Command Line Interface (CLI) Reference Guide for Cisco Unified Presence Release 8.0, 8.5, and 8.6

April 30, 2013

The command line interface (CLI), which you can access from the console or through a secure shell connection to the server, provides a subset of the operating system functionality that is available through the operating system user interface.

This appendix describes the CLI commands that you can use on the Cisco Unified Operating System to perform basic operating system functions. The Cisco Unified Operating System Administration application also makes these functions available.

Keep in mind that the CLI commands are designed for system emergencies and not as a replacement for the user interface. Typically, you would use the CLI only when a problem occurs while you are using the Cisco Unified Operating System Administration interface.

How to Work with the CLI

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Starting a CLI Session

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

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

Before You Begin

Ensure you have the following information that is 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 Unified Operating System.

Procedure

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

a. From a remote system, use SSH to connect securely to the Cisco Unified Operating System. 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**.

b. From a direct connection, you receive this prompt automatically:

ipt-1 login:

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

Enter the administrator ID that was defined during installation.

Step 2 Enter the password that was defined at installation.

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

```
admin:
```

You can now use any CLI command.

Completing Commands

To complete commands, use **Tab**:

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

Getting Help on Commands

You can get two kinds of help about 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

If you want to:	At the CLI prompt:
Get detailed help	Enter **help** *command* Where *command* specifies the command name or the command and parameter. See Example 1.
Query only command syntax	Enter *command***?** Where *command* represents the command name or the command and parameter. See Example 2.

Troubleshooting Tips

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

Example 1 Detailed Help Example:

```
admin:help file list activelog

activelog help:
This will list active logging files

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

file-spec can contain '*' as wildcards

Example:
admin:file list activelog platform detail
02 Dec,2004 12:00:59      <dir>    drf
02 Dec,2004 12:00:59      <dir>    log
```

```
16 Nov,2004 21:45:43        8,557  enGui.log
27 Oct,2004 11:54:33       47,916  startup.log
dir count = 2, file count = 2
```

Example 2 Query Example:

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

Exiting a Command with the Ctrl-C Key Sequence

You can stop most interactive commands by entering the Ctrl-C key sequence, as shown in the following example:

Example 3 Exiting a Command with Ctrl-C

```
admin:utils system upgrade initiate
Warning: Do not close this window without first exiting the upgrade command.
Source:
1) Remote Filesystem
2) DVD/CD
q) quit
Please select an option (1 - 2 or "q" ):
Exiting upgrade command. Please wait...
Control-C pressed
admin:
```

Note If you execute the command **utils system switch-version** and enter **Yes** to start the process, entering Ctrl-C exits the command but does not stop the switch-version process.

Ending a CLI Session

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

Delete Commands

delete account

This command allows you to delete an administrator account.

Command Syntax

delete account *account-name*

Parameters

- *account-name*—Represents the name of an administrator account.

Requirements

Command privilege level: 4

Allowed during upgrade: No

delete dns

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

Command Syntax

delete dns *ip-address*

Parameters

- *ip-address*—Represents the IP address of the DNS server that you want to delete.

Usage Guidelines

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

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

delete process

This command allows you to delete a particular process.

Command Syntax

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

Parameter

- *process-id*—Represents the process ID number.

Options

- **force**—Causes the process to stop
- **terminate**—Causes the operating system to terminate the process
- **crash**—Crashes the process and produces a crash dump

Usage Guidelines

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

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

delete smtp

This command allows you to delete the SMTP host.

Command Syntax

delete smtp

Requirements

Command privilege level: 1

Allowed during upgrade: No

File Commands

file check

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

Command Syntax

file check [*detection-size-kb*]

Options

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

Usage Guidelines

The command notifies you about a possible impact to system performance and requests confirmation that you want to continue.

Caution Because running this command can affect system performance, we recommend that you run the command during off-peak hours.

The display includes both deleted and new files.

Defaults

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

Requirements

Command privilege level: 0

Allowed during upgrade: No

file delete

This command deletes one or more files.

Command Syntax

file delete

activelog *directory/filename* {**detail** | **noconfirm**}

inactivelog *directory/filename* {**detail** | **noconfirm**}

install *directory/filename* {**detail** | **noconfirm**}

license *directory/filename* {**detail** | **noconfirm**}

Parameters

- **activelog—**Specifies a log on the active side.
- **inactivelog—**Specifies a log on the inactive side.
- **install—**Specifies an installation log.
- *directory/filename*—Specifies the path and filename of the file(s) to delete. You can use the wildcard character, *, for *filename*.

Options

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

Usage Guidelines

Caution You can only recover a deleted file using the Disaster Recovery System.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Example

The following example deletes the install log.

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

The following example deletes the license file.

```
file delete license <licName>.lic
```

file dump

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

Command Syntax

file dump

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

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

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

Parameters

- **activelog—**Specifies a log on the active side.
- **inactivelog—**Specifies a log on the inactive side.
- **install—**Specifies an installation log.
- *directory/filename***—**Specifies the path and filename of the file to dump. You can use the wildcard character, *, for *filename* as long as it resolves to one file.

Options

- **detail**—Displays listing with the date and time
- **hex**—Displays output in hexadecimal

Requirements

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

Allowed during upgrade: Yes

Example

This command dumps contents of file _cdrIndex.idx.

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

file fragmentation sdl

This command displays file fragmentation information about SDL log files.

Command Syntax

file fragmentation sdl

all *outfilename*

file *filename* {**verbose**}

most fragmented *number*

most recent *number*

Parameters

- **all—**Records information about all files in the directory in the file that is specified by *outfilename*.
- **file—**Displays information about the file that is specified by *filename*.
- **most fragmented—**Displays information about the most fragmented files.
- **most recent—**Displays information about the most recently logged fragmented file.
- *number***—**Specifies the number of files to list.

Options

- **verbose**—Displays more detailed information

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

file get

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

Command Syntax

file get

activelog *directory/filename* [**reltime**] [**abstime**] [**match**] [**recurs**]

inactivelog *directory/filename* [**reltime**] [**abstime**] [**match**] [**recurs**]

install *directory/filename* [**reltime**] [**abstime**] [**match**] [**recurs**]

Parameters

- **activelog—**Specifies a log on the active side.
- **inactivelog—**Specifies a log on the inactive side.
- **install—**Specifies an installation log.
- *directory/filename***—**Specifies the path to the file(s) to delete. You can use the wildcard character, *, for *filename* as long as it resolves to one file.

Options

- **abstime**—Absolute time period, specified as *hh:mm:MM/DD/YY hh:mm:MM/DD/YY*
- **reltime**—Relative time period, specified as **minutes | hours | days | weeks | months** *value*
- **match**—Match a particular string in the filename, specified as *string value*
- **recurs**—Get all files, including subdirectories

Usage Guidelines

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

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Examples

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

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

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

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

file list

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

Command Syntax

file list

activelog *directory* [**page**] [**detail**] [**reverse**] [**date | size**]

inactivelog *directory* [**page**] [**detail**] [**reverse**] [**date | size**]

install *directory* [**page**] [**detail**] [**reverse**] [**date | size**]

license *directory* [**page**] [**detail**] [**reverse**] [**date | size**]

Parameters

- **activelog—**Specifies a log on the active side.
- **inactivelog—**Specifies a log on the inactive side.
- **install—**Specifies an installation log.
- *directory***—**Specifies the path to the directory to list. You can use a wildcard character, *, for *directory* as long as it resolves to one directory.

Options

- **detail**—Long listing with date and time
- **date**—Sort by date
- **size**—Sort by file size
- **reverse**—Reverse sort direction

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

Requirements

Command privilege level: 1 for logs

Allowed during upgrade: Yes

Examples

This example lists operating system log files with details.

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

This example lists directories in CDR repository.

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

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

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

This example lists the names of the licenses.

```
file list license *
```

file search

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

Command Syntax

file search

activelog *directory/filename reg-exp* [**abstime** *hh*:*mm*:*ss mm*/*dd*/*yyyy hh*:*mm*:*ss mm*/*dd*/*yyyy*] [**ignorecase**] [**reltime** {**days** | **hours** | **minutes**} *timevalue*]

inactivelog *directory/filename reg-exp* [**abstime** *hh*:*mm*:*ss mm*/*dd*/*yyyy hh*:*mm*:*ss mm*/*dd*/*yyyy*] [**ignorecase**] [**reltime** {**days** | **hours** | **minutes**} *timevalue*]

install *directory/filename reg-exp* [**abstime** *hh*:*mm*:*ss mm*/*dd*/*yyyy hh*:*mm*:*ss mm*/*dd*/*yyyy*] [**ignorecase**] [**reltime** {**days** | **hours** | **minutes**} *timevalue*]

Parameters

- **activelog—**Specifies a log on the active side.
- **inactivelog—**Specifies a log on the inactive side.
- **install—**Specifies an installation log.
- *reg-exp***—**Represents a regular expression.
- *directory/filename***—**Represents the path to the file(s) to search. You can use the wildcard character, *, to represent all or part of the filename.

Options

- **abstime**—Specifies which files to search based on file creation time. Enter a start time and an end time.
- **days|hours|minutes**—Specifies whether the file age is in days, hours, or minutes.
- **ignorecase**—Ignores case when searching.

- **reltime**—Specifies which files to search based on file creation time. Enter the age of files to search.
- *hh*:*mm*:*ss mm*/*dd*/*yyyy*—An absolute time, in the format hours:minutes:seconds month/day/year.
- *timevalue*—The age of files to search. Specify the unit of this value with the {**days** | **hours** | **minutes**} option.

Usage Guidelines

Write the search term in the form of a regular expression, which is a special text string for describing a search pattern.

If the search term is found in only one file, the filename appears at the top of the output. If the search term is found in multiple files, each line of the output begins with the filename in which the matching line was found.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Example

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

file tail

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

Command Syntax

file tail

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

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

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

Parameters

- **activelog—**Specifies a log on the active side.
- **inactivelog—**Specifies a log on the inactive side.
- **install—**Specifies an installation log.
- *directory/filename***—**Specifies the path to the file to tail. You can use the wildcard character, *, for filename as long as it resolves to one file.

Options

- **detail**—Long listing with date and time
- **hex**—Hexadecimal listing
- **lines**—Number of lines to display

Requirements

Command privilege level: 1 for logs

Allowed during upgrade: Yes

Example

This example tails the operating system CLI log file.

