures an external SSH server as a kerneldump server to kernel dumps. |

| Parameters | Description |
|---|---|
| **disable** | Removes support of the external SSH server that is configured to collect kernel dumps. |
| **status** | Indicates whether an external SSH server is configured or not, to collect kernel dumps. |

**Command Modes** Administrator (admin:)

**Usage Guidelines** If external SSH server has the kerneldump service enabled and a kernel crash occurs, the capture kernel dumps the core on the external server that is configured to collect the dump. Enabling and disabling kerneldump require a system reboot for the changes to come into effect.

#### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM and Cisco Unity Connection

#### Example

```
admin: utils os kerneldump ssh disable 10.77.31.60
Disabling kerneldump requires system reboot
Would you like to continue (y/n): y
kerneldump disable operation succeeded
System going for a reboot
```

## utils os secure

This command is used to specify the level of security provided by selinux.

**utils os secure** {**enforce**| **permissive**| **status**}

**Syntax Description**

| Parameters | Description |
|---|---|
| **enforce** | |
| **permissive** | |
| **status** | |

**Command Modes** Administrator (admin:)

**Usage Guidelines** Note that selinux does not handle rate limiting. Rate limiting is handled by ipprefs and ip tables.

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: IM and Presence service on Unified CM

# utils remote_account*

## utils remote_account create

This command creates a remote account.

**utils remote_account create**

**Command Modes** Administrator (admin:)

**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.

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## utils remote_account disable

This command allows you to disable a remote account.

**utils remote_account disable**

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection

## utils remote_account enable

This command allows you to enable a remote account.

**utils remote_account enable**

**Command Modes** Administrator (admin:)

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

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection

### utils remote_account status

This command allows you to check the status of a remote account.

**utils remote_account status**

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection

## utils service*

### utils service

This command activates, deactivates, starts, stops, or restarts a service.

**utils service** {**activate**| **deactivate**| **start**| **stop**| **restart**} *service_name*

## Syntax Description

| Parameters | Description |
|---|---|
| *service_name* | Represents the name of the service you want to affect:<br>• System NTP<br>• System SSH<br>• Service Manager<br>• A Cisco DB<br>• Cisco Tomcat<br>• Cisco Database Layer Monitor<br>• Cisco Unified Serviceability<br>**Note** The following list of services are applicable to IM and Presence only.<br>• Cisco SIP Proxy<br>• Cisco Presence Engine<br>• Cisco Sync Agent<br>• Cisco XCP Router<br>• Cisco XCP Text Conference Manager<br>• Cisco XCP Web Connection Manager<br>• Cisco XCP Connection Manager<br>• Cisco XCP SIP Federation Connection Manager<br>• Cisco XCP XMPP Federation Connection Manager<br>• Cisco XCP Config Manager<br>• Cisco XCP Message Archiver<br>• Cisco XCP Directory Service<br>• Cisco XCP Authentication Service |

## Command Modes

Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection

### utils service list

This command retrieves a list of all services.

**utils service list [page]**

**Syntax Description**

| Parameters | Description |
|---|---|
| **[page]** | Displays the output one page at a time. |

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: IM and Presence service on Unified CM

## utils snmp*

### utils snmp config 1/2c community-string

This interactive command adds, deletes, lists or updates a community string.

**utils snmp config 1/2c community-string** {**add | delete | list | update**}

**Syntax Description**

| Parameters | Description |
|---|---|
| **add** | Adds a new community string. |
| **delete** | Deletes a community string. |
| **list** | Lists all community strings. |
| **update** | Updates a community string. |

**Command Modes** Administrator (admin:)

**Usage Guidelines** The system prompts you for the parameters.

The SNMP Master Agent service is restarted for configuration changes to take effect. Do not abort command after execution until restart is complete. If the command is aborted during service restart, verify service status of "SNMP Master Agent" by using `utils service list`. If service is down, start it by using `utils service start SNMP Master Agent`

#### Requirements

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## utils snmp config 1/2c inform

This interactive command adds, deletes, lists or updates inform notification destinations.

**utils snmp config 1/2c inform** {**add | delete | list | update**}

**Syntax Description**

| Parameters | Description |
|---|---|
| **add** | Adds a notification destination. |
| **delete** | Deletes a notification destination. |
| **list** | Lists all notification destinations. |
| **update** | Updates a notification destination. |

**Command Modes** Administrator (admin:)

#### Requirements

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## utils snmp config 1/2c trap

This interactive command affects trap notifications.

**utils snmp config 1/2c trap** {**add| delete| list| update**}

**Syntax Description**

| Parameters | Description |
|---|---|
| **add** | Adds a new v1/2c trap notification destination associated with a configured v1/2c community string. |
| **delete** | Deletes the configuration information for an existing v1/2c trap notification destination. |
| **list** | Lists the v1/2c trap notifications currently configured. |

| Parameters | Description |
|---|---|
| **update** | Updates configuration information for an existing v1/2c trap notification destination. |

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM and Cisco Unity Connection

## utils snmp config 3 inform

This interactive command affects the v3 inform notification.

