Cisco Intercompany Media Engine Command Line Interface Reference Guide

This document describes the Command Line Interface (CLI) commands that are available for the Cisco Intercompany Media Engine server.

Contents

This document comprises the following sections:

- Starting a CLI Session, page 1
- CLI Basics, page 2
- Generic Commands, page 5
- Add Commands, page 6
- Delete Commands, page 7
- File Commands, page 10
- Set Commands, page 19
- Show Commands, page 67
- Unset Commands, page 119
- Utils Commands, page 120
- Obtaining Documentation and Submitting a Service Request, page 170

Starting a CLI Session

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

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

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

© 2011 Cisco Systems, Inc. All rights reserved.

- You can access the Cisco Unified Communications Operating System CLI directly by using the monitor and keyboard that you used during installation or by using a terminal server that is connected to the serial port. Use this method if a problem exists with the IP address.

Before You Begin

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

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

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

Perform the following steps to start a CLI session:

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

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

  ssh *adminname@hostname*

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

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

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

  ```
  ipt-1 login:
  ```

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

  Enter your administrator ID.

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

Step 2 Enter your password.

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

```
admin:
```

CLI Basics

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

- Completing Commands, page 3
- Getting Help on Commands, page 3
- Ending a CLI Session, page 4

Completing Commands

To complete commands, use **Tab**:

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

Getting Help on Commands

You can get two kinds of help on any command:

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

Procedure

To get detailed help, at the CLI prompt, enter

help *command*

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

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

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

*command***?**

Where *command* represents the command name or the command and parameter. See Example 1-2.

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

Example 1-1 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 1-2 Query Example:

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

Ending a CLI Session

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

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

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
	This pointer highlights an important line of text in an example.

Convention	Description
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords, are in angle brackets.

Notes use the following conventions:

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

Timesavers use the following conventions:

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

Tips use the following conventions:

Tip Means *the information contains useful tips.*

Cautions use the following conventions:

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

Warnings use the following conventions:

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

Generic Commands

- help, page 5
- quit, page 6

help

This command displays help for the specified command.

Requirements

Command privilege level:0

Allowed during upgrade:Unknown

Command syntax

help [*command*]

Parameters

command specifies the command for which help is required.

quit

This command exits the CLI.

Requirements

Command privilege level:0

Allowed during upgrade:Unknown

Command syntax

quit

Parameters

None

Add Commands

- add ime vapserver, page 6
- add ime vapusercredentials, page 7

add ime vapserver

This command adds a vapserver.

Command syntax

add ime vapserver *vapservername* [*portnumber*]

Parameters

- *vapservername* (mandatory) represents the vapserver that will get added.
- *portnumber* (optional) represents the port number of the added vapserver.

Usage Guidelines

- *vapservername* cannot match an existing vapservername name.
  - Use the **show ime vapserver** all to see names that have been assigned.
- *portnumber* cannot match an existing port field for a row in the table. The default value is 5060.
- When the vapserver gets added, the default value for the other vapservers is used. You can change those values by using the **set** command.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

add ime vapusercredentials

This command adds a new user credential to the system.

This user name and password must match the ones that exist on the Unified CM client, to allow VAP messages to be sent between the IME server and Unified CM client.

Command syntax

add ime vapusercredentials

After you enter the command, the system prompts you for the parameters.

Parameters

- appusername (mandatory)
- password (optional)
- ticketpassword (optional)
- epoch (optional)

Usage Guidelines

Appusername cannot match an existing appusername field for a row in the table.

Example

```
add ime vapusercredentials
(user is prompted for input, and fields such as password will be obscured)
Application User name: john
Password: ******
Reconfirm Password: ******
Ticket password: ******
Reconfirm Ticket password: ******
Epoch [1]:

Record added successfully
```

Requirements

Command privilege level:0

Allowed during upgrade:Yes

Delete Commands

- delete account, page 8
- delete dns, page 8
- delete ime validation-confirmation-required, page 8
- delete ime vapserver, page 9

- delete ime vapusercredentials, page 9
- delete process, page 9
- delete smtp, page 10

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 ime validation-confirmation-required

This command deletes entries that are pending validation.

Command syntax

delete ime validation-confirmation-required {*called-dn* | **all**}{*publicKey* | **all**]

Parameters

- **all**
- *called-dn* specifies the called number (such as +13035551234).
- *publicKey* specifies the peerid of the server for which you want to delete the entry.

Example

delete ime validation-confirmation-required +123455689 all

This command deletes the all the confirmation-required for calling number +123455689.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

delete ime vapserver

This command deletes the specified vapserver.

Command syntax

delete ime vapserver *vapservername*

Parameters

- *vapservername* represents the name of the vapserver to be deleted.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

delete ime vapusercredentials

This command deletes the specified user credential.

Command syntax

delete ime vapusercredentials *appusername*

Parameters

- *appusername* name of appuser to be deleted.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

delete process

This command allows you to delete a particular process.

Command Syntax

delete process *process-id* {**force** | **terminate** | **crash**}

Parameters

- *process-id* represents the process ID number.

Options

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

Usage Guidelines

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

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

delete smtp

This command allows you to delete the SMTP host.

Command Syntax

delete smtp

Requirements

Command privilege level: 1

Allowed during upgrade: No

File Commands

- file check, page 11
- file delete, page 11
- file dump, page 12
- file fragmentation sdi, page 13
- file fragmentation sdl, page 14
- file get, page 14
- file list, page 15
- file search, page 16
- file tail, page 17

- file view, page 18

file check

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

Command Syntax

file check *detection-size-kb*

Options

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

Usage Guidelines

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

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

The display includes both deleted and new files.

Defaults

The default value of *detection-size-kb* 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**}

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 cannot recover a deleted file except, possibly, by using the Disaster Recovery System.

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

If you delete a TFTP data file on the inactive side, you may need to manually restore that file if you switch versions to the inactive side.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Example

The following example deletes the install log.

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

file dump

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

Command Syntax

file dump

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

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

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

sftpdetails *filename* [**hex**] [**regexp** *expression*] [**recent**]

Parameters

- **activelog** specifies a log on the active side.
- **inactivelog** specifies a log on the inactive side.
- **install** specifies an installation log.
- **sftpdetails** specifies SFTP-related files.
- *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.
- *filename* specifies the filename of the file to dump.

Options

- **detail**—Displays listing with the date and time
- **hex**—Displays output in hexadecimal
- **regexp** *expression*—Displays only the lines in the file that match the regular expression *expression*.
- **recent**—Displays the most recently modified file in the directory.

Usage Guidelines

To determine which files you can dump with the **sftpdetails** parameter, first enter the following command:

file list sftpdetails *

The output lists the filenames that you can dump.

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 sdi

This command displays file fragmentation information about SDI log files.

Command Syntax

file fragmentation sdi

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 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**]

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

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

Options

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

Usage Guidelines

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

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Examples

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

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

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

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

file list

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

Command Syntax

file list

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

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

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

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

salog *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, 0 for TFTP files

Allowed during upgrade: Yes

Examples

This example lists operating system log files with details.

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

This example lists directories in CDR repository.

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

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

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

In Cisco Unity Connection and in Cisco Unified Communications Manager Business Edition, this example lists all files in the cuc log directory.

```
file list activelog cuc *
```

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.

- **tftp** specifies a TFTP file.
- *reg-exp* represents a regular expression.
- *directory/filename* represents the path to the file(s) to search. You can use the wildcard character, *, to represent all or part of the filename.

Options

- **abstime**—Specifies which files to search based on file creation time. Enter a start time and an end time.
- **days|hours|minutes**—Specifies whether the file age is in days, hours, or minutes.
- **ignorecase**—Ignores case when searching.
- **reltime**—Specifies which files to search based on file creation time. Enter the age of files to search.
- *hh*:*mm*:*ss mm*/*dd*/*yyyy*—An absolute time, in the format hours:minutes:seconds month/day/year.
- *timevalue*—The age of files to search. 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, 0 for TFTP files

Allowed during upgrade: Yes

Example

This example tails the operating system CLI log file.