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

file view

This command displays the contents of a file.

Command Syntax

file view

activelog *directory/filename*

inactivelog *directory/filename*

install *directory/filename*

license *directory/filename*

Parameters

- **activelog—**Specifies a log on the active side.
- **inactivelog—**Specifies a log on the inactive side.
- **install—**Specifies an installation log.
- *directory/filename***—**Specifies the path to the file to view. You can use the wildcard character, *, for *filename* as long as it resolves to one file.

Usage Guidelines

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

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Examples

This example displays the install log.

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

This example displays a particular CDR file.

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

This example displays the contents of the license file.

```
file view license <licName>.lic
```

Run Commands

- run sql, page 15

run pe sql

Cisco Unified Presence Release 8.6(3) and Earlier

This command allows you to run an input SQL statement against the specified TimesTen datastore.

Command Syntax

run pe sql *database-name sql-statement*

Parameters

- *database-name*—Represents the name of the TimesTen datastore.
- *sql_statement*—Represents the SQL command to run.

Example

This example runs an SQL command against the TimesTen datastore.

```
run pe sql tthard select * from package
```

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Cisco Unified Presence Release 8.6(4) and Later

This command allows you to run an input SQL statement against the specified datastore.

Command Syntax

run pe sql *datastore-name sql-statement*

Parameters

- *datastore-name*—Represents the name of the datastore.
- *sql_statement*—Represents the SQL command to run.

Example

This example runs an SQL command against the datastore.

```
run pe sql ttroute select * from route
```

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

run sql

This command allows you to run an SQL command.

Command Syntax

run sql *sql_statement*

Parameters

- *sql_statement*—Represents the SQL command to run.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Example

This example runs an SQL command.

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

Set Commands

- set workingdir, page 32

set account

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

Command Syntax

set account *name*

Parameters

- *name*—Represents the username for the new account.

Usage Guidelines

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

Requirements

Command privilege level: 0

Allowed during upgrade: No

set cert

This command affects the certificates available in the preconfigured SFTP location.

Command syntax

set cert

delete *unitname*

Command privilege level:1

Allowed during upgrade:Yes

import [*type*][*name*][*caCert*]

Command privilege level: 1

Allowed during upgrade: Yes

regen [*name*]

Command privilege level: 1

Allowed during upgrade: No

Parameters

- **delete—Deletes the specified file from the specified unit.**
- **import—**Imports the specified certificate for the specified certificate type.
- **regen—**Regenerates the certificate for the specified unit.

Options

- *type*—(mandatory) Specifies the certificate type.

- *unit*— (mandatory) Specifies the name of the trust category, as “own” or “trust”.
- *name*—(mandatory) Represents the unit name.
- *caCert*—(optional) Represents the name of the CA certificate.

Delete Example

```
admin: set cert delete [cup] [ siptest.pem]
```
(Successfully deletes the certificate siptest.pem from the cup trust category)

Import Example

```
admin: set cert import trust tomcat
Successfully imported certificate for tomcat.
Please restart services related to tomcat for the new certificate to become active.
```

Regen Example

```
admin: set cert regen tomcat
Successfully regenerated certificate for tomcat.
```

Requirements

Command privilege level:1

Allowed during upgrade:Yes

set cli pagination

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

Command Syntax

set cli pagination {on | off}

Requirements

Command privilege level: 1

Allowed during upgrade: No

Example

```
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.

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.

Command Syntax

set cli session timeout *minutes*

Parameters

- *minutes*—Specifies the time, in minutes, that can elapse before an active CLI session times out and disconnects (value range is 5-99999 minutes and default value is 30 minutes).

Requirements

Command privilege level: 1

Allowed during upgrade: No

set csr gen

This command regenerates the Certificate Signing Request (CSR) for the specified unit.

Command Syntax

set csr gen ***unitname***

Parameters

- *unitname*—Specifies the unit on which the certificate is generated.

Example

```
admin:set csr gen tomcat
Successfully generated CSR for tomcat
```

set commandcount

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

Command Syntax

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

Parameters

- **enable—**Turns on command count.
- **disable—**Turns off command count.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set logging

This command allows you to enable or disable logging.

Command Syntax

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

Parameters

- **enable—**Turns on logging.
- **disable—**Turns off logging.

Requirements

Command privilege level: 0

Allowed during upgrade: No

set network

This command allows you to configure how your system is connected to the network.

Command Syntax

set network

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

Command privilege level: 1

Allowed during upgrade: No

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

Command privilege level: 1

Allowed during upgrade: No

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

Command privilege level: 0

Allowed during upgrade: Yes

domain *domain-name*

Command privilege level: 1

Allowed during upgrade: No

failover {**enable** | **disable**}

Command privilege level: 1

Allowed during upgrade: No

gateway *ip-address*

Command privilege level: 1

Allowed during upgrade: No

hostname ***hostname***

Command privilege level: 1

Allowed during upgrade: No

ip eth0 *ip-address ip-mask gateway_ip*

Command privilege level: 1

Allowed during upgrade: No

mtu *mtu_max*

Command privilege level: 1

Allowed during upgrade: No

max_ip_conntrack *ip_conntrack_max*

Command privilege level: 1

Allowed during upgrade: No

nic eth0 [**auto en** | **dis**] [**speed 10** | **100**] [**duplex half** | **full**]

Command privilege level: 1

Allowed during upgrade: No

pmtud [**enable** | **disable**]

Command privilege level: 1

Allowed during upgrade: No

restore eth0 *ip-address network-mask gateway*

Command privilege level: 0

Allowed during upgrade: Yes

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

Command privilege level: 1

Allowed during upgrade: No

Parameters

- **dhcp eth0—**Enables or disables DHCP for Ethernet interface 0. You cannot configure Ethernet interface 1. If you continue, this command causes the system to restart.
- **enable—**Enables DHCP, Network Fault Tolerance or Path MTU Discovery.
- **disable—**Disables DHCP, Network Fault Tolerance or Path MTU Discovery.
- *node_ip*—Represents the new 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.
- **dns—**Sets the IP address for the primary or secondary DNS server.
- *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.
- **dns options—**Sets DNS options.
- **domain—**Sets the domain name for the system. If you add, delete or change the domain name using this command, you must regenerate certificates and reboot the server. See the Troubleshooting Tips for more information.
- *domain-name*—Represents the system domain that you want to assign. If you add, delete or change the domain name using this command, you must regenerate certificates and reboot the server. See the Troubleshooting Tips for more information.

- **failover—**Enables and disables Network Fault Tolerance on the Media Convergence Server network interface card.
- **gateway—**Enables you to configure the IP address of the network gateway.
- **hostname—**Sets the network hostname and then causes a restart of the system.
- *hostname***—**Represents the hostname that you wish to assign.
- **ip eth0—**Sets the IP address for Ethernet interface 0. You cannot configure Ethernet interface 1. Cisco Unified Presence does not support changing the IP address. If you change the IP address, Cisco Unified Presence may not function properly.
- *ip-mask***—**Represents the IP mask that you want to assign.
- **mtu—**Sets the maximum MTU value.
- *mtu_max***—**Specifies the maximum MTU value. If you continue, the system will temporarily lose network connectivity.
- **max_ip_conntrack —**Sets the ip_conntrack_max value.
- *ip_conntrack_max***—**Specifies the value for ip_conntrack_max.
- **nic eth0—**Sets the properties of the Ethernet Interface 0. You cannot configure Ethernet interface 1.You can enable only one active NIC at a time. If you continue, this command causes a temporary loss of network connections while the NIC is reset.
- *network_mask***—**Represents the subnet mask for the server.
- **pmtud—**Enables and disables Path MTU Discovery. If you continue, the system will temporarily lose network connectivity.
- **restore—**Configures the specified Ethernet port to use a specified static IP address**.** Only use this command option if you cannot restore network connectivity by using any other **set network** commands. This command deletes all previous network settings for the specified network interface, including Network Fault Tolerance. After running this command, you must restore your previous network configuration manually. The server temporarily loses network connectivity when you run this command. The IP address must be a valid IP address to be assigned to this server.
- **status—**Sets the status of Ethernet 0 to up or down. You cannot configure Ethernet interface 1

Options

- **timeout—**Sets the DNS request timeout.
- *seconds***—**Specifies the DNS timeout period, in seconds.
- **attempts—**Sets the number of times to attempt a DNS request before quitting.
- *number***—**Specifies the number of attempts.
- **rotate—**Causes the system to rotate among the configured DNS servers, distributing the load.
- **auto—**Specifies whether auto negotiation is enabled or disabled.
- **speed—**Specifies whether the speed of the Ethernet connection: 10 or 100 Mbps.
- **duplex—**Specifies half-duplex or full-duplex.

Examples

Example: set network hostname

```
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 24 13:00:21 2008):

The system is going down for restart NOW!
```

Example: set network mtu

```
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...
```

Example: set network pmtud

```
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...
admin:
```

Example: set network restore eth0