**utils snmp config 3 inform** {**add | delete | list | update**}

**Syntax Description**

| Parameters | Description |
|---|---|
| **add** | Adds a new v3 inform notification destination associated with a configured v3 username. |
| **delete** | Deletes the configuration information for an existing v3 inform notification destination. |
| **list** | Lists the v3 inform notifications currently configured. |
| **update** | Updates configuration information for an existing v3 inform notification destination. |

**Command Modes** Administrator (admin:)

**Usage Guidelines** The system prompts you for the parameters.

The SNMP Master Agent service is restarted for configuration changes to take effect. Do not abort command after execution until restart is complete. If the command is aborted during service restart, verify service status of "SNMP Master Agent" by using `utils service list`. If service is down, start it by using `utils service start SNMP Master Agent`

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## utils snmp config mib2

This interactive command affects the Mib2 configuration information.

**utils snmp config mib2** {**add | delete | list | update**}

**Syntax Description**

| Parameters | Description |
|---|---|
| **add** | Adds the Mib2 configuration information. |
| **delete** | Deletes the Mib2 configuration information. |
| **list** | Lists the Mib2 configuration information. |
| **update** | Updates the Mib2 configuration information. |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

The system prompts you for the parameters.

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## utils snmp config 3 trap

This interactive command affects trap notifications.

**utils snmp config 3 trap** {**add | delete | list | update**}

**Syntax Description**

| Parameters | Description |
|---|---|
| **add** | Adds a new v3 trap notification destination associated with a configured v3 username. |
| **delete** | Deletes the configuration information for an existing v 3 trap notification destination. |
| **list** | Lists the v3 trap notifications currently configured. |

| Parameters | Description |
|---|---|
| **update** | Updates configuration information for an existing v3 trap notification destination. |

**Command Modes** Administrator (admin:)

**Usage Guidelines** The system prompts you for the parameters.

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## utils snmp config 3 user

This interactive command affects v3 user configuration.

**utils snmp config 3 user** {**add | delete | list | update**}

**Syntax Description**

| Parameters | Description |
|---|---|
| **add** | Adds a new v3 user with the v3 authentication and privacy passwords. |
| **delete** | Deletes the configuration information for an existing v3 user. |
| **list** | Lists the v3 users currently configured. |
| **update** | Updates configuration information for an existing v3 user. |

**Command Modes** Administrator (admin:)

**Usage Guidelines** The system prompts you for the parameters.

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## utils snmp get

This interactive command gets the SNMP data using the specified version for the specified MIB OID.

**utils snmp get** *version*

**Syntax Description**

| Parameters | Description |
|---|---|
| *version* | Specifies the SNMP version. Possible values include 1, 2c or 3. |
| *community* | Specifies the SNMP community string. |
| *ip-address* | Specifies the IP address of the server. Enter 127.0.0.0 to specify the local host. You can enter the IP address of another node in the cluster to run the command on that node. |
| *object* | Specifies the SNMP Object ID (OID) to get. |
| *file* | Specifies a file in which to save the command output. |

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

If you run the command on a specific OID (leaf) in the MIB you would get the value of the MIB. For example to get the system uptime: `iso.3.6.1.2.1.25.1.1.0 = Timeticks: (19836825) 2 days, 7:06:08.25`

If you provide the IP address of a remote host, the command gets executed on the remote host.

Be aware that the IP address is required. You cannot use a domain name.

### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## utils snmp hardware-agents

This command affects the SNMP agents on the server.

**utils snmp hardware-agents** {**status | start | stop | restart**}

**Syntax Description**

| Parameters | Description |
|---|---|
| **status** | Displays the status of the SNMP agents provided by the vendor of the hardware.<br>**Note** Only agents that provide status get displayed by this command. Not all hardware agents provide status. |
| **stop** | Stops all SNMP agents provided by the hardware vendor. |
| **restart** | Restarts all of the SNMP agents provided by the vendor of the hardware. |
| **start** | Starts all of the SNMP agents provided by the vendor of the hardware. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## utils snmp test

This command sends sample alarms to local syslog, remote syslog and snmp trap.

**utils snmp test**

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

### Example

```
admin: admin:utils snmp test
Service Manager is running
Test SNMP Trap starts with Local Host Name, Specify a Remote Sever Name to test Remote
Syslog
TestAlarmInformational sent [Returncode=0]
TestAlarmEmergency sent [Returncode=0]
TestAlarmAlert sent [returncode=0]
TestAlarmCritical sent [Returncode=0]
TestAlarmDebug sent [Returncode=0]
TestAlarmNotice sent [Returncode=0]
TestAlarmWarning sent [Returncode=0]
TestAlarmError sent [Returncode=0]
TestAlarmWindows sent [Returncode=0]
Message from syslogd@ipcbu-plat44 at Sat Jul 17 03:56:11 2010 ...
ipcbu-plat44 local7 0 : 1: ipcbu-plat44.blr.eng: Jul 16 2010 22:26:11.53 UTC :
%UC_-0-TestAlarmEmergency: %[AppID=Cisco CallManager][ClusterID=][NodeID=ipcbu-plat44]:
Testing EMERGENCY_ALARM
```

## utils snmp walk

This interactive commands walks through the SNMP MIB using the specified version, starting with the specified OID.