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

file view

This command displays the contents of a file.

Command Syntax

file view

activelog *directory/filename*

inactivelog *directory/filename*

install *directory/filename*

system-management-log

Parameters

- **activelog** specifies a log on the active side.
- **inactivelog** specifies a log on the inactive side.
- **install** specifies an installation log.
- **system-management-log** displays the contents of the Integrated Management Logs (IML).
- *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}
```

Set Commands

- set account name, page 21
- set account enable, page 22
- set accountlocking, page 22
- set accountlocking unlocktime, page 23
- set alarm default, page 23
- set alarm status, page 24
- set alarm severity, page 24
- set alarm remotesyslogserver, page 26
- set amc serviceparam AmcCollectionEnabled, page 26
- set amc serviceparam AmcCollectionPollingRate, page 27
- set amc serviceparam AlertMgrEnabled, page 27
- set amc serviceparam LoggerEnabled, page 27
- set auditlog status, page 27
- set auditlog purging, page 28
- set auditlog logrotation, page 28
- set auditlog maxfilesize, page 29
- set auditlog maxnumfiles, page 29
- set auditlog remotesyslogseverity, page 29
- set auditlog remotesyslogserver, page 30
- set cert, page 30
- set cli pagination, page 31
- set commandcount, page 32
- set csr gen, page 32
- set date, page 32
- set enterprise serviceparam ClusterID, page 33
- set enterprise serviceparam RemoteSyslogServerName, page 33
- set enterprise serviceparam RemoteSyslogSeverity, page 34
- set ime addressing dht, page 34
- set ime validator local, page 35
- set ime dht local readbufferdepth, page 35

- set ime peerid, page 36
- set ime serviceparam DhtRcvdMsgTraceFlag, page 36
- set ime serviceparam DhtSentMsgTraceFlag, page 37
- set ime serviceparam MaxVtraceP2pRecordsPerPeer, page 37
- set ime serviceparam MaxVtraceValRecordsPerPeer, page 37
- set ime serviceparam MaxVtraceVapRecordsPerPeer, page 38
- set ime serviceparam MaxVtraceTlsRecordsPerPeer, page 38
- set ime serviceparam MaxVtraceFetchRecordsPerPeer, page 38
- set ime serviceparam MaxVtraceStoreRecordsPerPeer, page 39
- set ime serviceparam NetMaskForNATEnvironment, page 39
- set ime serviceparam SdlTraceDataFlags, page 39
- set ime serviceparam SdlTraceDataSize, page 40
- set ime serviceparam SdlTraceFlag, page 40
- set ime serviceparam SdlTraceMaxFileSize, page 40
- set ime serviceparam SdlTraceTotalNumFiles, page 41
- set ime serviceparam SdlTraceTypeFlags, page 41
- set ime serviceparam TLSMaxConnections, page 42
- set ime serviceparam TLSValidationThreshhold, page 42
- set ime vapserver, page 42
- set ime vapusercredentials, page 43
- set ime vapusercredentials epoch, page 43
- set logging, page 44
- set network dns, page 44
- set network dns options, page 45
- set network domain, page 45
- set network failover, page 46
- set network gateway, page 46
- set network ip, page 47
- set network ipv6, page 48
- set network mtu, page 49
- set network max_ip_conntrack, page 49
- set network nic, page 49
- set network pmtud, page 50
- set network restore, page 51
- set network status, page 51
- set password age maximum, page 52
- set password age minimum, page 52
- set password complexity minimum-length, page 52

- set password expiry, page 53
- set password expiry minimum-age, page 53
- set password expiry user maximum-age, page 54
- set password expiry user minimum-age, page 54
- set password inactivity, page 54
- set password history, page 55
- set password user, page 55
- set risdc serviceparam RisClientTimeout, page 56
- set risdc serviceparam RisCleanupTimeOftheDay, page 56
- set risdc serviceparam RisSystemAccessMaxProcessesThreads, page 57
- set risdc serviceparam RisTLCThrottleEnable, page 57
- set risdc serviceparam RisTLCIOThrottleLimit, page 57
- set risdc serviceparam RisTLCCPUThrottleLimit, page 58
- set risdc serviceparam RisTLCThrottlePollRate, page 58
- set risdc serviceparam RisTLCSFTPKeepaliveDelay, page 58
- set risdc serviceparam RisTSEnableLogging, page 59
- set risdc serviceparam RisTSPollingInterval, page 59
- set risdc serviceparam RisTSFileSize, page 59
- set risdc serviceparam RisTSTotalNumberFiles, page 60
- set smtp, page 60
- set timezone, page 60
- set trace default, page 61
- set trace status, page 62
- set trace tracelevel, page 62
- set trace maxfilesize, page 63
- set trace maxnumfiles, page 64
- set trace usercategories, page 65
- set web-security, page 65
- set workingdir, page 66

set account name

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

Command Syntax

set account name *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 account enable

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

Password inactivity period is the number of days of inactivity after a password has expired, before the account is disabled. Upon executing this command the user account is enabled with current system settings. The system settings are Password min days, Password Max days, and Password inactivity period.

Command syntax

Set account enable *user-id*

Parameters

- *user-id* specifies the name of the user account that was disabled.

Requirements

Command privilege level: 4

Allowed during upgrade: No

Example

User account *test* was disabled due to password inactivity. Its enabled as follows:

```
admin:set account enable test
Enabling the account 'test' with current settings....
.....
Successfully enabled account 'test'
```

set accountlocking

This command enables or disables accountlocking for the current admin accounts.

Command syntax

set accountlocking {enable | disable}

Requirements

Command privilege level:0

Allowed during upgradeYes

set accountlocking unlocktime

Use this command to configure the unlock time for CUCM OS admin accounts in seconds.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Command syntax

set accountlocking unlocktime *seconds*

Parameters

- unlocktime in seconds

  Acceptable values should be greater than or equal to 300 seconds but less than 3600 seconds (60 minutes).

set alarm default

This command sets the alarm configuration to the factory defaults.

Command syntax

set alarm default

Note The system prompts you for the service name.

Parameter

Service names comprise:

- **Cisco AMC Service**
- **Cisco Audit Event Service**
- **Cisco DRF Local**
- **Cisco DRF Master**
- **Cisco IME Configuration Manager**
- **Cisco IME Service**
- **Cisco Log Partition Monitoring Tool**
- **Cisco RIS Data Collector**
- **Cisco RTMT Web Service**
- **Cisco RisBean Library**
- **Cisco Trace Collection Service**

Requirements

Command privilege level:0

Allowed during upgradeYes

set alarm status

This command enables or disables the specified monitor for the specified service.

Command syntax

set alarm status

Note The system prompts you to enable or disable a specified monitorname for a specified service.

Parameters

- status
  - **enable**
  - **disable**.
- monitorname
  - **SDI**
  - **SDL**
  - **Event Log**
  - **Sys Log**
- Service names comprise:
  - **Cisco AMC Service**
  - **Cisco Audit Event Service**
  - **Cisco DRF Local**
  - **Cisco DRF Master**
  - **Cisco IME Configuration Manager**
  - **Cisco IME Service**
  - **Cisco Log Partition Monitoring Tool**
  - **Cisco RIS Data Collector**
  - **Cisco RTMT Web Service**
  - **Cisco RisBean Library**
  - **Cisco Trace Collection Service**

Requirements

Command privilege level:0

Allowed during upgradeYes

set alarm severity

This command sets the specified monitor alarm to the specified severity for the specified service.

Command syntax

set alarm severity

Note The system prompts you for the severity, the monitorname and the servicename.

Parameters

- severity
  - **Emergency**
  - **Alert**
  - **Critical**
  - **Error**
  - **Warning**
  - **Notice**
  - **Informational**
  - **Debug**
- monitorname
  - **SDI**
  - **SDL**
  - **Event_Log**
  - **Sys_Log**
- servicename
  - **Cisco AMC Service**
  - **Cisco Audit Event Service**
  - **Cisco DRF Local**
  - **Cisco DRF Master**
  - **Cisco IME Configuration Manager**
  - **Cisco IME Service**
  - **Cisco Log Partition Monitoring Tool**
  - **Cisco RIS Data Collector**
  - **Cisco RTMT Web Service**
  - **Cisco RisBean Library**
  - **Cisco Trace Collection Service**

Requirements

Command privilege level:0

Allowed during upgradeYes

set alarm remotesyslogserver

This command sets the alarm for the remote syslog server.

Command syntax

set alarm remotesyslogserver

Note The system prompts you for the parameters.

Parameters

- remotesyslogserver specifies the name of the remote syslog server.
- servicename specifies name of the service.
  - **Cisco AMC Service**
  - **Cisco Audit Event Service**
  - **Cisco DRF Local**
  - **Cisco DRF Master**
  - **Cisco IME Configuration Manager**
  - **Cisco IME Service**
  - **Cisco Log Partition Monitoring Tool**
  - **Cisco RIS Data Collector**
  - **Cisco RTMT Web Service**
  - **Cisco RisBean Library**
  - **Cisco Trace Collection Service**

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set amc serviceparam AmcCollectionEnabled

This commands sets the amc serviceparam for collecting, and alerting of the real-time cluster information.

Command syntax

show amc serviceparam AmcCollectionEnabled [true | false | default]

Requirements

Command Privilege level:0

Allowed During Upgrade:Yes

set amc serviceparam AmcCollectionPollingRate

This command sets the AMC collecting rate, in seconds.

Command syntax

set amc serviceparam AmcCollectionPollingRate [paramValue]

Parameters

- paramValue can be greater than or equal to15 and less than or equal to 300
- default

Requirements

Command Privilege level:0

Allowed During Upgrade:Yes

set amc serviceparam AlertMgrEnabled

This parameter enables or disables the alerting (email/epage) feature. This command is used only for AMC troubleshooting purposes.

Command syntax

set amc serviceparam AlertMgrEnabled [true | false | default]

Requirements

Command Privilege level:0

Allowed During Upgrade:Yes

set amc serviceparam LoggerEnabled

This parameter enables or disables the logging feature(.csv files for generating reports). This command is used for AMC troubleshooting purpose only.

Command syntax

set amc serviceparam LoggerEnabled [true | false | default]

Requirements

Command Privilege level:0

Allowed During Upgrade:Yes

set auditlog status

This command enables or disables the auditlog.

Command syntax

set auditlog status

Note The system prompts you for the parameters.

Parameters

- status
  - **enable**
  - **disable**

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set auditlog purging

This command enables or disables auditlog purging.

Command syntax

set auditlog purging

Note The system prompts you for the parameters.

Parameters

- status
  - **enable**
  - **disable**

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set auditlog logrotation

This command enables or disables the auditlog logrotation.

Command syntax

set auditlog logrotation

Note The system prompts you for the parameters.

Parameters

- status
  - **enable**

– **disable**

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set auditlog maxfilesize

This command sets the auditlog maxfilesize.

Command syntax

set auditlog maxfilesize

Note The system prompts you for the parameters.

Parameters

- size specifies an integer between 1 and 10.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set auditlog maxnumfiles

This command sets the auditlog maxnumfiles count.

Command syntax

set auditlog maxnumfiles

Note The system prompts you for the parameters.

Parameters

- filecount specifies an integer between 1 and 10000.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set auditlog remotesyslogseverity

This command sets the auditlog remotesyslogseverity to the specified severity.

Command syntax

set auditlog remotesyslogseverity

Note The system prompts you for the parameters.

Parameters

- severity
  - **Emergency**
  - **Alert**
  - **Critical**
  - **Error**
  - **Warning**
  - **Notice**
  - **Informational**
  - **Debug**

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set auditlog remotesyslogserver

This command sets the remote syslog server name to a name specified.

Command syntax

set auditlog remotesyslogserver

Note The system prompts you for the parameters.

Parameters

- remotesyslogserver name represents a valid hostname of a remote syslog server.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set cert

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

Command syntax

set cert

import [*unit*]

Command privilege level:1

Allowed during upgrade:Yes

regen [*name*]

Command privilege level: 1

Allowed during upgrade: No

delete [*unit*] [*name*]

Command privilege level: 1

Allowed during upgrade: No

Parameters

- **import** imports the certificates available in the SFTP location into the specified unit trust-store.
- **regen** regenerates the certificate for the specified unit.
- **delete** deletes the certificate siptest.pem for the specified unit.

Options

- *unit* represents the unit name.
- *name* represents the unit name.

Requirements

Command privilege level:1

Allowed during upgrade:Yes

Import Example

```
admin:set cert import all

Successfully imported tomcat certificates.
Successfully imported tftp certificates.
```

Regen Example

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

set cli pagination

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

Command Syntax

set cli pagination {on | off}

Parameters

- **on** turns pagination On.
- **off** turns pagination Off.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Example

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

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 csr gen

This command regenerates the certificate for the specified unit name.

Command syntax

set csr gen *unitname*

Parameters

- *unitname* is mandatory and specifies the unit name from which the certificate is generated.

Requirements

Command privilege level:1

Allowed during upgrade:No

Example

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

set date

This command changes the date/time on the server.

Command syntax

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

Parameters

- *HH:mm:ss* specifies the time (24 hours format).
- *MM/DD/YY* specifies the date.

Usage Guidelines

The following date format is also accepted: *MM/DD/YYYY.*

If the server is configured to synchronize with any external NTP server(s), this command requires the user to remove all such NTP servers.

Requirements

Command privilege level:1

Allowed during upgrade:No

Example

To set date and time to 2:10:33 pm Feb 13th 2008

```
admin:set date 14:10:33:02/13/08
```

set enterprise serviceparam ClusterID

This parameter provides a unique identifier for this cluster.

Command syntax

set enterprise serviceparam ClusterID [paramValue | default]

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set enterprise serviceparam RemoteSyslogServerName

Enter the name or the IP address of the remote Syslog server that should accept Syslog messages. If the server name is not specified, Cisco Unified Serviceability does not send the Syslog messages. Do not specify a Cisco Unified Communications Manager.

Command syntax

set enterprise serviceparam RemoteSyslogServerName [paramValue | default]

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set enterprise serviceparam RemoteSyslogSeverity

Select the desired severity for the syslog messages that are to be sent to the remote syslog server. All the syslog messages with the selected or higher severity level are sent to the remote syslog. If the remote server name is not specified, Cisco Unified Serviceability does not send the syslog messages.

Command syntax

set enterprise serviceparam RemoteSyslogSeverity [paramValue]

Parameters

- severity
  - **Emergency**
  - **Alert**
  - **Critical**
  - **Error**
  - **Warning**
  - **Notice**
  - **Informational**
  - **Debug**
  - **default**

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set ime addressing dht

This command sets the IP addresses for this server in the public and private networks.

Command syntax

set ime addressing dht

publicipaddrv4 *ipaddr*

privateipaddrv4 *ipaddr*

Parameters

- *ipaddr* represents the public and private IP addresses.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

Examples