```
Example
set network restore eth0   10.94.150.108   255.255.255.0   10.94.150.1
```

Troubleshooting Tips

- 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 relevant chapter of the *Cisco Unified Operating System Maintenance 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.

Usage Guidelines

If you change the NIC speed, NIC duplex, hostname, DHCP, IP address, IP mask, gateway, or primary DNS, the license MAC value will change if the server is hosted on virtual hardware. You must request a new license with the new license MAC value, upload the new license, and restart the License Manager. Cisco recommends that you delete the old license before you request a new one. For more information, see the *Installation Guide for Cisco Unified Presence, Release 8.6*.

set password

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

Command Syntax

set password

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

age maximum: Command privilege level: 1

Allowed during upgrade: No

age minimum: Command privilege level:1

Allowed during upgrade:Yes

age {user admin | user security}

Command privilege level: 1

Allowed during upgrade: No

history *number*

Command privilege level:1

Allowed during upgrade:Yes

Parameters

- **maximum**—Sets the value of the maximum password age for Cisco Unified Operating System administrator accounts in days.
- **minimum**— Sets the value of the minimum password age for Cisco Unified Operating System administrator accounts in days.
- *days*—Specifies the minimum password age, with acceptable values of between 0 - 10. Specifies the maximum password age, which must be greater-than or equal-to 90 days.
- **user admin**—Sets a new administrator password.
- **user security**—Sets a new platform security password. The security password on all nodes in a cluster must match, including Cisco Unified Communication Manager and all Cisco Unified Presence nodes. Once the password has been changed on Cisco Unified Communication Manager, it must be retyped on the Cisco Unified Presence Admin pages in **System->Cisco Unified Communication Manager Publisher** for the communication to re-establish.
- **history**—Specifies the number of passwords that are maintained in the history for Cisco Unified Operating System Administrator accounts. New passwords matching remembered passwords are rejected
- *number*—Specifies the number of passwords (mandatory) to maintain in history
  - To disable, enter 0.

- Default specifies 10.
- Upper limit specifies 20.

Usage Guidelines

The systems prompts you for the old and new passwords.

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

set password complexity character

Note This command only applies to Cisco Unified Presence Release 8.6(4) and later.

This command enables password complexity rules for the type of characters in a password.

Command Syntax

set password complexity character {enable|disable} [*num-chars*]

Parameters

- **enable**—Turns on password complexity for character types
- **disable**—Turns off password complexity for character types

Note When you disable password complexity, you also turn off **password character difference**, **password character max-repeat**, and **password history**.

- ***num-chars***—specifies the number of characters required from each of the four character sets: lowercase, uppercase, numbers, and special characters.
  - Value range: 0-8
  - Default value: 1

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 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 the command.

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 lowercase characters.
- 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

set password complexity character difference

Note This command only applies to Cisco Unified Presence Release 8.6(4) and later.

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.

Command syntax

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

Parameters

- num-chars specifies the number of characters that the character sequence in a new password must differ from the character sequence in the old password.
  - Value range: 0-31

Note The maximum password length is 31 characters.

Usage Guidelines

Enter 0 to indicate no difference.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set password complexity character max-repeat

Note This command only applies to Cisco Unified Presence Release 8.6(4) and later.

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

Command syntax

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

Parameters

- num-repeat specifies the number of times you can consecutively repeat a single character in a new password.
  - Value range: 0-10
  - Default value: 0 (disabled)

Requirements

Command privilege level: 1

Allowed during upgrade: No

set password complexity minimum-length

Note This command only applies to Cisco Unified Presence Release 8.6(4) and later.

This command modifies the value for the minimum password length for Cisco Unified Operating System accounts.

Note Use this command only after you enable password character complexity.

Command Syntax

set password complexity minimum-length ***length***

Parameters

- *length* specifies the minimum number of characters. If password character complexity (see set password complexity character) has been enabled at least once on the system, the value must be greater-than or equal-to 8. Otherwise, if password character complexity has never been enabled on the system, the value must be greater-than or equal-to 6.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

set password expiry

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

Command Syntax

set password expiry

maximum- age {enable | disable}

minimum- age {enable | disable}

user maximum- age {enable | disable} ***userid***

user minimum- age {disable | enable} ***userid***

Parameters

- **enable**—Turns on password expiry and minimum/maximum age settings for the specified Cisco Unified Operating System administrator account. 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 and minimum/maximum age settings for the specified Cisco Unified Operating System administrator account. The set **password expiry disable** command results in Cisco Unified Operating System Administrator accounts never expiring.
- **maximum-age**—Displays the value of the maximum password age for Cisco Unified Operating System administrator accounts in days.
- **minimum-age**— Displays the value of the minimum password age for Cisco Unified Operating System administrator accounts in days.
- *days*—Specifies the minimum password age, with acceptable values of between 0 - 3650 (10 years). Specifies the maximum password age, which must be greater-than or equal-to 90 days.
- **user maximum-age** —Enables or disables the maximum age password expiry for a particular Cisco Unified Operating System Administrator account.
- **user minimum-age**—Enables or disables the minimum age password expiry for a particular Cisco Unified Operating System Administrator account.
- *userid*—Specifies a particular Cisco Unified Operating System Administrator account.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Enable Examples

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

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

Disable Example

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

User Examples

```
admin:set password expiry user
Operation Successful.

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

set replwatcher monitor

This command enables or disables replication monitoring by the Cisco UP Replication Watcher service. The Cisco UP Replication Watcher service blocks other services from starting until database replication is setup and functioning normally.

Command Syntax

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

Parameters

- **enable—**Turns on the replication monitoring service.
- **disable—**Turns off the replication monitoring service.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set smtp

This command sets the SMTP server hostname.

Command Syntax

set smtp *hostname*

Parameters

- *hostname*—Represents the SMTP server name.

Usage Guidelines

If you change the SMTP location, the license MAC value will change if the server is hosted on virtual hardware. You must request a new license with the new license MAC value, upload the new license, and restart the License Manager. Cisco recommends that you delete the old license before you request a new one. For more information, see the *Installation Guide for Cisco Unified Presence, Release 8.6*.

Requirements

Command privilege level: 0

Allowed during upgrade: No

set strace

This command enables or disables the service trace and sets the trace level.

Command Syntax

set strace

enable [**all**] *tracevalue servicename*

disable [**all**] *servicename*

Parameters

- [all]— Optional parameter to propagate the service trace setting change (enable/disable) to all nodes.
- *tracevalue*—Allowed trace values are [Info| Debug | Warn | Error | Fatal]
- *servicename*—Represents the service for which the trace is set (enabled/disabled)

Requirements

Command privilege level: 0

Allowed during upgrade: No

Enable Examples

```
admin: set strace enable Info Cisco UP Sync Agent
Operation Successful.

admin:set strace enable all Debug Cisco UP SIP Proxy
Operation Successful.
```

Disable Example

```
admin: set strace disable Cisco UP Sync Agent
Operation Successful.

admin:set strace disable all Cisco UP SIP Proxy
Operation Successful.
```

set timezone

This command lets you change the system time zone.

Command Syntax

set timezone *timezone*

Parameters

- *timezone*—Specifies the new timezone.

Usage Guidelines

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

If you change the primary node's time zone, the license MAC value will change if the server is hosted on virtual hardware. You must request a new license with the new license MAC value, upload the new license, and restart the License Manager. Cisco recommends that you delete the old license before you request a new one. For more information, see the *Installation Guide for Cisco Unified Presence, Release 8.6*.

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

Requirements

Command privilege level: 0

Allowed during upgrade: No

Example

This example sets the time zone to Pacific time.

```
set timezone Pac
```

set trace

This command sets trace activity for the specified task.

Command Syntax

set trace

enable Error *tname*

enable Special *tname*

enable State_Transition *tname*

enable Significant *tname*

enable Entry_exit *tname*

enable Arbitrary *tname*

enable Detailed *tname*

disable *tname*

Parameters

- *tname*—Represents the task for which you want to enable or disable traces.
- **enable Error**—Sets task trace settings to the error level.
- **enable Special**—Sets task trace settings to the special level.
- **enable State_Transition**—Sets task trace settings to the state transition level.
- **enable Significant**—Sets task trace settings to the significant level.
- **enable Entry_exit** —Sets task trace settings to the entry_exit level.
- **enable Arbitrary**—Sets task trace settings to the arbitrary level.
- **enable Detailed**—Sets task trace settings to the detailed level.
- **disable**—Unsets the task trace settings.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set webapp session timeout

This command sets the time, in minutes, that can elapse before a web application, such as Cisco Unified Presence Administration, times out and logs off the user. For the new webapp session timeout to become effective, you must restart the Cisco Tomcat service. 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 hours.

Tip Until you restart the Cisco Tomcat service, the show webapp session timeout command reflects the new values, but the system continues to use and reflect the old values.

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

Note This command is only supported in Cisco Unified Presence 8.6(4) and later.

Command Syntax

set webapp session timeout *minutes*

Parameters

- *minutes*—Specifies the time, in minutes, that can elapse before a web application times out and logs off the user (Value range is 5-99999 minutes and default value is 30 minutes)

Requirements

Command privilege level: 1

Allowed during upgrade: No

set web-security

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

Command Syntax

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

Parameters

- *orgunit*—Represents the organizational unit (OU) name.

Tip 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.

Note When you set an alternate-host-name parameter with the **set web-security** command, self-signed certificates for tomcat will contain the Subject Alternate Name extension with the alternate-host-name specified. CSR for Cisco Unified Presence will contain Subject Alternate Name Extension with the alternate host name included in the CSR.

Usage Guidelines

If you change the certificate information, the license MAC value will change if the server is hosted on virtual hardware. You must request a new license with the new license MAC value, upload the new license, and restart the License Manager. Cisco recommends that you delete the old license before you request a new one. For more information, see the *Installation Guide for Cisco Unified Presence, Release 8.6*.

Requirements

Command privilege level: 0

Allowed during upgrade: No

Example

This example shows the **set web-security** command with multiple organizational unit names that include commas.

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

In the above example, the certificate will have three OU fields:

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

set workingdir

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

Command Syntax

set workingdir

activelog *directory*

inactivelog *directory*

install *directory*

Parameters

- **activelog**—Sets the working directory for active logs.
- **inactivelog**—Sets the working directory for inactive logs.
- **install**—Sets the working directory for installation logs.
- *directory*—Represents the current working directory.

Requirements

Command privilege level: 0 for logs

Allowed during upgrade: Yes

Show Commands

show account

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

Command Syntax

show account

Requirements

Command privilege level: 4

Allowed during upgrade: Yes

show cert

This command displays certificate contents and certificate trust lists.

Command Syntax

show cert

own *filename*

trust *filename*

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

Parameters

- *filename*—Represents the name of the certificate file.
- **own**—Specifies owned certificates.
- **trust**—Specifies trusted certificates.
- **list**—Specifies a certificate trust list.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Example

This command displays own certificate trust lists.

```
show cert list own
```

show cli pagination

This command displays the status of automatic pagination.

Command Syntax

show cli pagination

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

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.

Command Syntax

show cli session timeout

Parameters

None

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show csr

This command displays Certificate Sign Request (CSR) contents.

Command Syntax

show csr

own ***name***

list {own | trust}

Parameters

- name—Represents the name of the csr file.

- own—Specifies owned csr.
- trust—Specifies trusted csr.

Usage guidelines

Use the **show cert list own** command to obtain the certificate name.

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

show ctl

This command displays the contents of the Certificate Trust List (CTL) file on the server. It notifies you if the CTL is not valid.

Command Syntax

show ctl

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show date

This command displays the date and time on the server.