**utils snmp walk** *version*

### Syntax Description

| Parameters | Description |
|---|---|
| *version* | Specifies the SNMP version. Possible values include 1, 2c or 3. |
| *community* | Specifies the SNMP community string. |
| *ip-address* | Specifies the IP address of the server. Enter 127.0.0.0 to specify the local host. You can enter the IP address of another node in the cluster to run the command on that node. |
| *object* | Specifies the SNMP Object ID (OID) to walk |
| *file* | Specifies a file in which to save the command output. |

### Command Modes

Administrator (admin:)

#### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

### Example

If you run `snmp walk` on a leaf in the MIB you basically get what you would get with `utils snmp get ...` command. Here in the example we are getting the system's uptime.

```
iso.3.6.1.2.1.1.1.0 = STRING: "Hardware:7825H, 1 Intel(R) Pentium(R) 4 CPU 3.40GHz, 2048
MB Memory: Software:UCOS 2.0.1.0-62"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.9.1.583
iso.3.6.1.2.1.1.3.0 = Timeticks: (15878339) 1 day, 20:06:23.39
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "bldr-ccm34.cisco.com"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
iso.3.6.1.2.1.2.1.0 = INTEGER: 3
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.1.3 = INTEGER: 3
iso.3.6.1.2.1.2.2.1.2.1 = STRING: "lo"
Press <enter> for 1 line, <space> for one page, or <q> to quit
```

# utils system*

## utils system restart

This command allows you to restart the system on the same partition.

**utils system restart**

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

## utils system shutdown

This command allows you to shut down the system.

**utils system shutdown**

**Command Modes** Administrator (admin:)

**Usage Guidelines** This command has a five-minute timeout. If the system does not shut down within five minutes, the command gives you the option of doing a forced shutdown.

### Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unifed CM, Cisco Unity Connection

## utils system switch-version

This command allows you to restart the system on the inactive partition.

**utils system switch-version**

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified CM, IM and Presence service on Unified CM, and Cisco Unity Connection

## utils system boot

This command redirects where the system boot output gets sent.

**utils system boot** {**console**| **serial**}

**Syntax Description**

| Parameters | Description |
|---|---|
| *console* | Redirects the system boot output to the console. |
| *serial* | Redirects the system boot output to the COM1 (serial port 1). |

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified CM and Cisco Unity Connection

## utils system upgrade

This command allows you to install upgrades and Cisco Option (COP) files from both local and remote directories.

**utils system upgrade** {**initiate**| **cancel**| **status**}

## Syntax Description

| Parameters | Description |
|---|---|
| **cancel** | Cancels the active upgrade. |
| **initiate** | Starts a new upgrade wizard or assumes control of an existing upgrade wizard. The wizard prompts you for the location of the upgrade file. |
| **status** | Displays the status of an upgrade. |

## Command Modes

Administrator (admin:)

### Requirements

Applies to: Unified CM, IM and Presence service on Unified CM, Cisco Unity Connection

**utils system***

CHAPTER 8

# Troubleshooting PAWS Management


- SNMP setup, page 211
- Troubleshooting installation, page 221
- Troubleshooting PAWS-M components, page 222
- Alarm management, page 225
- Trace management, page 227


# SNMP setup

SNMP version 3 provides security features such as authentication (verifying that the request comes from a genuine source), privacy (encryption of data), authorization (verifying that the user allows the requested operation), and access control (verifying that the user has access to the objects requested). To prevent SNMP packets from being exposed on the network, you can configure encryption with SNMPv3.

This chapter, which describes how to configure SNMP v3 so the network management system can monitor Cisco PAWS-M, contains the following topics:

## SNMP configuration checklist

The following table provides an overview of the steps for configuring SNMP:

| Configuration steps | | Related Procedures and Topics |
|---|---|---|
| **Step 1** | Install and configure the SNMP NMS. | SNMP product documentation that supports the NMS |

| Configuration steps | | Related Procedures and Topics |
|---|---|---|
| **Step 2** | In the CLI, verify that the system started the SNMP services, including:<br>• SNMP Master Agent<br>• Native Agent<br>• System Application Agent<br>• Cisco Syslog Agent<br>• MIB2 Agent<br>• Host Resources Agent | In the command line interface, enter the following command:<br>utils service list |
| **Step 3** | Configure the SNMP user. | SNMP users, on page 213 |
| **Step 4** | Configure the notification destination for traps or informs. | • SNMP trap notification destinations, on page 215<br>• SNMP inform notification destination, on page 216 |
| **Step 5** | Configure the system contact and location for the MIB2 system group. | MIB2 system group, on page 218 |

| Configuration steps | | Related Procedures and Topics |
|---|---|---|
| **Step 6** | Configure trap settings for CISCO-SYSLOG-MIB. | Use these guidelines to configure CISCO-SYSLOG-MIB trap settings on your system:<br>• Set clogsNotificationEnabled (1.3.6.1.4.1.9.9.41.1.1.2) to true by using the SNMP Set operation; for example, use the net-snmp set utility to set this OID to true from the linux command line using: snmpset -c <community string> -v2c <transmitter ipaddress> 1.3.6.1.4.1.9.9.41.1.1.2.0 i 1<br>You can also use any other SNMP management application for the SNMP Set operation.<br>• Set clogMaxSeverity (1.3.6.1.4.1.9.9.41.1.1.3) value by using the SNMP Set operation; for example, use the net-snmp set utility to set this OID value from the linux command line using: snmpset -c public -v2c 1<transmitter ipaddress> 1.3.6.1.4.1.9.9.41.1.1.3.0 i <value><br>Enter a severity number for the <value> setting. Severity values increase as severity decreases. A value of 1 (Emergency) indicates highest severity, and a value of 8 (Debug) indicates lowest severity. Syslog agent ignores any messages greater than the value that you specify; for example, to trap all syslog messages, use a value of 8. |
| **Step 7** | Restart the SNMP Master Agent service. (Optional)<br>**Tip** The system automatically restarts the SNMP Master Agent after you execute the utils snmp config commands. | At the command line, enter the following command:<br>utils service start SNMP Master Agent |
| **Step 8** | On the NMS, configure the Cisco PAWS-M trap parameters. | • SNMP Management Information Base (MIB), on page 219<br>• SNMP product documentation that supports the NMS |

# SNMP users

The following table shows the commands that you need to work with SNMP users on the Cisco PAWS-M platform:

*Table 14: Trace CLI commands*

| Task | Command |
|---|---|
| List the SNMP users. | utils snmp config user 3 list |
| Add an SNMP user. | utils snmp config user 3 add<br>The system prompts you for the parameters. See the SNMP users, on page 213 table for parameter names and descriptions. |
| Update an SNMP user. | utils snmp config user 3 update<br>The system prompts you for the parameters. See the SNMP users, on page 213 table for parameter names and descriptions. |
| Delete an SNMP user. | utils snmp config user 3 delete<br>The system prompts you for the parameters. See the SNMP users, on page 213 table for parameter names and descriptions. |

### SNMP user CLI parameters

The following table describes the SNMP user parameter settings for V3.

*Table 15: SNMP User Parameter Settings for V3*

| Field | Description |
|---|---|
| username | The name of the user for which you want to provide access. The name can contain up to 32 characters and can contain any combination of alphanumeric characters, hyphens (-), and underscore characters (_).<br>**Tip** Enter users that you have already configured for the network management system (NMS). |
| authprotocol | Authentication protocol. To specify HMAC-SHA, enter SHA. |
| authpassphrase | Specifies the authentication protocol password. The password must contain at least 8 characters. |
| privprotocol | Specifies the privacy protocol, either AES128, AES192, or AES256 |
| privpassphrase | Specifies the privacy protocol password. The password must contain at least 8 characters. |

| Field | Description |
|---|---|
| accessprivilege | Enter one of the following options for the access level:<br>• **ReadOnly**—The user can only read the values of MIB objects.<br>• **ReadWrite**—The user can read and write the values of MIB objects.<br>• **ReadWriteNotify**—The user can read and write the values of MIB objects and send MIB object values for a trap and inform messages.<br>• **NotifyOnly**—The user can only send MIB object values for trap and inform messages.<br>• **ReadNotifyOnly**—The user can read values of MIB objects and also send the values for trap and inform messages.<br>• **None**—The user cannot read, write, or send trap information.<br>**Tip** To change the trap configuration parameters, you need to configure a user with NotifyOnly, ReadNotifyOnly, or ReadWriteNotify privileges. |
| ipaddress1 | Specify an IP address from which to accept packets. The default specifies to accept packets from all hosts. |
| ipaddress2 | Specify an IP address from which to accept packets. The default specifies to accept packets from all hosts. |

# SNMP trap notification destinations

An SNMP agent sends notifications to NMS in the form of traps or informs to identify important system events. Traps do not receive acknowledgments from the destination whereas informs do receive acknowledgments.

The following section applies to SNMP V3 notification destination configuration.