```
set ime addressing dht publicipaddrv4 10.76.242.45
set ime addressing dht privateipaddrv4 10.76.242.45
```

set ime validator local

This command sets the configuration parameters for validation on this server.

Command syntax

set ime validator local

roundinginterval *ms*

ticketvalidationlifetime *secs*

cleanupinterval *secs*

maxvalidationtime *secs*

minvalidationtime *secs*

bucketentropy *bits*

sameDNvalidationint *secs*

Parameters

- *ms* represents the length of the rounding interval in milliseconds.
- *secs* specifies a length of time in seconds.
  - **ticketvalidationlifetime** secs represents the amount of time, in seconds, that tickets are valid once they get created. Default specifies 31536000.
  - **cleanupinterval** *secs* represents the amount of time, in seconds, between periodic garbage collection runs, which remove expired terminating VCRs and DHT data. Range is between 60 and 4,294, 967, 296. Default is 86400, which is 24 hours.
  - **maxvalidationtime** secs represents the maximum time after a call that validation will happen. Value must be more than 30 seconds and less than 86400. This value must be greater than the minvalidationtime.
  - **minvalidationtime** *secs* represents the amount of time, after a VCR is uploaded, before validation happens. Value must be between 30 and 86400 seconds. It must be less than the maxvalidationtime.
  - **sameDNvalidationint** secs specifies the number of seconds you must wait between validating calls to the same DN. Range is 1 to 7200 (2 hr). Default specifies 3600 (1 hr).
- *bits* represents the total number of bits required in a bucket before it is considered validated.Value must be between 1 and 64.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set ime dht local readbufferdepth

This command sets the depth of the local read request queue.

Command syntax

set ime dht local

readbufferdepth *depth*

joinretrytimer *seconds*

Parameters

- *depth* specifies the number of pending read requests that are allowed in the read buffer. Value must be between 10 and 1000. Default value specifies 100.
- *seconds* specifies the amount of time the IME server will retry the joining process, if that process fails. Value must be between 10 and 65535. Default value specifies 360.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set ime peerid

This command enables or disables the peerids on the server.

Note When you disable the peerids, the IME server no longer publishes DIDs, so disable peerids only for maintenance. Enable the peerids when maintenance is done.

Command syntax

set ime peerid {enabled | disabled} all

Parameters

- **enabled** enables the peerID(s) on the server.
- **disabled** disables the peerID(s) on the server.
- **all** specifies all peers to be enabled.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set ime serviceparam DhtRcvdMsgTraceFlag

This parameter specifies whether the received DHT messages should be traced.

Command syntax

set ime serviceparam DhtRcvdMsgTraceFlag [true | false | default]

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set ime serviceparam DhtSentMsgTraceFlag

This parameter specifies whether the DHT messages sent should be traced.

Command syntax

set ime serviceparam DhtSentMsgTraceFlag [true | false | default]

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set ime serviceparam MaxVtraceP2pRecordsPerPeer

This parameter specifies the maximum number of P2P vtrace records that would be maintained.

Command syntax

set ime serviceparam MaxVtraceP2pRecordsPerPeer [paramValue]

Parameters

- paramValue can be greater than or equal to 1500 and less than or equal to 15000
- default

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set ime serviceparam MaxVtraceValRecordsPerPeer

This parameter specifies the maximum number of Validation vtrace records that would be maintained. Increasing this number makes the vtrace feature use more space.

Command syntax

set ime serviceparam MaxVtraceValRecordsPerPeer [paramValue]

Parameters

- paramValue can be greater than or equal to 1000 and less than or equal to 10000
- default

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set ime serviceparam MaxVtraceVapRecordsPerPeer

This parameter specifies the maximum number of VAP vtrace records that would be maintained. Increasing this number makes the vtrace feature use more space.

Command syntax

set ime serviceparam MaxVtraceVapRecordsPerPeer [paramValue]

Parameters

- paramValue can be greater than or equal to 200 and less than or equal to 2000
- default

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set ime serviceparam MaxVtraceTlsRecordsPerPeer

This parameter specifies the maximum number of TLS vtrace records that would be maintained. Increasing this number makes the vtrace feature use more space.

Command syntax

set ime serviceparam MaxVtraceTlsRecordsPerPeer [paramValue]

Parameters

- paramValue can be greater than or equal to 600 and less than or equal to 6000
- default

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set ime serviceparam MaxVtraceFetchRecordsPerPeer

This parameter specifies the maximum number of fetch records per peer, that vtrace maintains. Increasing this number makes the vtrace feature to use more space.

Command syntax

set ime serviceparam MaxVtraceFetchRecordsPerPeer [paramValue]

Parameters

- paramValue can be greater than or equal to 3000 and less than or equal to 30000
- default

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set ime serviceparam MaxVtraceStoreRecordsPerPeer

This parameter specifies the maximum number of store records per peer that vtrace would maintain. Increasing this number makes the vtrace feature use more space.

Command syntax

set ime serviceparam MaxVtraceStoreRecordsPerPeer [paramValue]

Parameters

- paramValue can be greater than or equal to 3000 and less than or equal to 30000
- default

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set ime serviceparam NetMaskForNATEnvironment

This parameter is used in a NAT environment to determine if outbound TCP/TLS connections are attempted to a remote IME Server, using its configured public or private IP address. The public and private IP addresses for an IME Server can be displayed.

Command syntax

set ime serviceparam NetMaskForNATEnvironment [paramValue]

Parameters

- paramValue can be greater than or equal to 0 and less than or equal to 32
- default

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set ime serviceparam SdlTraceDataFlags

This parameter provides a bit mask for enabling tracing of SDL non-application-specific components, or for modifying the behavior of SDL tracing. Keep this parameter set to the default value, unless a Cisco support engineer instructs otherwise.

Command syntax

set ime serviceparam SdlTraceDataFlags [paramValue]

Parameters

- paramValue can be greater than or equal to 0 and less than or equal to 4294967295
- default

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set ime serviceparam SdlTraceDataSize

This parameter specifies the number of bytes of raw SDL data that is to be dumped into the SDL trace file, from each signal.

Command syntax

set ime serviceparam SdlTraceDataSize [paramValue]

Parameters

- paramValue can be greater than or equal to 0 and less than or equal to 10000
- default

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set ime serviceparam SdlTraceFlag

This command enables or disables the SDL traces. Specifying True enables SDL tracing, and specifying False disables SDL tracing.

Command syntax

set ime serviceparam SdlTraceFlag [true | false | default]

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set ime serviceparam SdlTraceMaxFileSize

This parameter specifies the maximum number of Megabytes of space in each file, before the next file is started. You can update this parameter from SDL Trace Configuration in Cisco Unified CM Serviceability.

Command syntax

set ime serviceparam SdlTraceMaxFileSize [paramValue]

Parameters

- paramValue can be greater than or equal to 1 and less than or equal to 10
- default

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set ime serviceparam SdlTraceTotalNumFiles

This parameter specifies the maximum number of SDL trace files created, before the file count restarts. Old files are overwritten in a round-robin fashion, with the oldest file getting overwritten first. You can update this parameter from the SDL Trace Configuration in Cisco Unified CM Serviceability.

Command syntax

set ime serviceparam SdlTraceTotalNumFiles [paramValue]

Parameters

- paramValue can be greater than or equal to 0 and less than or equal to 500
- default

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set ime serviceparam SdlTraceTypeFlags

This parameter provides an application-specific bit mask, that is used for the application tracing and signal tracing. Retain the default value of the parameter unless a Cisco support engineer instructs otherwise.

Command syntax

set ime serviceparam SdlTraceTypeFlags [paramValue]

Parameters

- paramValue can be greater than or equal to 0 and less than or equal to 4294967295
- default

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set ime serviceparam TLSMaxConnections

This parameter specifies the maximum number of TLS connections the server can have.

Command syntax

set ime serviceparam TLSMaxConnections [paramValue]

Parameters

- paramValue can be greater than or equal to 500 and less than or equal to 900
- default

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set ime serviceparam TLSValidationThreshhold

This parameter specifies the maximum number of TLS connections that can be used on this server by the Cisco IME Service, for Validation.

Command syntax

set ime serviceparam TLSValidationThreshhold [paramValue]

Parameters

- paramValue can be greater than or equal to 10 and less than or equal to 750
- default

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set ime vapserver

This command changes a parameter value for a vapserver that is administered on this system.

Command syntax

set ime vapserver

authenticationmode *vapservername* {**authenticated | encrypted}**

enabled *vapservername enabledvalue*

keepaliveinterval *vapservername secs*

maxconnectionsallowed *vapservername count*

port *vapservername portnumber*

Parameters

- *vapservername* specifies the vapserver to be updated.
- *enabledvalue* specifies {**true** | **false**} and enables or disables client connections.
- *secs* specifies the number of seconds between keepalive messages sent from the ime clients.
- *count* specifies the maximum number of client connections allowed for the vapserver specified by *vapservername*.
- *portnumber* specifies the port the vapserver will listen to for client connections.

Options

- **authenticated** specifies authenticated authentication mode.
- **encrypted** specifies encrypted authentication mode.
- **true** specifies that the port that is associated with the *vapsername* is enabled.
- **false** specifies that the port that is associated with the *vapservername* is disabled.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set ime vapusercredentials

This command changes a parameter for a vapusercredentials entry.

Command syntax

set ime vapusercredentials

password *appusername password*

ticketpassword *appusername ticketpassword*

Parameters

- **password**
- **ticketpassword**
- *appusername* specifies the username whose password needs to be set,
- *password* specifies the desired password.
- *ticketpassword* specifies the ticket password configured in the enterprise firewall.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set ime vapusercredentials epoch

This command sets the value of the version of the ticketpassword you use.

Command syntax

set ime vapusercredentials epoch {*appusername*} {*value*}

Parameters

- *appusername* is mandatory and represents a vapusercredential that exists in the system.
- *value* is an integer and represents the epoch for this ticketpassword. The minimum integer allowed equals 1.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

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 dns

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

Command Syntax

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

Parameters

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

Usage Guidelines

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

Note 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.

Caution If you continue, this command causes a temporary loss of network connectivity. If you change the IP address of the DNS server, you must restart Cisco Tomcat. For more information, see utils service, page 157.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set network dns options

This command sets DNS options.

Command Syntax

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

Parameters

- **timeout** sets the DNS request timeout.
- **attempts** sets the number of times to attempt a DNS request before quitting.
- **rotate** causes the system to rotate among the configured DNS servers, distributing the load.
- *seconds* specifies the DNS timeout period, in seconds.
- *number* specifies the number of attempts.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

set network domain

This command sets the domain name for the system.

Command Syntax

set network domain *domain-name*

Parameters

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

Usage Guidelines

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

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

set network failover

This command enables or disables network failover.

Command syntax

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

Parameters

- **enable** enables network failover.
- **disable** disables network failover.

Usage Guidelines

When you enable network failover a virtual interface (bond0) that uses the ethernet interface eth0, but fails over to eth1 if eth0 fails gets created. All three interfaces (bond0, eth0, and eth1) share the same IP and MAC addresses.

When you disable network failover ethernet interface eth0 with equivalent configuration parameters gets restored and virtual interface bond0 gets removed.

When you set failover a restart of the system occurs.

Requirements

Command privilege level:1

Allowed during upgrade:No

Example