Command Syntax

show date

Parameters

None

Example

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

show diskusage

This command displays information about disk usage on the server.

Command Syntax

show diskusage

activelog {**filename** *filename* | **directory** | **sort**}

common {**filename** *filename* | **directory** | **sort**}

inactivelog {**filename** *filename* | **directory** | **sort**}

install {**filename** *filename* | **directory** | **sort**}

tftp {**filename** *filename* | **directory** | **sort**}

tmp {**filename** *filename* | **directory** | **sort**}

Parameters

- **activelog**—Displays disk usage information about the activelog directory.
- **common**—Displays disk usage information about the common directory.
- **inactivelog**—Displays disk usage information about the inactivelog directory.
- **install**—Displays disk usage information about the install directory.
- **tftp** —Displays disk usage information about the TFTP directory.
- **tmp**—Displays disk usage information about the TMP directory.

Options

- **filename** *filename*—Saves the output to a file that is specified by *filename*. These files are stored in the **platform/cli** directory. To view saved files, use the **file view activelog** command.
- **directory**—Displays just the directory sizes.
- **sort**—Sorts the output on the basis of file size. File sizes display in 1024-byte blocks.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show environment

This command displays environmental information for three types of hardware components.

Command Syntax

show environment

fans

power-supply

temperatures

Parameters

- **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 temperature values, thresholds, and status.

The output data from the **show environment** command varies between IBM and HP server models.

Requirements

Command Level Privilege: 0

Allowed During Upgrade:Yes

show hardware

This command displays the following information about the platform hardware.

Command Syntax

show hardware

Usage Guidelines

This command displays the following information about the platform hardware:

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

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show itl

This command displays the ITL file contents or prints an error message if the ITL file is not valid.

Command syntax

show itl

Parameters

None

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show logins

This command lists recent logins to the server.

Command Syntax

show logins *number*

Parameters

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

show memory

This command displays information about the onboard memory.

Command Syntax

show memory

count

modules

size

Options

- **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.

Parameters

None

Requirements

Command Level Privilege: 0

Allowed During Upgrade:Yes

show myself

This command displays information about the current account.

Command Syntax

show myself

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show network

This command displays network information.

Command Syntax

show network

eth0 [**detail**]

failover [**detail**] [**page**]

route [**detail**]

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

ip_conntrack

max_ip_conntrack

dhcp eth0 status

all [**detail**]

ipprefs all

ipprefs enabled

ipprefs public

Parameters

- **eth0** specifies Ethernet 0.
- **failover** specifies Network Fault Tolerance information.
- **route** specifies network routing information.
- **status** specifies active Internet connections.
- **ip_conntrack** specifies ip_conntrack usage information.
- **max_ip_conntrack** specifies max_ip_conntrack information.
- **dhcp eth0 status** displays DHCP status information.
- **all** specifies all basic network information.
- **ipprefs all** displays all incoming ports that may be used on Cisco Unified Presence.

- **ipprefs enabled** displays all incoming ports that are currently open.
- **ipprefs public** displays all incoming ports that are currently open for any remote client.

Options

- **detail**—Displays additional information.
- **page**—Displays information 1 page at a time.
- **listen**—Displays only listening sockets
- **process**—Displays the process ID and name of the program to which each socket belongs.
- **all**—Displays both listening and nonlistening sockets.
- **nodns**—Displays numerical addresses without any DNS information.
- **search stext**—Searches for the stext in the output.

Usage Guidelines

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

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Example

This example displays active Internet connections.

```
show network status
```

show open

This command displays open files and ports on the system.

Syntax Description

show open

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

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

Parameters

- **files**—Displays open files on the system.
- **ports**—Displays open ports on the system.

Options

- **all**—Displays all open files or ports
- **process**—Displays open files that belong to the specified process
- *processID*—Specifies a process
- **regexp**—Displays open files or ports that match the specified regular expression
- *reg_exp*—A regular expression

show packages

This command displays the name and version for installed packages.

Command Syntax

show packages

active *name* [**page**]

inactive *name* [**page**]

Parameters

name—Represents the package name. To display all active or inactive packages, use the wildcard character, *.

Options

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

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show password

This command displays the information about the configured password.

Command Syntax

show password

age—Displays information about the configured password age parameters

complexity [character|length]—Displays password complexity or length parameters for OS accounts.

history *number*—Displays the number of passwords that the history maintains for OS administration accounts.

Parameters

- **character**—Displays the status of the password complexity as enabled or disabled.
- **length**—Displays the minimum length of passwords that get used for OS accounts. If password character complexity (see set password complexity character) has been enabled at least once on the system, the default length value is 8. If password complexity has never been enabled, the default value is 6.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show password expiry

This command enables or disables password expiry for Cisco Unified Operating System Administrator accounts.

Command Syntax

show password expiry

{maximum-age *days***| minimum-age** *days***}**

{user maximum-age *userid* **| user minimum-age** *userid***}**

Parameters

- **maximum-age**—Displays the value of the maximum password age for Cisco Unified Operating System administrator accounts in days.
- **minimum-age**— Displays the value of the minimum password age for Cisco Unified Operating System administrator accounts in days.
- *days*—Specifies the minimum password age, with acceptable values of between 0 - 3650 (10 years). Specifies the maximum password age, which must be greater-than or equal-to 90 days.
- **user maximum-age** —Displays the maximum age password expiry for a particular Cisco Unified Operating System Administrator account.
- **user minimum-age**—Displays the minimum age password expiry for a particular Cisco Unified Operating System Administrator account.
- ***userid*—**Displays a particular Cisco Unified Operating System Administrator account.

Requirements

Command privilege level: 0

Allowed during upgrade: No

show pe dbstatus

Note This command only applies to Cisco Unified Presence Release 8.6(3) and earlier.

This command displays the status of the Presence Engine's datastores in the TimesTen database.

Command Syntax

show pe dbstatus

Example

```
show pe dbstatus

**  Datastore: ttsoft **
RAM Residence Policy            : inUse
Replication Agent Policy        : manual
Replication Manually Started    : False
Cache Agent Policy              : manual
Cache Agent Manually Started    : False
```

```
**  Datastore: tthard **
RAM Residence Policy            : inUse
Replication Agent Policy        : manual
Replication Manually Started    : False
Cache Agent Policy              : manual
Cache Agent Manually Started    : False
```

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show pe dbconnections

Note This command only applies to Cisco Unified Presence Release 8.6(3) and earlier.

This command displays the connections to each of the Presence Engine datastores in the TimesTen database.

Command Syntax:

show pe dbconnections

Example

admin:show pe dbconnections

```
...
------------------------------------------------------------------------
Data store /common/tt/db/data/tt60/ttsoft
There are 86 connections to the data store
Data store is in shared mode
Shared Memory KEY 0x04017e6b ID 196612
Type            PID     Context     Connection Name              ConnID
Process         13347   0x0b95f6e8  pe                                1
Process         13347   0x0b9d42f8  pe                               23
Process         13347   0x96452990  pe                               82
Process         13347   0x96500880  pe                               79
Process         13347   0x965718b0  pe                               80
Process         13347   0x965e2918  pe                               81
Process         13347   0x9661e750  pe                               77
Process         13347   0x9668f7b8  pe                               78
Process         13347   0x9673c660  pe                               75
Process         13347   0x967ad6d8  pe                               76
Process         13347   0x967eb008  pe                               72
Process         13347   0x9685a590  pe                               73
Process         13347   0x968cb5f8  pe                               74
Process         13347   0x96908440  pe                               70
```

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show perf

This command displays information about the specified perfmon counter.

Command Syntax

show perf

counterhelp *class-name counter-name*

list

categories.

classes [**cat** *category*] [**detail**]

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

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

query

class *class-name* [,*class-name*...]

counter *class-name counter-name* [,*counter-name*...]

instance *class-name instance-name* [,*instance-name*...]

path *path-spec* [,*path-spec*...]

Parameters

- **counterhelp**—Displays the explanation text for the specified perfmon counter.
- *class-name*—Represents the class name that contains the counter.
- *counter-name*—Represents the counter that you want to view.
- **list**—Displays the information about the perform system.
- **categories**—Lists all categories in the perfmon system.
- **class**—Lists or queries a perfmon class and displays all the instances and counter values of each instance.
- **counter**—Lists or queries perfmon counters for the specified perfmon class.
- **instance**—Lists or queries the perfmon instances for the specified perfmon class.
- **query**—Displays the information about the perform system.
- **path**—Queries a specified perfmon path.

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

Options

- **detail**—Displays detailed information about the perfmon classes or objects.
- **cat** *category*—Displays perfmon classes for the specified category.
- *class-name*—Specifies the perfmon class that you want to query. You can specify a maximum of 5 classes per command.
- *counter-name*—Specifies the counter to view. You can specify a maximum of 5 counters per command.

- *instance-name*—Specifies the perfmon instance to view. You can specify a maximum of 5 instances per command. This command does not apply to singleton perfmon classes.
- *path-spec*—You can specify a maximum of 5 paths per command.
  - For an instance-based perfmon class, specify *path-spec* as *class-name*(*instance-name*)*counter-name*.
  - For a noninstance-based perfmon class (a singleton), specify *path-spec* as *class-name**counter-name*.

Example

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

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show process

This command displays process and load information.

Command Syntax

show process

load [**cont**] [**clear**] [**noidle**] [**num** *xx*] [**thread**] [**cpu**] [**memory**] [**time**] [**specified**] [**page**]

list [**page**] [**short**] [**detail**] [**thread**] [**fd**] [**cont**] [**clear**] [**process id** *id*] [**argument id** *id*] [**owner name** *name*]

Parameters

- **load**—Displays the CPU load for each active process.
- **list**—Displays all processes.

Options

- **cont**—Command repeats continuously
- **clear**—Clears screen before displaying output
- **noidle**—Ignore idle or zombie processes
- **num** *xx*—Sets the number of processes to display (Default=10, **all** = all processes)
- **thread**—Displays threads
- **cpu**—Displays output by CPU usage
- **memory**—Sorts output by memory usage
- **short**—Displays short listing
- **time**—Sorts output by time usage
- **page**—Displays one page at a time
- **detail**—Displays a detailed listing
- **process id** *id*—Shows only specific process number or command name

- **argument name** *name*—Show only specific process with argument name
- **thread**—Include thread processes in the listing
- **fd**—Show file descriptors that are associated with a process

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Example

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

```
show process list detail page
```

show registry

This command displays the contents of the registry.