The following table shows the commands that you need to work with SNMP trap notification destinations on the PAWS-M platform:

***Table 16: SNMP Trap Notification Destinations CLI commands***

| Task | Command |
|---|---|
| List trap notification destinations. | utils snmp config trap 3 list |

| Task | Command |
|---|---|
| Add a v3 trap notification destination that is associated with a configured v3 username. | utils snmp config trap 3 add<br>The system prompts you for the parameters. See the SNMP trap notification destinations, on page 215 table for parameter names and descriptions. |
| Update a trap notification destination. | utils snmp config trap 3 update<br>The system prompts you for the parameters. See the SNMP trap notification destinations, on page 215 table for parameter names and descriptions. |
| Delete a trap notification destination. | utils snmp config trap 3 delete<br>The system prompts you for the parameters. See the SNMP trap notification destinations, on page 215 table for parameter names and descriptions. |

### Trap Notification Destination Parameter settings

The following table describes the trap notification destination parameter settings for V3.

***Table 17: Trap Notification Destination Parameter Settings for V3***

| Field | Description |
|---|---|
| ipaddress | The host IP address of the notification destination. |
| portno | The notification-receiving port number on the destination server. |
| oldportno | The notification-receiving port number on the destination server that is currently configured. |
| newportno | The notification-receiving port number on the destination server that you want to use when updating the trap notification destination. |
| username | Specifies the SNMP user associated to the notification destination. |

# SNMP inform notification destination

An SNMP agent sends notifications to NMS in the form of traps or informs to identify important system events. Traps do not receive acknowledgments from the destination whereas informs do receive events. Traps do not receive acknowledgments from the destination whereas informs do receive acknowledgments.

The following table describes the inform notification destination configuration settings for V3.

*Table 18: SNMP inform notification destination CLI commands*

| Task | Command |
|---|---|
| List inform notification destinations. | utils snmp config inform 3 list |
| Add a v3 inform notification destination. | utils snmp config inform 3 add<br>The system prompts you for the parameters. See SNMP inform notification destination, on page 216 for parameter names and descriptions. |
| Update an inform notification destination. | utils snmp config inform 3 update<br>The system prompts you for the parameters. See SNMP inform notification destination, on page 216 for parameter names and descriptions. |
| Delete an inform notification destination. | utils snmp config inform 3 delete<br>The system prompts you for the parameters. See SNMP inform notification destination, on page 216 for parameter names and descriptions. |

### Inform notification destination parameter settings

*Table 19: Inform notification destination parameter settings for V3*

| Field | Description |
|---|---|
| ipaddress | The host IP address of the notification destination. |
| portno | The notification-receiving port number on the destination server. |
| oldportno | The notification-receiving port number on the destination server that is currently configured. |
| newportno | The notification-receiving port number on the destination server that you want to use when updating the inform notification destination. |
| username | Specifies the SNMP user associated to the notification destination. |
| oldusername | Specifies the v3 username that is currently associated with the inform. |
| newusername | Specifies the v3 username that you want to associate with the inform. |

| Field | Description |
|---|---|
| deleteuserconf | Specifies confirmation for deleting the old user, either Y or N. |
| authprotocol | Authentication protocol. To specify HMAC-SHA, enter SHA. |
| authpassphrase | Specifies the authentication protocol password. The password must contain at least 8 characters. |
| privprotocol | Specifies the privacy protocol, either AES128, AES192, or AES256 |
| privpassphrase | Specifies the privacy protocol password. The password must contain at least 8 characters. |
| accessprivilege | Enter one of the following options for the access level:<br>• **ReadWriteNotify**—The user can read and write the values of MIB objects and send MIB object values for a trap and inform messages.<br>• **NotifyOnly**—The user can only send MIB object values for trap and inform messages.<br>• **ReadNotifyOnly**—The user can read values of MIB objects and also send the values for trap and inform messages. |
| engineId | Specifies the remote engine ID of the server to which to send inform messages. |

# MIB2 system group

You can use the CLI to configure the system contact and system location objects for the MIB-II system group. For example, you could enter Administrator, 555-121-6633, for the system contact and San Jose, Bldg 23, 2nd floor, for the system location.

The following table shows the commands that you need to work with MIB2 system groups on the Cisco IME server:

***Table 20: MIB2 CLI commands***

| Task | Command |
|---|---|
| List the MIB2 system group configuration. | utils snmp config mib2 list |

| Task | Command |
|---|---|
| Add a MIB2 system group. | utils snmp config mib2 add<br>The system prompts you for the parameters. See MIB2 system group, on page 218 for parameter names and descriptions. |
| Update a MIB2 system group. | utils snmp config mib2 update<br>The system prompts you for the parameters. See MIB2 system group, on page 218 for parameter names and descriptions. |
| Delete a MIB2 system group. | utils snmp config mib2 delete<br>The system prompts you for the parameters. See MIB2 system group, on page 218 for parameter names and descriptions. |

### MIB2 system group CLI parameters

*Table 21: MIB2 system group CLI parameter settings*

| Field | Description |
|---|---|
| Server | The server for which you want to configure contacts. |
| SysContact | Specifies a person to notify when problems occur. |
| SysLocation | Specifies the location of the person that is identified as the system contact. |

# SNMP Management Information Base (MIB)

SNMP allows access to Management Information Base (MIB), which is a collection of information that is organized hierarchically. MIBs comprise managed objects, which are identified by object identifiers. A MIB object, which contains specific characteristics of a managed device, comprises one or more object instances (variables).