```
admin:set network failover enable
Creating virtual interface bond0 to failover ethernet interface eth0 to eth1
should eth0 fail.

          ***   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 2004):

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

set network gateway

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

Command Syntax

set network gateway *ip-address*

Parameters

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

Usage Guidelines

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

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

set network hostname

This command sets the network hostname, and restarts the system.

Command Syntax

set network hostname *name*

Parameters

- *name*—hostname to be assigned

  The name should follow ARPANET rules for host names. The hostname must start with an alphabet, end with an alphanumeric, and may contain alphanumeric characters or hyphen in between. The maximum length of the hostname can be 63 characters.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Example:

```
admin:set network hostname myname
*** W A R N I N G ***
This will cause the system to restart - Do you want to continue ?
Enter "yes" to continue and restart or any other key to abort
yes
executing...
Broadcast message from root (Thu Jun 24 13:00:21 2004):
The system is going down for restart NOW!
```

set network ip

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

Command Syntax

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

Parameters

- **eth0** specifies Ethernet interface 0.
- *ip-address* represents the IP address that you want to assign.

- *ip-mask* represents the IP mask that you want to assign.

Usage Guidelines

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

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

set network ipv6

This command sets system and network options for IPv6.

Note IPv6 is not supported in Cisco Unified Communications Manager Business Edition or Cisco Unity Connection.

Command Syntax

set network ipv6

dhcp {**enable**|**disable**} [**reboot**]

service {**enable**|**disable**} [**reboot**]

static_address *ipv6_address mask* [**reboot**]

Parameters

- **dhcp** enables or disables the DHCPv6 client on the server. By default, the server does not restart after you enable the DHCPv6 client. For your changes to take effect, you must restart the server by either entering the **reboot** parameter or manually restarting the server.
- **service** enables or disables the IPv6 service on the server. By default, the server restarts after you enable or disable the IPv6 service. If you enter the **noreboot** parameter, the server does not restart automatically, and you must restart it manually before your changes take effect.
- **static_address** assigns a static IPv6 address to the server. By default, the server does not restart after you assign the static IPv6 address. For your changes to take effect, you must restart the server by either entering the **reboot** parameter or manually restarting the server.
- *ipv6_address* specifies the static IPv6 address you assign to the server.
- *mask* specifies the IPv6 network mask (0-128).
- **reboot** causes the server to automatically restart after you enter the command.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set network mtu

This command sets the maximum MTU value.

Command Syntax

set network mtu *mtu_max*

Parameters

- *mtu_max* specifies the maximum MTU value.

Note The system default MTU value equals 1500.

Usage Guidelines

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

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:set network mtu 576
              W A R N I N G
This will cause the system to temporarily lose network connectivity

          Do you want to continue ?

Enter "yes" to continue or any other key to abort

yes
executing...
```

set network max_ip_conntrack

This command sets the ip_conntrack_max value.

Command Syntax

set network max_ip_conntrack *ip_conntrack_max*

Parameters

- *ip_conntrack_max* specifies the value for ip_conntrack_max.

set network nic

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

Command Syntax

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

Parameters

- **eth0** specifies Ethernet interface 0.

  auto specifies whether auto negotiation gets enabled or disabled.

  speed specifies whether the speed of the Ethernet connection: 10 or 100 Mb/s.

  duplex specifies half-duplex or full-duplex.

Usage Guidelines

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

Note You can enable only one active NIC at a time.

Caution If you continue, this command causes a temporary loss of network connections while the NIC gets reset.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set network pmtud

This command enables and disables Path MTU Discovery.

Command Syntax

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

Parameters

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

Usage Guidelines

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

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:set network pmtud enable
             W A R N I N G
```

```
This will cause the system to temporarily lose network connectivity

          Do you want to continue ?

Enter "yes" to continue or any other key to abort
yes
executing...
admin:
```

set network restore

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

Caution 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.

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

Command Syntax

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

Parameters

- **eth0** specifies Ethernet interface 0.
- *ip-address* specifies the IP address.
- *network-mask* specifies the subnet mask.
- *gateway* specifies the IP address of the default gateway.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

set network status

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

Command Syntax

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

Parameters

- **eth0** specifies Ethernet interface 0.

Usage Guidelines

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

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

set password age maximum

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

Command Syntax

set password age maximum *days*

Parameters

days specifies the maximum password age and must be greater-than or equal-to 90 days.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set password age minimum

Use this command to modify the value of minimum password age for OS admin accounts in days.

Command syntax

set password age minimum *days*

Parameters

- *days* is mandatory and represents the password age. Acceptable values specify 0 - 10.

Requirements

Command privilege level:1

Allowed during upgrade:Yes

set password complexity minimum-length

This command modifies the value for the minimum password length for Cisco Unified Communications 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 and must be greater-than or equal-to 6.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set password expiry

This command enables or disables password expiry for Cisco Unified Communications Manager OS accounts.

Command syntax

set password expiry{enable|disable}

Parameters

- **enable** turns on password expiry.
- **disable** turns off password expiry.

Usage Guidelines

The **set password expiry enable** command sets the value of maximum password age to 3650 days (10 yrs) for Cisco Unified Communications Manager OS admin accounts.

The set **password expiry disable** command results in Cisco Unified Communications Manager OS admin accounts never expiring.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

set password expiry minimum-age

This command disables or enables minimum password aging for OS accounts.

Command syntax

set password expiry minimum-age {enable | disable}

Parameters

- **enable** enables password expiry for OS accounts. This command sets the value of minimum password age to one day (24 hrs) for OS admin accounts.
- **disable** disables minimum password aging for OS accounts. This means that passwords for OS admin accounts can be changed at any interval.

set password expiry user maximum-age

This command disables or enables password expiry maximum age settings for a specified OS account.