Command Syntax

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

Parameters

- *system*—(mandatory) Represents the registry system name.
- *component*—(mandatory) Represents the registry component name.
- *name*—(optional) Represents the name of the parameter to show.

Note To display all items, enter the wildcard character, *.

Options

- *page*— Displays one page at a time.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Example

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

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

show risdb

This command displays RIS database table information.

Command Syntax

show risdb

list [**file** *filename*]

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

Parameters

- **list**—Displays the tables supported in the Realtime Information Service (RIS) database.
- **query**—Displays the contents of the RIS tables.

Options

file *filename*—Outputs the information to a file

Note The file option saves the information to platform/cli/*filename*.txt. The file name cannot contain the "." character.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Example

This example displays a list of RIS database tables.

```
show risdb list
```

show smtp

This command displays the name of the SMTP host.

Command Syntax

show smtp

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show stats io

This command displays system I/O statistics.

Command Syntax

show stats io [**kilo**] [**detail**] [**page**] [**file** *filename*]

Options

- **kilo**—Displays statistics in kilobytes
- **detail**—Displays detailed statistics on every available device on the system and overrides the kilo option
- **file** *filename*—Outputs the information to a file

Note The file option saves the information to platform/cli/*filename*.txt. The file name cannot contain the "." character.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show status

This command displays basic platform status.

Command Syntax

show status

Usage Guidelines

This command displays the following basic platform status:

- Host name
- Date
- Time zone
- Locale
- Product version
- Platform version
- CPU usage
- Memory and disk usage

Requirements

Command privilege level: 0

show strace

This command lists the current service trace level.

Command Syntax

show strace *servicename*

Parameters

- *servicename*—Represents the service for which the trace is set (enabled/disabled)

Note If you do not enter any parameters, the command returns a list of available tasks.

Requirements

Command privilege level: 0

Allowed during upgrade: No

Example

```
admin:show strace Cisco UP XCP Router
Trace is enabled
Trace level is set to Info
```

show tech

This command displays the information about the database.

Command Syntax

show tech

activesql

all [**page**] [**file** *filename*]

ccm_service

database dump sessions

dberrcode [*errorcode*]

dbintegrity

dbinuse

dbschema

dbstateinfo

devdefaults

dumpCSVandXML

gateway

locales

network [**page**] [**file** *filename*]

notify

params all

params enterprise

params runtime [all] [cpu] [disk] [env] [memory] [**page**] [**file** *filename*]

params service

prefs

procedures

repltimeout

routepatterns

routeplan

systables

system [all] [bus] [hardware] [host] [kernal] [software] [tools] [**page**] [**file** *filename*]

table *table_name* [**page**] [**csv**]

triggers

version [**page**]

Parameters

- **activesql**—Displays the active queries to the database taken at one minute intervals as far back as the logs allow.
- **all**—Displays the combined output of all **show tech** commands.
- **ccm_service** —Displays information about all Cisco Unified Communications services that can run on the system.
- **database dump** —Creates a CSV file of the entire database.
- **sessions**—Redirects the session and SQL information of the present session IDs to a file.
- **dbintegrity**—Displays the database integrity.
- **dbinuse**—Displays the database in use.
- **dbschema**—Displays the database schema in a CSV file.
- **dbstateinfo**—Displays the state of the database.
- **devdefaults**—Displays the device defaults table.
- **dumpCSVandXML**—displays the device defaults table. collects csv and xml files into a single tar file. You can retrieve the tar file using any of these methods:
  - Enter **file view activelog cm/trace/dbl/xmlcsv.tar** to view the contents of the file.
  - Enter **file get activelog cm/trace/dbl/xmlcsv.tar** to download the file.
  - Use RTMT.
- **gateway**—Displays the gateway table from the database.
- **locales**—Displays the locale information for devices, device pools, and end users.
- **network** [**page**] [**file** *filename*]—Displays network aspects of the server.
- **notify**—Displays the database change notify monitor.
- **params all**—Displays all the database parameters.
- **params enterprise**—Displays the database enterprise parameters.
- **params runtime**—Displays runtime aspects of the server.
- **params service**—Displays the database service parameters.
- **prefs**—Displays database settings.
- **procedures**—Displays the procedures in use for the database.
- **repltimeout**—Displays the replication timeout. When it increases, it ensures that as many servers as possible in a large system will be included in the first round of replication setup. If you have the maximum number of servers and devices, set the replication timeout to the maximum value. Be aware that this will delay the initial set up of replication (giving a chance for all servers to be ready for setup).
- **routepatterns**—Displays the route patterns that are configured for the system.
- **routeplan**—Displays the route plan that are configured for the system.
- **systables**—Displays the name of all tables in the sysmaster database.
- **system**—Displays system aspects of the server.

- **table**—Displays the contents of the specified database table.
- **triggers**—Displays table names and the triggers that are associated with those tables.
- **version**—Displays the version of the installed components.
- *table_name*—Represents the name of the table to display.

Options

- **page**—Displays one page at a time.
- **file** *filename*—Outputs the information to a file.The file option saves the information to platform/cli/*filename*.txt. The file name cannot contain the "." character.
- **errorcode**—Specifies the error code as positive integer. If the error code is a negative number, enter it without the minus sign (-).
- **cpu**—Displays the cpu usage (top) at the time the command is executed.
- **disk**—Displays the disk usage for the system.
- **env**—Displays the runtime environment variables.
- **memory**—Displays disk usage information for the system.
- **bus**—Displays information about the data buses on the server.
- **hardware**—Displays information about the server hardware.
- **host**—Displays information about the server.
- **kernel**—Lists the installed kernel modules.
- **software**—Displays information about the installed software versions.
- **tools**—Displays information about the software tools on the server.
- **csv**—Sends the output to a comma separated values file

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show timezone

This command displays timezone information.

Command Syntax

show timezone

config

list [**page**]

Parameters

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

Options

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

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show trace

This command displays trace information for a particular task.

Command Syntax

show trace [*task_name*]

Parameters

task_name—Represents the name of the task for which you want to display the trace information.

Note If you do not enter any parameters, the command returns a list of available tasks.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Example

This example displays trace information for cdp.

```
show trace cdps
```

show ups status

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

This command provides full status only for 7835-H2 and 7825-H2 servers.

Command Syntax

show ups status

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show version

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

Command Syntax

show version

active

inactive

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show 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.

Command Syntax

show webapp session timeout

Parameters

None

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show web-security

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

Command Syntax

show web-security

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show workingdir

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

Command Syntax

show workingdir

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Unset Commands

unset network dns options

This command unsets DNS options.

Command Syntax

unset network dns options [**timeout**] [**attempts**] [**rotate**]

Parameters

- **timeout**—Sets the wait time before the system considers a DNS query failed to the default.
- **attempts**—Sets the number of DNS attempts to make before failing to the default.
- **rotate**—Sets the method for selecting a nameserver to the default. This affects how loads are distributed across nameservers.

Usage Guidelines

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

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

Utils Commands

utils auditd

This command is used to start or stop the system auditing service. The system auditing service monitors Linux events such as the creation and removal of users, as well as the editing or deleting of files.

Command Syntax

utils auditd [enable | disable | status]

Parameters

- **enable**—Enables the collection of audit logs
- **disable**—Disables the collection of audit logs
- **status**—Provides a status of the audit log collection

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

utils core analyze

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

Command Syntax

utils core [active | inactive] analyze *core file name*

Parameters

- **active**—Specifies an active version
- **inactive**—Specifies an inactive version
- *core file name*—Specifies the name of a core file.

Usage Guidelines

The command creates a file of the same name as the core file, with a .txt extension, in the same directory as the core file. This command works only on the active partition.

Requirements

Command privilege level:1

Allowed during upgrade:Yes

utils core list

This command lists all existing core files.

Command Syntax

utils core [active | inactive] list

Parameters

- **active**—Specifies an active version
- **inactive**—Specifies an inactive version

Requirements

Command privilege level:1

Allowed during upgrade:Yes

utils create report

This command creates reports about the server in the platform/log directory.

Command Syntax

utils create report

hardware

platform

csa

Parameters

- **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 and copies them to a common log location.
- **csa**—Collects all the files required for CSA diagnostics and assembles them ino a single CSA diagnostics file. You can retrieve this file by using the **file get** command.

Usage Guidelines

You are prompted to continue after you enter the command.

After creating a report, use the command **file get activelog platform/log/***filename*, where *filename* specifies the report filename that displays after the command completes, to get the report.

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils csa

This command starts and stops the Cisco Security Agent (CSA).

Command Syntax

utils csa

disable

enable

status

Parameters

- **disable**—Stops the Cisco Security Agent (CSA).
- **enable**—Enables the Cisco Security Agent (CSA). The system prompts you to confirm that you want to enable CSA.
- **status**—Displays the current status of Cisco Security Agent (CSA). The system indicates whether CSA is running.

Caution You must restart the system after you start CSA.

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils dbreplication

This command displays information about database replication.

Command Syntax

utils dbreplication

status

stop [*nodename* | *all*]

repair

reset [*nodename* | *all*]

clusterreset

dropadmindb

forcedatasyncsub

quickaudit [*nodename* | *all*]

repairreplicate *replicatename [nodename* | *all]*]

repairtable *tablename* [*nodename* | *all]*]

runtimestate [*nodename*]

setrepltimeout

Parameters

- **status**—Displays the status of database replication and indicates whether the servers in the cluster are connected and the data is in sync. You should run this command only on the first node (publisher server) of a cluster.