The SNMP interface provides these Cisco Standard MIBs:

- CISCO-CDP-MIB
- CISCO-SYSLOG-MIB

The Simple Network Management Protocol (SNMP) extension agent resides in the server. The SNMP interface also provides these Industry Standard MIBs:

- SYSAPPL-MIB

- MIB-II (RFC 1213)
- HOST-RESOURCES-MIB

Cisco PAWS-M SNMP Interface supports the following MIBs.

### CISCO-CDP-MIB

Use the CDP subagent to read the Cisco Discovery Protocol MIB, CISCO-CDP-MIB. This MIB enables Cisco PAWS-M to advertise itself to other Cisco devices on the network.

The CDP subagent implements the CDP-MIB. The CDP-MIB contains the following objects:

- cdpInterfaceIfIndex
- cdpInterfaceMessageInterval
- cdpInterfaceEnable
- cdpInterfaceGroup
- cdpInterfacePort
- cdpGlobalRun
- cdpGlobalMessageInterval
- cdpGlobalHoldTime
- cdpGlobalLastChange
- cdpGobalDeviceId
- cdpGlobalDeviceIdFormat
- cdpGlobalDeviceIdFormatCpd

### SYSAPPL-MIB

Use the System Application Agent to get information from the SYSAPPL-MIB, such as installed applications, application components, and processes that are running on the system.

System Application Agent supports the following object groups of SYSAPPL-MIB:

- sysApplInstallPkg
- sysApplRun
- sysApplMap
- sysApplInstallElmt
- sysApplElmtRun

### MIB-II

Use MIB2 agent to get information from MIB-II. The MIB2 agent provides access to variables that are defined in RFC 1213, such as interfaces, IP, and so on, and supports the following groups of objects:

- system
- interfaces

- at
- ip
- icmp
- tcp
- udp
- snmp

### HOST-RESOURCES MIB

Use Host Resources Agent to get values from HOST-RESOURCES-MIB. The Host Resources Agent provides SNMP access to host information, such as storage resources, process tables, device information, and installed software base. The Host Resources Agent supports the following groups of objects:

- hrSystem
- hrStorage
- hrDevice
- hrSWRun
- hrSWRunPerf
- hrSWInstalled

### CISCO-SYSLOG-MIB

Syslog tracks and logs all system messages, from informational through critical. With this MIB, network management applications can receive syslog messages as SNMP traps.

The Cisco Syslog Agent supports trap functionality with the following MIB objects:

- clogNotificationsSent
- clogNotificationsEnabled
- clogMaxSeverity
- clogMsgIgnores
- clogMsgDrops

# Troubleshooting installation

Use the following sections to troubleshoot problems that occur during installation of the Cisco PAWS-M:

- Manage network errors during installation, on page 222
- Examine log files, on page 222

# Manage network errors during installation

During the installation process, the installation program verifies that the server can successfully connect to the network by using the network configuration that you enter. If the server cannot connect, a message appears; you get prompted to select one of the following options:

- **RETRY** —The installation program tries to validate networking again. If validation fails again, the error dialog box appears again.
- **REVIEW (Check Install)**—This option allows you to review and modify the networking configuration. When detected, the installation program returns to the network configuration windows. Networking is validated after you complete each networking window, so the message may appear multiple times.
- **HALT**— The installation halts. You can copy the installation log files to a USB disk to aid troubleshooting of your network configuration.
- **IGNORE** —The installation continues. The networking error gets logged. In some cases, the installation program validates networking multiple times, so this error dialog box may appear multiple times. If you choose to ignore network errors, the installation may fail.

# Examine log files

If you encounter problems with the installation, you may be able to examine the install log files by entering the following commands in Command Line Interface.

To obtain a list of install log files from the command line, enter

**CLI> file list install ***

To view the log file from the command line, enter

**CLI> file view install** *log_file*

where:

log_file specifies a log file name having the format: install_log_YYYY-MM-DD.HH.MM.SS.log in which the date and time of the log file is the time at which the install or the upgrade was initiated on the system.

You can get more information about installation events by viewing or downloading the System History log. Refer to the following for more information: System History Log section in the Cisco Intercompany Media Engine Installation and Configuration Guide.