Command syntax

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

Parameters

- **disable** disables password expiry maximum age settings for the specified OS account.
- **enable** enables password expiry maximum age settings for the specified OS account.
- *userid* specifies the affected OS account.

set password expiry user minimum-age

This command disables or enables password expiry minimum age settings for a specified OS account.

Command syntax

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

Parameters

- **disable** disables password expiry minimum age settings for the specified OS account.
- **enable** enables password expiry minimum age settings for the specified OS account.
- *userid* specifies the affected OS account.

set password inactivity

This command enables, disables and configures password inactivity.

Command syntax

set password inactivity [**enable | disable | period** *days*]

Parameters

- *days* specifies the number of days of inactivity after a password has expired before the account gets disabled.

Usage guidelines

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

  A user whose account is disabled must contact the system administrator to use the system again.

- To configure the password inactivity period execute the **set password inactivity period** *days* command. This command configures the password inactivity globally and updates individual OS users according to the setting.

set password history

This command sets the number of passwords that will be maintained in the history, for OS admin accounts. New passwords that match the existing passwords in history will not be allowed.

Command Syntax

set password history *number*

Parameters

- *number* specifies the number of passwords to be maintained in history
  - Enter 0 to disable this option
  - Default value is 10
  - Upper limit is 20

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

set password user

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

Command Syntax

set password user {**admin** | **security**}

Parameters

- **admin** specifies the administrator password.
- **security** specifies the security password.

Usage Guidelines

The systems prompts you for the old and new passwords.

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

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

Procedure

Step 1 Change the security password on the publisher server (first node) and then reboot the server (node).

Step 2 Change the security password on all the subsequent servers/nodes to the same password that you created on the first node and restart subsequent nodes, including application servers, to propagate the password change.

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

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

set risdc serviceparam RisClientTimeout

This parameter specifies the time, in seconds, that a RIS client will wait for a reply from the Cisco RIS Data Collector service. The RIS Data Collector service running on each node internally, distributes 90 percent of the value specified in this parameter.

Command Syntax

set risdc serviceparam RisClientTimeout [paramValue]

Parameters

- paramValue can be greater than or equal to 10 and less than or equal to 1000
- default

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set risdc serviceparam RisCleanupTimeOftheDay

This parameter specifies the time of the day that the RIS database will be cleaned up to remove any unused, old device information. During this time, the NumofRegistrationAttempts performance counters for all devices are reset to 0.

Command Syntax

set risdc serviceparam RisCleanupTimeOftheDay [paramValue | default]

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set risdc serviceparam RisSystemAccessMaxProcessesThreads

This parameter specifies the maximum number of processes and threads that can run on a machine. If the total number of processes and threads running on the machine exceeds this maximum number, SystemAccess sends the TotalProcessesThreadsExceededThresholdStart alarm.

Command Syntax

set risdc serviceparam RisSystemAccessMaxProcessesThreads [paramValue]

Parameters

- paramValue can be greater than or equal to 1000 and less than or equal to 3000
- default

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set risdc serviceparam RisTLCThrottleEnable

This parameter enables or disables the throttling behavior of Trace and Log Central.

Command Syntax

set risdc serviceparam RisTLCThrottleEnable [true | false | default]

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set risdc serviceparam RisTLCIOThrottleLimit

This parameter specifies the system IOWait percentage that TLC throttles toward.

Command Syntax

set risdc serviceparam RisTLCIOThrottleLimit [paramValue]

Parameters

- paramValue can be greater than or equal to 10 and less than or equal to 40
- default

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set risdc serviceparam RisTLCCPUThrottleLimit

This parameter specifies the system CPU utilization percentage that TLC throttles towards.

Command Syntax

set risdc serviceparam RisTLCCPUThrottleLimit [paramValue]

Parameters

- paramValue can be greater than or equal to 65 and less than or equal to 90
- default

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set risdc serviceparam RisTLCThrottlePollRate

This parameter specifies the minimum delay in milliseconds between IO wait and CPU usage polls, for the purpose of trace collection throttling.

Command Syntax

set risdc serviceparam RisTLCThrottlePollRate [paramValue]

Parameters

- paramValue can be greater than or equal to 200 and less than or equal to 2000
- default

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set risdc serviceparam RisTLCSFTPKeepaliveDelay

This parameter specifies the maximum number of times an SFTP transfer will be paused, in order to prevent timeouts.

Command Syntax

set risdc serviceparam RisTLCSFTPKeepaliveDelay [paramValue]

Parameters

- paramValue can be greater than or equal to 1000 and less than or equal to 10000
- default

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set risdc serviceparam RisTSEnableLogging

This parameter determines whether collecting and logging of troubleshooting perfmon data is enabled (True), or disabled (False).

Command Syntax

set risdc serviceparam RisTSEnableLogging [true | false | default]

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set risdc serviceparam RisTSPollingInterval

This parameter specifies the polling rate for troubleshooting perfmon data, in seconds.

Command Syntax

set risdc serviceparam RisTSPollingInterval [paramValue]

Parameters

- paramValue can be greater than or equal to 5 and less than or equal to 300
- default

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set risdc serviceparam RisTSFileSize

This parameter specifies the maximum file size in megabytes, for each troubleshooting perfmon log file, before the next file is started. If the *Maximum File Size* is set to a large number, you should reduce the *Maximum Number of Files*.

Command Syntax

set risdc serviceparam RisTSFileSize [paramValue]

Parameters

- paramValue can be greater than or equal to 1 and less than or equal to 500
- default

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set risdc serviceparam RisTSTotalNumberFiles

This parameter specifies the maximum number of troubleshooting perfmon log files that are saved on the disk. If the *Maximum Number of Files* is set to a large number, you should reduce the *Maximum File Size*.

Command Syntax

set risdc serviceparam RisTSTotalNumberFiles [paramValue]

Parameters

- paramValue can be greater than or equal to 1 and less than or equal to 100
- default

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set smtp

This command sets the SMTP server hostname.

Command Syntax

set smtp *hostname*

Parameters

- *hostname* represents the SMTP server name.

Requirements

Command privilege level: 0

Allowed during upgrade: No

set timezone

This command lets you change the system time zone.

Command Syntax

set timezone *timezone*

Parameters

- *timezone* specifies the new time zone.

Note Although the list of available time zones produced by the **show timezone list** command includes **Factory**, Cisco Unified Communications Manager does not support the **Factory** time zone.

Usage Guidelines

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

Caution You must restart the system after you change the time zone.

Requirements

Command privilege level: 0

Allowed during upgrade: No

Example

This example sets the time zone to Pacific time.

```
set timezone Pac
```

set trace default

This command sets the default (factory reset) trace configuration for the specified service.

Command syntax

set trace default

Note The system prompts you for the servicename.

Usage Guidelines

Service names comprise:

- **Cisco AMC Service**
- **Cisco Audit Event Service**
- **Cisco DRF Local**
- **Cisco DRF Master**
- **Cisco IME Configuration Manager**
- **Cisco IME Service**
- **Cisco Log Partition Monitoring Tool**
- **Cisco RIS Data Collector**
- **Cisco RTMT Web Service**
- **Cisco RisBean Library**
- **Cisco Trace Collection Service**

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set trace status

This command enables or disables the tracing for the specified service.

Command syntax

set trace status

Usage Guidelines

The system prompts you for the status and servicename.

- status = **enable** | **disable**
- servicename possibilities comprise:
  - **cdpmib**
  - **servm**
  - **syslogmib**
  - **Cisco AMC Service**
  - **Cisco Audit Event Service**
  - **Cisco DRF Local**
  - **Cisco DRF Master**
  - **Cisco IME Configuration Manager**
  - **Cisco IME Service**
  - **Cisco Log Partition Monitoring Tool**
  - **Cisco RIS Data Collector**
  - **Cisco RTMT Web Service**
  - **Cisco RisBean Library**
  - **Cisco Trace Collection Service**

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set trace tracelevel

This commands sets the tracelevel for the specified service.