- **stop**—Stops the automatic setup of database replication. Use this command on subscriber and publisher servers prior to executing the CLI command **utils dbreplication reset** or **utils dbreblication clusterreset**. You can run this command on the subscriber servers simultaneously, before you run it on the publisher server.
- **repair**—Repairs database replication.
- **reset**—Resets and restarts database replication. It can be used to tear down and rebuild replication when the system has not set up properly.
- **clusterreset**—Resets replication on an entire cluster. You can use this command to debug database replication. However, you should only use it if you have already tried **utils dbreplication reset all**, and it failed to restart replication on the cluster. This command will tear down and rebuild replication for the entire cluster. Before you run this command, run the command **utils dbreplication stop** first on all subscribers servers and then on the publisher server. After using this command, you must restart each subscriber server. After all subscriber servers have been restarted, you must go to the publisher server and issue the CLI command **utils dbreplication reset all**.
- **dropadmindb**—Drops the Informix syscdr database on any server in the cluster. You should run this command only if database replication reset or cluster reset fails and replication cannot be restarted.
- **forcedatasyncsub**—Forces subscriber nodes to take a backup from the publisher node. Use this command only after you have run the **utils dbreplication repair** command several times, but the **utils dbreplication status** command still shows non-dynamic tables that are not in sync. You can only run this command from the publisher server. Use the *all* parameter to force sync on all subscriber servers in the cluster. If only one subscriber server is out of sync, use the *hostname* parameter. After you run this command, you must restart the restored subscriber servers. This command can take a significant amount of time to execute and can affect the system-wide IOWAIT.

Caution The **utils dbreplication forcedatasyncsub** command erases existing data on the subscriber node.

- **quickaudit**—Runs a quick database check on selected content in dynamic database tables.
- **repairreplicate**—Repairs mismatched data between cluster nodes and changes the data on the node to match the data on the publisher node. It does not repair replication setup. Nodename may not specify the publisher; any subscriber nodename is acceptable. If "all" is specified, the table gets repaired on all subscribers. This command can be executed on publisher.
- *replicatename*—Specifies the replicate to repair.
- **repairtable tablename**—Repairs mismatched table data between cluster nodes and changes the data on the node to match the data on the publisher node. It does not repair replication setup.
- *tablename*—Specifies the table to repair.
- **runtimestate**—Monitors the progress of the database replication process and provides replication state in the cluster.
- **setrepltimeout**—Sets the timeout for replication setup on large clusters. The default database replication timeout equals 5 minutes (value of 300). When the first subscriber server requests replication with the publisher server, the system sets this timer. When the timer expires, the first subscriber server, plus all other subscriber servers that requested replication within that time period, begin data replication with the publisher server in a batch. If you have several subscriber servers, batch replication is more efficient than individual server replication. For large clusters, you can use the command to increase the default timeout value, so that more subscriber servers will be included in the batch. After you upgrade the publisher server and restart it on the upgraded partition, you

should set this timer value before you switch the first subscriber server to the new release. When the first subscriber server requests replication, the publisher server will set the replication timer based on the new value.

Tip We recommend that you restore this value back to the default of 300 (5 minutes) after you finish upgrading the entire cluster, and the subscriber servers have successfully set up replication.

Parameters

- *all*—Causes the audit to be run on all nodes, or the data repair to take place on all subscriber servers, or fix replication on all nodes.
- *nodename*—*S*pecifies the node on which the quick audit should be run, the node on which to repair replication, or the node to monitor.

Requirements

Command privilege level: 0

Allowed during upgrade: No

utils diagnose

This command enables you to diagnose and attempt to automatically fix system problems.

Command Syntax

utils diagnose

fix

list

module *module_name*

test

version

Parameters

- **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.

Options

- *module_name*—Specifies the name of a diagnostics module.

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils disaster_recovery backup

This command backs up files on tape, and on a remote server.

Command Syntax

utils disaster_recovery backup

tape *featurelist device_name*

network *featurelist path servername username*

Parameters

- **tape**—Displays information about the backup files that are stored on a tape.
- *featurelist*—Specifies a list of features to back up, separated by commas.
- *device_name*—Represents the name of the device (mandatory) to back up.
- **network**—Displays information about the backup files that are stored on a remote server.
- *path*—Represents the location of the backup files on the remote server.
- *servername*—Represents the IP address or host name of the server where you stored the backup files.
- *username*—Represents the username that is needed to log in to the remote server.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

utils disaster_recovery cancel_backup

This command cancels the ongoing backup job.

Command Syntax

utils disaster_recovery cancel_backup

Usage Guidelines

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

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

utils disaster_recovery device

This command allows you to manage the devices for backup operations.

Command syntax

utils disaster_recovery device

list

Command privilege level:1

Allowed during upgrade:Yes

delete [*device_name*|*]

Command privilege level:1

Allowed during upgrade:No

add tape *device_name tapeid*

add network *device_name path servername username Number_of_backups*

Parameters

- **list**—Displays the device name, device type and device path for all the backup devices.
- **delete**—Deletes the specified device. *This command deletes all the existing devices except for the ones associated with a schedule.
- **add**— Specifies the new backup devices on which you want to perform backup jobs.
- **tape**—Displays information about the backup files that are stored on a tape.
- **network**—Displays information about the backup files that are stored on a remote server.

Options

- *device_name*—Represents the name of the back up device.
- *tapeid*—Specifies the ID of an available tape device.
- *path*—Represents the location of the backup files on the remote server.
- *servername*—Represents the IP address or host name of the server where the backup files will be stored.
- *username*—Represents the username that is required to log in to the remote server.
- *Number_of_backups*— specifies the number of files to back up.

Requirements

Command privilege level:1

Allowed during upgrade:Yes

utils disaster_recovery restore

This command backs up files on tape, and a remote servers.

Command Syntax

utils disaster_recovery restore

tape *server tarfilename device_name*

network *restore_server tarfilename device_name*

Parameters

- **tape**—Displays information about the backup files that are stored on a tape.
- *server*—Specifies the hostname of the server that you want to restore.

- *tarfilename*—Specifies the name of the file to restore.
- *device_name*—Specifies the name of the device (mandatory) on which to restore files.
- **network**—Displays information about the backup files that are stored on a remote server.
- *restore_server*—Specifies the hostname of the remote server that you want to restore.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

utils disaster_recovery schedule

This command affects schedules that are configured.

Command syntax

utils disaster_recovery schedule

list

Command privilege level:1

Allowed during upgrade:Yes

add *schedulename devicename featurelist datetime frequency*

Command privilege level:1

Allowed during upgrade:No

enable *schedulename*

Command privilege level:1

Allowed during upgrade:No

disable *schedulename*

Command privilege level:1

Allowed during upgrade:No

delete [*schedulename*|*]

Command privilege level:1

Allowed during upgrade:No

Parameters

- **list**—Displays the schedules that are configured.
- **add**—Adds the configured schedules.
- **enable**—Enables the specified schedule.
- **disable**—Disables the specified schedule
- **delete**—Deletes the specified schedule.

Options

- *schedulename*—Represents (mandatory) name of the scheduler.
- *devicename*—Represents (mandatory) name of the device for which scheduling is done

- *featurelist*—Represents (mandatory) comma-separated feature list to backup
- *datetime*—Represents (mandatory) date when the scheduler is set. Format specified (yyyy/mm/dd-hh:mm) 24 hr clock
- *frequency*—Represents (mandatory) frequency at which the scheduler is set to take a backup. Examples: once, daily, weekly and monthly
- * all

List Example

```
admin:utils disaster_recovery schedule list
schedule name device name Schedule Status
----------------------------------------
schedule1      dev1         enabled
schedule2      dev2         disabled
```

Enable Example

```
utils disaster_recovery schedule enable schedule1
Schedule enabled successfully.
```

Disable Example

```
utils disaster_recovery schedule disable schedule1
Schedule disabled successfully.
```

Requirements

Command privilege level:1

Allowed during upgrade:No

utils disaster_recovery show_backupfiles

This command displays information about backup files.

Command Syntax

utils disaster_recovery show_backupfiles

network *path servername username*

tape *tapeid*

Parameters

- **network**—Starts a restore job and takes the backup tar file from a remote server.
- **tape**—Displays information about the backup files that are stored on a tape.
- *path*—Represents the location of the backup files on the remote server.
- *servername*—Represents the IP address or host name of the server where you stored the backup files.
- *tapeid*—Represents the ID of an available tape device.
- *username*—Represents the username that is needed to log in to the remote server.

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils disaster_recovery show_registration

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

Command Syntax

utils disaster_recovery show_registration *hostname*

Parameters

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils disaster_recovery show_tapeid

This command displays a list of tape device IDs.

Command Syntax

utils disaster_recovery show_tapeid

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils disaster_recovery status

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

Command Syntax

utils disaster_recovery status *operation*

Parameters

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils fior

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

Command Syntax

utils fior

disable

enable

list [**start=***date-time*] [**stop=***date-time*]

start

status

stop

top *number* [**read** | **write** | **read-rate** | **write-rate**] [**start=***date-time*] [**stop=***date-time*]

Parameters

- **disable**—Prevents the file I/O reporting service from starting automatically when the machine boots. This command does not stop the service without a reboot. Use the **stop** option to stop the service immediately.
- **enable**—Enables the file I/O reporting service to start automatically when the machine boots. This command does not start the service without a reboot. Use the **start** option to start the service immediately.
- **list**—This command displays a list of file I/O events, in chronological order, from oldest to newest.
- **start**—Starts a previously stopped file I/O reporting service. The service remains in a started state until it is manually stopped or the machine is rebooted.
- **status**—Displays the status of the file I/O reporting service.
- **stop**—Stops the file I/O reporting service. The service remains in a stopped state until it is manually started or the machine is rebooted.
- **top**—Displays a list of top processes that create file I/O. You can sort this list by the total number of bytes read, the total number of bytes written, the rate of bytes read, or the rate of bytes written.
- **start**—Specifies a starting date and time.
- **stop**—Specifies a stopping date and time.
- *date-time*—Specifies a date and time, in any of the following formats: *H*:*M*, *H*:*M*:*S a*, *H*:*M*, *a*, *H*:*M*:*S Y*-*m*-*d*, *H*:*M*, *Y*-*m*-*d*, *H*:*M*:*S*.
- *number*—Specifies how many of the top processes to list.

Options

- **[read | write | read-rate | write-rate]**—Specifies the metric that is used to sort the list of top process.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

utils fips enable

This command allows you to enable FIPS mode. By default, Cisco Unified Presence is in non-FIPS mode. The administrator must enable FIPS mode.

Caution Before enabling FIPS mode, Cisco recommends that you perform a system backup. If FIPS checks fail at start-up, the system halts and requires a recovery CD to be restored.