# Troubleshooting PAWS-M components

Use the following sections to troubleshoot problems with Cisco PAWS-M components:

- Troubleshoot PAWS-M services, on page 223
- Troubleshoot PAWS-M administrative interface, on page 225

# Troubleshoot PAWS-M services

The following table lists the troubleshooting steps to perform for Cisco PAWS-M.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Check to see that the Cisco Platform Manager service is running. | Services, on page 17 |
| **Step 2** | Check for communication problems between the servers. | Configuration checklist for PAWS Management, on page 46 |
| **Step 3** | If you have an issue with an upgrade task, check the server type in the server group. For Upgrade Tasks, publisher server and subscriber servers cannot be in the same group. | Manage server groups, on page 49<br>Failed COP file install or UC application server upgrade section below |
| **Step 4** | Check PAWS-M error messages. | Common PAWS-M errors section below |
| **Step 5** | Check the Platform Manager Log Files. | PAWS-M Log files section below<br>Traces, on page 23 |

## Failed COP file install or UC application server upgrade

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | If the UC application server with the failed upgrade is version 8.6.1, check the server inventory page. Be sure the correct publisher is administered in the publisher field. (This field will not appear if the server is version 8.6.2 or later.) | |
| **Step 2** | If the upgrade (or COP file install) on a UC application server is not successful, obtain the install log files from the UC application server and check for errors. | An upgrade on a UC application server that is scheduled using PAWS-M is performed in the same manner as upgrades done using the UC application server's CLI or GUI interface. Therefore, all normal upgrade troubleshooting logs should be gathered from the UC Application server, to diagnose the problem. |

## Common PAWS-M errors

The following section contains common PAWS-M errors and possible reasons for those errors.

**"Could not contact server" or “Server not available”.**

- All connections between UC applications and PAWS-M must be established before you run a task.
- All UC applications must be contacted at least once prior to the first PAWS-M task run.
- SFTP or FTP and UC Applications must be routable from the PAWS-M; for example, use public IP if NATs are used. Likewise, the SFTP or FTP servers must be routable from the UC Applications.

Go to the UC application server that can not be contacted, and verify that the "Platform Administrative Web Service" is running on the UC application server. See Configuration checklist for PAWS Management, on page 46.

## PAWS-M Log files

When you troubleshoot issues for PAWS-M, you can access the following log files on the PAWS-M platform at the following locations:

- **file get activelog tomcat/logs/platform-api/log4j/***— This log file includes information generated by the UC Applications. The same log file is also stored on the application server. Using this command, you can view:
  - SOAP messages from the Platform Manager to the UC App server - including inputs, results, errors, and messages
- **file get activelog tomcat/logs/pm/log4j/***— This log file includes information from the Platform Manager. Using this command, you can view:
  - REST traffic between the browser and the Platform Manager including inputs, results, errors, and messages
  - SOAP messages to the UC Applications including inputs, results, errors, and messages
  - Database access including updates, queries, and results
  - Task related events like scheduling, starting, and updating tasks
  - Background jobs like synchronization tasks
- If you are troubleshooting communication between PAWS-M and an application server, you can also get these files from the UC application server: **file get activelog tomcat/logs/platform-api/log4j/***— This log file includes information generated by the UC applications. The same log file is also stored on the application server. Using this command, you can view:
  - SOAP messages from the Platform Manager including inputs, results, errors, and messages
  - Calls to underlying OS components like the upgrade scripts

# Troubleshoot PAWS-M administrative interface

The following table lists the troubleshooting steps to perform for the Administrative Interface.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Check to see that the following services are running:<br>• Cisco Tomcat<br>• Cisco Platform Manager | Services, on page 17 |
| **Step 2** | Check the following log file: **activelog tomcat/logs/pm/log4j** | Troubleshoot PAWS-M services, on page 223<br>Trace management, on page 227<br>Traces, on page 23 |

# Alarm management

Alarms provide information on runtime status and the state of the system, so you can troubleshoot problems that are associated with your system; for example, to identify issues with the Disaster Recovery System. Alarm information, which includes an explanation and recommended action, also includes the application name, machine name, and so on, to help you perform troubleshooting.

You configure the alarm interface to send alarm information to multiple locations, and each location can have its own alarm event level (from debug to emergency). Alarms can go to the Syslog Viewer (local syslog), Syslog file (remote syslog), SNMP traps, or to all destinations.

When a service issues an alarm, the alarm interface sends the alarm information to the locations that you configure (and that are specified in the routing list in the alarm definition). The system can either forward the alarm information, as is the case with SNMP traps, or the system can write the alarm information to its final destination (such as a log file).

As soon as you enter the CLI command, the system will prompt you for the required parameters. Enter the values to see the output.