Command syntax

set trace tracelevel

Parameters

- **cdpmib** tracelevels comprise Error, Special, State Transition, Significant, Entry_exit, Arbitrary, Detailed
- **servm** tracelevels comprise Error, Special, State Transition, Significant, Entry_exit, Arbitrary, Detailed

- **syslogmib** tracelevels comprise Error, Special, State Transition, Significant, Entry_exit, Arbitrary, Detailed
- **Cisco AMC Service** tracelevels comprise Fatal, Error, Warning, Informational, Detailed.
- **Cisco Audit Event Service** tracelevels comprise tracelevels comprise Error, Special, State Transition, Significant, Entry_exit, Arbitrary, Detailed
- **Cisco DRF Local** tracelevels comprise Fatal, Error, Warning, Informational, Detailed.
- **Cisco DRF Master** tracelevels comprise Fatal, Error, Warning, Informational, Detailed.
- **Cisco IME Configuration Manager** tracelevels comprise Error, Special, State Transition, Significant, Entry_exit, Arbitrary, Detailed.
- **Cisco IME Service** tracelevels comprise Error, Special, State Transition, Significant, Entry_exit, Arbitrary, Detailed.
- **Cisco Log Partition Monitoring Tool** tracelevels comprise Error, Special, State Transition, Significant, Entry_exit, Arbitrary, Detailed.
- **Cisco RIS Data Collector** tracelevels comprise Error, Special, State Transition, Significant, Entry_exit, Arbitrary, Detailed.
- **Cisco RTMT Web Service** tracelevels comprise Fatal, Error, Warning, Informational, Detailed.
- **Cisco RisBean Library** tracelevels comprise Fatal, Error, Warning, Informational, Detailed.
- **Cisco Trace Collection Service** tracelevels comprise Fatal, Error, Warning, Informational, Detailed.

Usage Guidelines

The system prompts you for the tracelevel and the service name.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set trace maxfilesize

This command sets the max trace file size for the specified service.

Command syntax

set trace maxfilesize

Note The system prompts you for the size (in MBs) and the service name.

Parameters

- size in MBs specifies an integer value between 1 and 10.
- servicename possibilities comprise:
  - **cdpmib**
  - **servm**
  - **syslogmib**

- **Cisco AMC Service**
- **Cisco Audit Event Service**
- **Cisco DRF Local**
- **Cisco DRF Master**
- **Cisco IME Configuration Manager**
- **Cisco IME Service**
- **Cisco Log Partition Monitoring Tool**
- **Cisco RIS Data Collector**
- **Cisco RTMT Web Service**
- **Cisco RisBean Library**
- **Cisco Trace Collection Service**

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set trace maxnumfiles

This command sets the maximum trace file count for the specified service.

Command syntax

set trace maxnumfiles

Note The system prompts you for the filecount and the service name.

Parameters

- filecount represents an integer value between 1 to 10000.
- servicename possibilities comprise:
  - **cdpmib**
  - **servm**
  - **syslogmib**
  - **Cisco AMC Service**
  - **Cisco Audit Event Service**
  - **Cisco DRF Local**
  - **Cisco DRF Master**
  - **Cisco IME Configuration Manager**
  - **Cisco IME Service**
  - **Cisco Log Partition Monitoring Tool**
  - **Cisco RIS Data Collector**
  - **Cisco RTMT Web Service**

- **Cisco RisBean Library**
- **Cisco Trace Collection Service**

Requirements

Command privilege level:0

Allowed during upgrade:Yes

set trace usercategories

This command sets the usercategories flag to the value provided for the service specified.

Command syntax

set trace usercategories

Note The system prompts you for the flagnumber and the service name.

Parameters

- flagnumber specifies 0 to 7FFF. 7FFF means all the flags get enabled.
- servicename possibilities comprise:
  - **Cisco AMC Service**
  - **Cisco Audit Event Service**
  - **Cisco DRF Local**
  - **Cisco DRF Master**
  - **Cisco IME Configuration Manager**
  - **Cisco IME Service**
  - **Cisco Log Partition Monitoring Tool**
  - **Cisco RIS Data Collector**
  - **Cisco RTMT Web Service**
  - **Cisco RisBean Library**
  - **Cisco Trace Collection Service**

Requirements

Command privilege level:0

Allowed during upgrade:Yes

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 Communications Manager will contain Subject Alternate Name Extension with the alternate host name included in the CSR.

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*

tftp *directory*

Parameters

- **activelog** sets the working directory for active logs.
- **inactivelog** set the working directory for inactive logs.
- **tftp** sets the working directory for TFTP files.
- *directory* represents the current working directory.

Requirements

Command privilege level: 0 for logs, 1 for TFTP

Allowed during upgrade: Yes

Show Commands

- show account, page 70
- show accountlocking, page 70
- show alarm, page 71
- show amc serviceparam AmcCollectionEnabled, page 71
- show amc serviceparam AmcCollectionPollingRate, page 71
- show amc serviceparam AlertMgrEnabled, page 72
- show amc serviceparam LoggerEnabled, page 72
- show auditlog, page 72
- show auditlogconfig, page 72
- show cert, page 73
- show cli pagination, page 73
- show csr own, page 74
- show csr list own, page 74
- show date, page 75
- show diskusage, page 75
- show environment, page 76
- show enterprise serviceparam ClusterID, page 76
- show enterprise serviceparam RemoteSyslogServerName, page 77
- show enterprise serviceparam RemoteSyslogSeverity, page 77
- show hardware, page 77
- show ime accesscontrollist, page 78
- show ime addressing dht, page 78
- show ime addressing validator, page 78
- show ime certenrollment serverID, page 79
- show ime dht config local, page 79
- show ime motd, page 79

- show ime dht, page 80
- show ime dht counters, page 80
- show ime peerid, page 80
- show ime serviceparam DhtRcvdMsgTraceFlag, page 81
- show ime serviceparam DhtSentMsgTraceFlag, page 81
- show ime serviceparam MaxVtraceP2pRecordsPerPeer, page 81
- show ime serviceparam MaxVtraceValRecordsPerPeer, page 81
- show ime serviceparam MaxVtraceVapRecordsPerPeer, page 82
- show ime serviceparam MaxVtraceTlsRecordsPerPeer, page 82
- show ime serviceparam MaxVtraceFetchRecordsPerPeer, page 82
- show ime serviceparam MaxVtraceStoreRecordsPerPeer, page 83
- show ime serviceparam NetMaskForNATEnvironment, page 83
- show ime serviceparam SdlTraceDataFlags, page 83
- show ime serviceparam SdlTraceDataSize, page 83
- show ime serviceparam SdlTraceFlag, page 84
- show ime serviceparam SdlTraceMaxFileSize, page 84
- show ime serviceparam SdlTraceTotalNumFiles, page 84
- show ime serviceparam SdlTraceTypeFlags, page 85
- show ime serviceparam TLSMaxConnections, page 85
- show ime serviceparam TLSValidationThreshhold, page 85
- show ime software-config version, page 85
- show ime validation counters, page 86
- show ime validation details, page 87
- show ime validation DID, page 87
- show ime validation originating-aborted, page 87
- show ime validation pending, page 88
- show ime validation summary, page 88
- show ime validation success, page 89
- show ime validation confirmation-required, page 89
- show ime validation terminating-aborted, page 89
- show ime validation failed, page 90
- show ime validation route-discarded, page 90
- show ime validator config, page 90
- show ime vapserver, page 91
- show ime vapstatus summary, page 91
- show ime vapstatus subscriptions, page 91
- show ime vapusercredentials, page 92
- show ime voicerecord details, page 92