Consider the following information before you enable FIPS 140-2 mode on Cisco Unified Presence:

- After FIPS mode is enabled on a server, please wait until the server reboots and the services are restarted before enabling FIPS on the next server.
- In FIPS mode, Cisco Unified Presence uses Red Hat Openswan (FIPS validated) in place of Racoon (non-FIPS validated). If the security policies in Racoon contain functions that are not FIPS approved, the CLI command will ask you to redefine the security policies with FIPS approved functions and abort.

Command Syntax

utils fips enable

Note Certificates and SSH key are regenerated automatically, in accordance with FIPS requirements.

Requirements

Command privilege level: 0

Allowed during upgrade: No

utils fips disable

This command allows you to disable FIPS mode.

Consider the following information before you disable FIPS 140-2 mode on Cisco Unified Presence:

- In multiple server clusters, each server must be disabled separately; FIPS mode is not disabled cluster-wide but rather on a per server basis.

Command Syntax

utils fips disable

Note Certificates and SSH key are regenerated automatically, in accordance with FIPS requirements.

Requirements

Command privilege level: 0

Allowed during upgrade: No

utils fips status

This command allows you to check the status of FIPS mode to determine whether FIPS is enabled or disabled.

Command Syntax

utils fips status

Requirements

Command privilege level: 0

Allowed during upgrade: No

utils ha

This command supports high availability (HA) in a subcluster, which means that if a node in the subcluster fails, the Instant Message and Availability services from that node can fail over to the second node in the subcluster, fall back to the first node, and/or be recovered from a Failed state.

Command Syntax

utils ha

failover [node name]

fallback [node name]

recover [subcluster name]

status [subcluster name]

Parameters

- **failover**— Initiates a manual failover for a specified node, where the Cisco UP Server Recovery Manager stops the critical services on the failed node and moves all users to the backup node.
- **fallback**— Initiates a manual fallback for a specified node, where the Cisco UP Server Recovery Manager restarts critical services on the active node and moves users back to the active node.
- **recover**—Initiates a manual recovery for the subcluster (when nodes are in a Failed state) where Cisco Unified Presence restarts the Cisco UP Server Recovery Manager service on that subcluster.
- **status**—Displays the HA status for the subcluster.
- **node name** —*S*pecifies the node on which to perform a manual failover, fallback, or recovery.
- **subcluster name** —*S*pecifies the subcluster on which to monitor HA status. If no Subcluster Name is provided all cluster information is displayed.

Failover Example

```
admin: ha failover shorty-cups
Initiate Manual Failover for Node >shorty-cups<
Request SUCCESSFUL.
Subcluster Name: DefaultCUPSubCluster
Node 1 Name : kal-cup1 State: Taking Over Reason: On Admin Request
Node 2 Name : shorty-cups State: Failing Over Reason: On Admin Request
```

Fallback Example

```
admin: ha fallback shorty-cups
```

```
Initiate Manual fallback for Node >shorty-cups<
Request SUCCESSFUL.
Subcluster Name: DefaultCUPSubCluster
Node 1 Name : kal-cup1 State: Falling Back Reason: On Admin Request
Node 2 Name : shorty-cups State: Taking Back Reason: On Admin Request
```

Recover Example

```
admin: ha recover DefaultCUPSubcluster
Stopping services... Stopped
Starting services... Started
admin:
```

Status Example - HA Not Enabled

```
admin: ha status
Subcluster Name: DefaultCUPSubCluster
Node 1 Name : kal-cup1 State: Unknown Reason: High Availability Not Enabled
Node 2 Name : shorty-cups State: Unknown Reason: High Availability Not Enabled
```

Status Example - HA Enabled

```
admin: ha status
Subcluster Name: DefaultCUPSubCluster
Node 1 Name : kal-cup1 State: Normal Reason: Normal
Node 2 Name : shorty-cups State: Normal Reason: Normal
```

Status Example - Critical Service Down

```
admin: ha status
Subcluster Name: DefaultCUPSubCluster
Node 1 Name : kal-cup1 State: Failed Over with Critical Services not Running Reason:
Critical Service Down
Node 2 Name : shorty-cups State: Running in Backup Mode Reason: Critical Service Down
```

Status Example - Failed

```
admin: ha status
Subcluster Name: DefaultCUPSubCluster
Node 1 Name : kal-cup1 State: Failed Reason: Critical Service Down
Node 2 Name : shorty-cups State: Failed Reason: Critical Service Down
```

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.

Command Syntax

utils import config

Parameters

None

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Usage Guidelines

This command can be executed on any VMware deployment.

Step 1 Power on the VM.

Step 2 Use the Answer File Generator (AFG) tool (http://www.cisco.com/web/cuc_afg/index.html) to create a platformConfig.xml file.

Step 3 Insert the Config.xml file into a virtual floppy instance (see http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1739 for directions).

Step 4 Mount the .flp file in the floppy drive of the new VM.

Step 5 Log into the CLI of the VM (using console or SSH) and execute the `utils import config` command.
The command cycles through all of the data found in the xml file and if data is found that is different than what is currently set on the VM, it modifies the VM to match the new data.

Step 6 The system reboots with the new identity.
When you first sign-in to the Cisco Unified Presence Administration GUI, the post-install wizard will run. This is the same post-install wizard that runs after a fresh installation is completed. You need to identify the Cisco Unified Communications Manager you want Cisco Unified Presence to point to.

utils iostat

This command displays the iostat output for the given number of iterations and interval.

Command Syntax

utils iostat [*interval* | *iterations* | *filename*]

Options

- *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 iteration parameter.
- *filename*—Redirects the output to a file.

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils iothrottle

This command allows you to manage and monitor IO throttling on the server.

Command Syntax

utils iothrottle

disable

enable

status

Parameters

- **disable**—Disables I/O throttling enhancements. This could adversely affect the system during upgrades.
- **enable**—Enables I/O throttling enhancements. When enabled, I/O throttling enhancements lower the impact of upgrades on an active system.
- **status**—Displays the status of I/O throttling enhancements.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

utils netdump

This command configures the netdump client and server.

Command Syntax

utils netdump

client

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

status

stop

server

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

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

list-clients

start

status

stop

Parameters

- **client**—Configures the netdump client.
- **start**—Starts the netdump client or server.
- **status**—Displays the status of the netdump client or server.
- **stop**—Stops the netdump client or server.
- *ip-address-of-netdump-server*—Specifies the IP address of the netdump server to which the client will send diagnostic information.
- **server**—Configures the netdump server.
- **add-client**—Adds a netdump client.

- *ip-address-of-netdump-client*—Specifies the IP address of a netdump client.
- **delete-client**—Deletes a netdump client.
- **list-clients**—Lists the clients that are registered with this netdump server.

Usage Guidelines

- In the event of a kernel panic crash, the netdump client sends diagnostic information about the crash to a netdump server.
- The system stores netdump diagnostic information in the following location on the netdump server: *crash/*. The subdirectories whose names comprise a client IP address and a date contain netdump information.
- You can configure each Cisco Unified Operating System server as both a netdump client and server.
- If the server is on another Cisco Unified Operating System server, only the kernel panic trace signature is sent to the server; otherwise, an entire core dump is sent.

Requirements

Command privilege level: 0

Allowed during upgrade: No

utils network arp

This command lists the contents of the Address Resolution Protocol (ARP) table.

Command Syntax

utils network arp

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

set {*host*} {*address*}

delete *host*

Parameters

- **list**—Lists the contents of the address resolution protocol table.
- **set**—Sets an entry in the address resolution protocol table.
- **delete**—Deletes an entry in the address resolution table.
- *host*—Represents the host name or IP address of the host to add or delete in the table.
- *address*—Represents the MAC address of the host to be added. Enter the MAC address in the following format: XX:XX:XX:XX:XX:XX.

Options

- **page**—Displays the output one page at a time
- **numeric**—Displays hosts as dotted IP addresses

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

List Usage Guidelines

In the Flags column, C=cached, M=permanent, P=published.

List Example

```
admin: utils network arp list
Address                  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
```

Set Example

```
admin: utils network arp set myhost 11:22:33:44:55:66
```

Delete Example

```
admin: utils network arp delete myhost
```

utils network capture eth0

This command captures IP packets on the specified Ethernet interface.

Command Syntax

utils network capture

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

Parameters

- **eth0**—Specifies Ethernet interface 0.

Options

- **page**—Displays the output one page at a time.When you use the page or file options, the complete capture of all requested packets must occur before the command completes.
- **numeric**—Displays hosts as dotted IP addresses
- **file** *fname*—Outputs the information to a file. The file option saves the information to platform/cli/*fname*.cap. The filename cannot contain the "." character.
- **count** *num*—Sets a count of the number of packets to capture

  For screen output, the maximum count equals 1000, and, for file output, the maximum count equals 10,000.
- **size** *bytes*—Sets the number of bytes of the packet to capture

  For screen output, the maximum number of bytes equals 128, for file output, the maximum of bytes can be any number or **ALL**
- **src** *addr*—Specifies the source address of the packet as a host name or IPV4 address
- **dest** *addr*—Specifies the destination address of the packet as a host name or IPV4 address
- **port** *num*—Specifies the port number of the packet, either source or destination

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils network host

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

Command Syntax

utils network host

hostname [**server** *server-name*] [**page**] [**detail**] [**srv**]

Parameters

- *hostname*—Represents the host name or IP address that you want to resolve.

Options

- *server-name*—Specifies an alternate domain name server
- **page**—Displays the output one screen at a time
- **detail**—Displays a detailed listing
- **srv**—Displays DNS SRV records.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils network ipv4 firewall

This commands sets options and displays status for the IPv4 firewall.

Command Syntax

utils network ipv4 firewall

debug [**off**|*time*]

disable [*time*]

enable

list

status

Parameters

- **debug**—Turns debugging on or off. If you do not enter the *time* parameter, this command turns on debugging for 5 minutes.
- **disable**—Turns off the IPv4 firewall. If you do not enter the *time* parameter, this command disables the firewall for 5 minutes.
- **enable**—Turns on the IPv4 firewall.
- **list**—Displays the current configuration of the firewall.
- **status**—Displays the current status of the firewall.

Options

- *time* sets duration for the command in one of the following formats:
  - Minutes: 0–1440m
  - Hours: 0–23h
  - Hours and minutes: 0–23h 0–60m

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils network

This command monitors network communication and traffic.