The following table shows the commands that you need to work with alarms on the Cisco PAWS-M platform:

*Table 22: Alarm CLI commands*

| Task | Command |
|---|---|
| Display the alarm configuration for a specific service/list of all services | show alarm<br>Required Parameter:<br>*servicename*—Name of the service. It can contain multiple words.<br>Example:<br>Enter the servicename as *all* to show the alarm configurations of all the services.<br>Enter the servicename as *Cisco Tomcat* to show the alarm configuration of Cisco Tomcat service. |
| Enable/Disable alarms for a particular destination | set alarm *status*<br>Required Parameters:<br>*status*—enable or disable.<br>*servicename*—Name of the service. It can contain multiple words.<br>*monitorname*—SDI, SDL, Event_Log, or Sys_Log. |
| Enable alarms for a remote Syslog server | set alarm remotesyslogserver<br>Required Parameters:<br>*servicename*—Name of the service. It can contain multiple words.<br>*servername*—Name of the remote syslog server. |

| Task | Command |
|---|---|
| Set the event level for an alarm | set alarm *severity*<br>Required Parameters:<br>*servicename*—Name of the service. It can contain multiple words.<br>*monitorname*—SDI, SDL, Event_Log, or Sys_Log.<br>*severity* equals one of the following:<br>• Emergency—This level designates the system as unusable.<br>• Alert—This level indicates that immediate action is needed.<br>• Critical—The system detects a critical condition.<br>• Error—This level signifies that an error condition exists.<br>• Warning—This level indicates that a warning condition is detected.<br>• Notice—This level designates a normal but significant condition.<br>• Informational—This level designates information messages only.<br>• Debug—This level designates detailed event information that Cisco TAC engineers use for debugging. |
| Set alarm configuration to default values<br>**Tip** This option is available only for service names beginning with Cisco. | set alarm default<br>Required Parameters:<br>*servicename*—Name of the service. It can contain multiple words. |

# Trace management

Traces assist you in troubleshooting issues with your application. You use the CLI to specify the level of information that you want traced as well the type of information that you want to be included in each log file. You can configure trace parameters for any service on the Cisco PAWS-M platform.

After you have configured information that you want to include in the log files for the various services, you can collect and view log files through log collection. To do this, configure trace using set trace CLI command.

You can configure the level of information that you want traced (debug level), what information you want to trace (trace fields), and information about the trace files (such as number of files per service, size of file, and time that the data is stored in the log files)

### Trace configuration

You use the command line interface (CLI) to enable and disable tracing as well as to configure trace settings for specific services on the Cisco PAWS-M platform. As soon as you enter the CLI command, the system prompts you for the required parameters. For more information regarding trace collection, see the Trace management, on page 227.

The following table shows the commands that you need to work with traces on the Cisco PAWS-M platform:

***Table 23: Trace CLI commands***

| Task | Command |
|---|---|
| Display the trace configuration for a specified service | show trace<br>Required Parameter:<br>*servicename*—Name of the service. It can contain multiple words.<br>Example:<br>Enter the servicename as *all* to show the trace configurations of all the services.<br>Enter the servicename as *Cisco AMC Service* to show the trace configuration of Cisco AMC service. |
| Display the trace levels available for a specified service | show tracelevels<br>Required Parameter:<br>*servicename*—Name of the service. It can contain multiple words. |
| Enable/Disable trace for a specified service | set trace *status*<br>Required Parameters:<br>*status*— enable or disable<br>*servicename*—Name of the service. It can contain multiple words. |
| Specify the debug trace level settings for a specified service | set trace *tracelevel*<br>Required Parameters:<br>*tracelevel*—Use show tracelevels CLI command to find the trace levels for a given servicename.<br>*servicename*—Name of the service. It can contain multiple words. |

| Task | Command |
|---|---|
| Specify the maximum size of a trace files for a specific service from 1 to 10 megabytes | set trace maxfilesize<br>Required Parameters:<br>*servicename*—Name of the service. It can contain multiple words.<br>*size*—Maximum size of the trace files from 1 to 10 megabytes. |
| Specify the maximum number of log files per service.<br>The system automatically appends a sequence number to the file name to indicate which file it is; for example, cus299.txt. When the last file in the sequence is full, the trace data begins writing over the first file. | set trace maxnumfiles<br>Required Parameters:<br>*servicename*—Name of the service. It can contain multiple words.<br>*filecount*—Number of trace files from 1 to 10000. |
| Set the user categories flag to the value provided, for a specified service.<br>**Tip** This option is available only for service names beginning with Cisco. | set trace usercategories<br>Required Parameters:<br>*flagnumber*—Hexadecimal value from 0 to 7FFF. 7FFF means all the flags are enabled.<br>*servicename*—Name of the service. It can contain multiple words. |
| Set trace configuration to default values for a specified service.<br>**Tip** This option is available only for service names beginning with Cisco. | set trace default<br>Required Parameter:<br>*servicename*—Name of the service. It can contain multiple words. |

### Log collection

You can collect log files by performing any of the following tasks:

- To view the log files directly from the CLI, enter the following the CLI commands:
  - file list
  - file view
  - file search
- To bundle the various log files and send them to the local SFTP directory, enter the CLI command file get. Then, use a SFTP client to obtain the .tar files and send to the team that troubleshoots.