Command Syntax

utils network

ping *destination* [*count*]

tracert *destination*

Parameters

- **ping**—Allows you to ping another server.
- **tracert**—Traces IP packets that are sent to a remote destination.
- *destination*—Represents the hostname or IP address of the server that you want to ping or trace.

Options

- *count*—Specifies the number of times to ping the external server. The default count equals 4.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils nscd

This command allows you to manage the network service cache daemon (nscd)

Command Syntax

utils nscd

restart

status

Parameters

- **restart**—Restarts the nscd.
- **tracert**—Tests the nscd.

utils ntp

This command displays the NTP status or configuration.

Command Syntax

utils ntp {**status** | **config**}

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

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils ntp config

This command displays the current configuration of the NTP client and server.

Command Syntax

utils ntp config

Parameters

None

utils ntp restart

This command restarts the NTP service.

Command Syntax

utils ntp restart

Parameters

None

Requirements

Level privilege: 0

Command privilege: 0

Allowed during upgrade: Yes

utils ntp server list

This command lists all NTP servers.

Note This command is only valid on Cisco Unified Presence Release 8.5 and 8.6.

Command Syntax

utils ntp server list

Parameters

None

Requirements

Level privilege: 0

Command privilege: 0

Allowed during upgrade: Yes

utils ntp start

If it is not already running, this command starts the NTP service.

Note You cannot stop the NTP service from the command line interface. Use this command when the **utils ntp status** command returns **stopped**.

Command Syntax

utils ntp start

Parameters

None

Requirements

Level privilege: 0

Command privilege: 0

Allowed during upgrade: Yes

utils ntp status

This command displays the current status of NTP.

Command Syntax

utils ntp status

Parameters

None

utils pe replication-agent

Note This command only applies to Cisco Unified Presence Release 8.6(3) and earlier.

This command is used to manage the replication agent for the Presence Engine (PE).

Command Syntax

utils pe replication-agent

start

stop

Parameters

- **start**—Manually starts the replication agent for the soft-state datastore in the Presence Engine.
- **stop**—Manually stops the replication agent for the soft-state datastore in the Presence Engine.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

utils remote_account

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

Command Syntax

utils remote_account

status

enable

disable

create *username life*

Parameters

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

Usage Guidelines

A remote account generates a pass phrase that allows Cisco Systems support personnel to get access to the system for the specified life of the account. You can have only one remote account that is enabled at a time.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Example

```
utils remote_account status
```

utils reset_ui_administrator_name

This command resets the Administrator user name that you use to log in the administration user interface for the installed product.

Command Syntax

utils reset_ui_administrator_name

Usage Guidelines

If this user name is reset, you must manually update the user name of the Cisco Ajax XMPP Libraries (AXL) on each intercluster peer (if any) to match it: Select **Cisco Unified Presence Administration > Presence > Inter-clustering**.

utils reset_ui_administrator_password

This command resets the Administrator password that you use to log in the administration user interface for the installed product.

Command Syntax

utils reset_ui_administrator_password

Usage Guidelines

If this password is reset, you must manually update the Cisco Ajax XMPP Libraries (AXL) on each intercluster peer (if any) to match it: Select **Cisco Unified Presence Administration > Presence > Inter-clustering**.

utils service

This command stops, starts, or restarts a service, and retrieves a list of all services and their status.

Command Syntax

utils service

list [**page**]

start *service-name*

stop *service-name*

restart *service-name*

auto-restart {**enable** | **disable** | **show**} *service-name*

Parameters

- *service-name* represents the name of the service that you want to stop or start:
  - System SSH

  - Service Manager
  - A Cisco DB
  - Cisco Tomcat
  - Cisco Database Layer Monitor
  - Cisco Unified Serviceability
  - Cisco UP SIP Proxy
  - Cisco UP Presence Engine
  - Cisco UP Sync Agent
  - Cisco UP XCP Router
  - Cisco UP XCP Text Conference Manager
  - Cisco UP XCP Web Connection Manager
  - Cisco UP XCP Connection Manager
  - Cisco UP XCP SIP Federation Connection Manager
  - Cisco UP XCP XMPP Federation Connection Manager
  - Cisco UP XCP Counter Aggregator
  - Cisco UP XCP Message Archiver
  - Cisco UP XCP Directory Service
  - Cisco UP XCP Authentication Service
- **enable**—Enables auto-restart.
- **disable**—Disables auto-restart
- **show**—Shows the auto-restart status
- **page**—Displays the output one page at a time

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils snmp

This command manages SNMP on the server.

Command Syntax

utils snmp

get *version*

hardware-agents [**status | start | stop | restart**]

test

walk *version*

Parameters

- **get**—Displays the SNMP data for the specified MIB Object ID (OID). For example: If you run this cmdlet on a specific OID (leaf) in the MIB you 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.
- *version*—Specifies the SNMP version. Possible values include 1, 2c and 3.
- **hardware-agents status**—Displays the status of the hardware agents on the server. Note that only the agents that provide status will display. Not all hardware agents provide status.
- **hardware-agents stop**—Stops all SNMP agents provided by the hardware vendor.
- **hardware-agents restart**—Restarts the hardware agents on the server.
- **hardware-agents start**—Starts all of the SNMP agents provided by the vendor of the hardware.
- **test**—Tests the SNMP host by sending sample alarms to local syslog, remote syslog, and SNMP trap.
- **walk** —Walks through the SNMP MIB, starting with the specified SNMP object.

Test Example

```
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
```

Walk 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 that displays for 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
```

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

utils snmp config

This interactive command affects the v3 inform notification, Mib2 configuration information, trap notifications., and v3 user configuration.

Command Syntax

utils snmp config

inform 3 [add | delete | list | update]

mib 2 [**add | delete | list | update**]

trap 3 [**add | delete | list | update**]

user 3 [**add | delete | list | update**]

Parameters

- **add**—Adds a new v3 inform, trap or user notification destination associated with a configured v3 username. Adds the Mib2 configuration information such as System Contact and System Location.
- **delete**—Deletes the configuration information for an existing v3 inform. trap or user notification destination. Deletes the Mib2 configuration information such as System Contact and System Location.
- **list**—Lists the v3 inform, trap or user notifications currently configured. Lists the Mib2 configuration information such as System Contact and System Location.
- **update**—Updates configuration information for an existing v3 inform, trap or user notification destination. Updates the Mib2 configuration information such as System Contact and System Location.

Usage guidelines - utils snmp config inform 3

The SNMP Master Agent service will be 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

utils soap realtimeservice test

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

Command Syntax

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

Parameters

- *remote-ip*—Specifies the IP address of the server under test.
- *remote-https-user*—Specifies a username with access to the SOAP API.
- *remote-https-password*—Specifies the password for the account with SOAP API access.

Requirements

Command privilege level: 0

Allowed during upgrade: No

utils sso

This command affects SSO based authentication.

Command Syntax

utils sso [enable | disable | status]

Parameters

- **enable**—enables SSO based authentication.
- **disable**—disables SSO based authentication.
- **status**—provides the status of SSO on this node.

Example

The following example makes use of the parameters and values provided in the Configuring Single Sign-On chapter of the *Deployment Guide for Cisco Unified Presence Release 8.6*.

Note The Cisco UP Client Profile Agent option below is only available in Cisco Unified Presence Release 8.6(5) and later and is only applicable to customers using Common Access Card (CAC) sign-on.

```
admin:utils sso enable
    *****WARNING*****
This command will restart Tomcat for successful completion.
This command needs to be executed on all the nodes in the cluster.
Do you want to continue (yes/no): yes
List of apps for which SSO can be enabled:
1) Cisco Unified Presence Administration (CUP Admin, CU Serviceability, CU Reporting)
2) Cisco Unified Operating System Administration (CUOS Admin, DRF)
3) Cisco UP Client Profile Agent
4) RTMT
4) Cisco Unified Presence User Options (CUP User options)

Do you want to enable SSO for Cisco Unified Presence Administration (CUP Admin, CU
Serviceability, CU Reporting) (yes/no): yes
Do you want to enable SSO For Cisco Unified Operating System Administration (CUOS Admin,
DRF) (yes/no): yes
Do you want to enable SSO for Cisco UP Client Profile Agent (yes/no): yes
Do you want to enable SSO for RTMT (yes/no):yes
```

```
Do you want to enable SSO for Cisco Unified Presence User Options (CUP End User options)
(yes/no): yes
Enter URL of the Open Access Manager (OpenAM) server:
https://examplehost.corp.com:8443/opensso
Enter the relative path where the policy agent should be deployed: agentapp
Enter the name of the profile configured for this policy agent: CUPUser
Enter the password of the profile name: ********
Enter the login module instance name configured for Windows Desktop SSO: CUPUser
Validating connectivity and profile with Open Access Manager (OpenAM) Server:
https://examplehost.corp.com:8443/opensso
Valid profile
Valid module name
Enabling SSO ... This will take up to 5 minutes
SSO Enable Success
```

utils system

This command allows you to restart the system on the same partition, restart the system on the inactive partition, or shut down the system.

Command Syntax

utils system {**restart** | **shutdown** | **switch-version**}

Parameters

- **restart**—Restarts the system.
- **shutdown**—Shuts down the system.
- **switch-version**—Switches to the product release that is installed on the inactive partition.

Usage Guidelines

The **utils system shutdown** 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

utils system upgrade

This command allows you to install upgrades and Cisco Option Package (COP) files from both local and remote directories.

Command Syntax

utils system upgrade

cancel

get {**local** | **remote**} *filename*

list {**local** | **remote**] *path*

start

Parameters

- **cancel**—Cancels the active upgrade.
- **get**—Gets an upgrade file from which to upgrade.
- **local**—Specifies that the upgrade files are on a local drive.
- **remote**—Specifies that the upgrade files are on a remote system.
  - *filename* specifies the name of the upgrade file.
  - *path* is the path to the upgrade file(s).
- **list**—Lists the available upgrade files.
- **start**—Starts an upgrade with the upgrade file obtained with the **get** parameter.

utils vmtools status

For information about this command, see the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions Release 8.5(1)*.

utils vmtools upgrade

For information about this command, see the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions Release 8.5(1)*.

Related Documentation

For the latest Cisco Unified Presence requirements, see the *Release Notes for Cisco Unified Presence* at the following URL:
http://www.cisco.com/en/US/products/ps6837/prod_release_notes_list.html