- show ime voicerecord summary, page 92
- show ime vservice, page 93
- show logins, page 93
- show memory, page 93
- show myself, page 94
- show network, page 94
- show network ipprefs, page 95
- show network ipv6, page 96
- show open, page 97
- show packages, page 97
- show password age, page 98
- show password complexity character, page 98
- show password complexity length, page 99
- show password history, page 99
- show password inactivity, page 99
- show perf counterhelp, page 99
- show perf list categories, page 100
- show perf list classes, page 100
- show perf list counters, page 101
- show perf list instances, page 102
- show perf query path, page 102
- show perf query class, page 103
- show perf query counter, page 104
- show perf query instance, page 104
- show process, page 105
- show registry, page 106
- show risdb list, page 107
- show risdb query, page 108
- show risdc serviceparam RisClientTimeout, page 108
- show risdc serviceparam RisCleanupTimeOftheDay, page 109
- show risdc serviceparam RisSystemAccessMaxProcessesThreads, page 109
- show risdc serviceparam RisTLCThrottleEnable, page 109
- show risdc serviceparam RisTLCIOThrottleLimit, page 109
- show risdc serviceparam RisTLCCPUThrottleLimit, page 110
- show risdc serviceparam RisTLCThrottlePollRate, page 110
- show risdc serviceparam RisTLCSFTPKeepaliveDelay, page 110
- show risdc serviceparam RisTSEnableLogging, page 110
- show risdc serviceparam RisTSPollingInterval, page 111

- show risdc serviceparam RisTSFileSize, page 111
- show risdc serviceparam RisTSTotalNumberFiles, page 111
- show smtp, page 112
- show stats io, page 112
- show status, page 112
- show tech all, page 113
- show tech network, page 113
- show tech system, page 114
- show tech runtime, page 115
- show timezone, page 116
- show trace, page 116
- show tracelevels, page 117
- show ups status, page 118
- show version, page 118
- show web-security, page 118
- show workingdir, page 118

show account

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

Command Syntax

show account

Parameters

None

Requirements

Command privilege level: 4

Allowed during upgrade: Yes

show accountlocking

This command displays the current account locking settings.

Command Syntax

show accountlocking

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Example:

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

show alarm

This command displays alarm configurations.

Command syntax

show alarm

Usage Guidelines

- The system prompts you for the servicename. Servicename can comprise multiple words.
- Enter servicename **all** to show alarm configurations of all the services.

Requirements

Command privilege level: 0

Allowed during upgrade:Yes

show amc serviceparam AmcCollectionEnabled

This commands displays if the amc serviceparam is enabled (True) for collecting, and alerting of the real-time cluster information.

Command syntax

show amc serviceparam AmcCollectionEnabled

Requirements

Command Privilege level: 0

Allowed During Upgrade:Yes

show amc serviceparam AmcCollectionPollingRate

This command displays the AMC collecting rate, in seconds.

Command syntax

show amc serviceparam AmcCollectionPollingRate

Requirements

Command Privilege level: 0

Allowed During Upgrade:Yes

show amc serviceparam AlertMgrEnabled

This parameter enables or disables the alerting (email/epage) feature. This command is used for AMC troubleshooting purpose only.

Command syntax

show amc serviceparam AlertMgrEnabled

Requirements

Command Privilege level: 0

Allowed During Upgrade:Yes

show amc serviceparam LoggerEnabled

This parameter enables or disables the logging feature(.csv files for generating reports). This command is used for AMC troubleshooting purpose only.

Command syntax

show amc serviceparam LoggerEnabled

Requirements

Command Privilege level: 0

Allowed During Upgrade:Yes

show auditlog

This command displays the AuditLog configuration.

Command syntax

show auditlog

Parameters

None

Requirements

Command privilege level: 0

Allowed during upgrade:Yes

show auditlogconfig

This command displays the AuditLog configuration.

Command syntax

show auditlogconfig

Parameters

None

Requirements

Command privilege level:0

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

show cli pagination

This command displays the status of automatic CLI pagination.

Command Syntax

show cli pagination

Parameters

None

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Example

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

show csr own

This command displays the selected own certificate file.

Command syntax

show csr own *name*

Parameters

- *name* is mandatory and represents the name of the certificate sign request.

Usage Guidelines

You can get the certificate name by executing the **show cert list own** command.

Requirements

Command privilege level:1

Allowed during upgrade:Yes

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
Q3ocBr9CZ5OTt7N6asZth4ggZ0ihJGXy6LKQmuUNIlJbNyQteM2Ak/E6usYBiCmUq0uhkf8g+ZFc
UmmqGOBORwQDSAEC69T98IUeTYM3jBwtGFRE3qsxWok=
-----END CERTIFICATE SIGN REQUEST -----
```

show csr list own

This command displays the own CSR file.

Command syntax

show csr list own

Parameters

None

Requirements

Command privilege level:1

Allowed during upgrade:Yes

Example

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

show date

The command displays the date and time on the server.

Command syntax

show date

Parameters

None

Requirements

Command privilege level:0

Allowed during upgrade:Yes

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 get 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

Options

- **fans**—Displays the fan speeds in Rotations per Minute (RPMs), fan-speed thresholds, and status.
- **power-supply**—Displays the power-supply status only on servers with redundant power supplies.
- **temperatures**—Displays the temperature sensor temperature values, thresholds, and status.

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

- RAID controller status

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show enterprise serviceparam ClusterID

This parameter provides a unique identifier for this cluster.

Command Syntax

show enterprise serviceparam ClusterID

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show enterprise serviceparam RemoteSyslogServerName

Enter the name or the IP address of the remote Syslog server that should accept Syslog messages. If the server name is not specified, Cisco Unified Serviceability does not send the Syslog messages. Do not specify a Cisco Unified Communications Manager.

Command Syntax

show enterprise serviceparam RemoteSyslogServerName

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show enterprise serviceparam RemoteSyslogSeverity

This command displays the selected severity of the Syslog messages that are sent to the remote syslog server. All the syslog messages with the selected or higher severity level are sent to the remote syslog server. If remote server name is not specified, Cisco Unified Serviceability does not send the Syslog messages.

Command Syntax

show enterprise serviceparam RemoteSyslogSeverity

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show hardware

This command displays the following information on the platform hardware.

Command Syntax

show hardware

Usage Guidelines

This command displays the following information on the platform hardware:

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

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show ime accesscontrollist

This command displays the black-listed peerids.

Command syntax

show ime accesscontrollist

Parameters

None

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime addressing dht

This command displays the dht addressing configuration for this overlay.

Command syntax

show ime addressing dht

Parameters

None

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime addressing validator

This command displays the validator addressing configuration for this overlay.

Command syntax

show ime addressing validator

Parameters

None

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime certenrollment serverID

This will retrieve the Cisco IME Server ID number assigned by the Certification Authority.

Command syntax

show ime certenrollment serverID

Requirements

Command privilege level:0

Allowed during upgrade:Yes

Example:

```
admin:show ime certenrollment serverID
Cisco IME ServerID: 12345
```

show ime dht config local

This command displays local DHT configuration data associated with this server.

Command syntax

show ime dht config local

Parameters

None

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime motd

This command displays the Message of the Day for the system.

Command syntax

show ime motd

Parameters

None

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime dht

This dynamic command shows the current status for the server.

Command syntax

show ime dht

peerIDStatus [*peerID* | **all**]

summary *peerID*

route-table *peerID*

Parameters

- *peerID* represents the peerID to display.
- **all** displays the status for all peerIDs.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime dht counters

This command displays all the DHT counters.

Command syntax

show ime dht counters

server

peer

Parameters

- **server** displays the DHT counters for the specified server.
- **peer** displays the DHT counters for the specified peer.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime peerid

This command displays the peerids for the server.

Command syntax

show ime peerid [*peerID* | *peerIndex* | **all**]

Parameters

- *peerID* represents the peerID. to display.

- *peerIndex* specifies a peerIndex to display.
- **all** displays all peerIDs.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime serviceparam DhtRcvdMsgTraceFlag

This parameter specifies whether the received DHT messages should be traced.

Command syntax

show ime serviceparam DhtRcvdMsgTraceFlag

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime serviceparam DhtSentMsgTraceFlag

This parameter specifies whether the DHT messages sent should be traced.

Command syntax

show ime serviceparam DhtSentMsgTraceFlag

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime serviceparam MaxVtraceP2pRecordsPerPeer

This parameter specifies the maximum number of P2P vtrace records that would be maintained.

Command syntax

show ime serviceparam MaxVtraceP2pRecordsPerPeer

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime serviceparam MaxVtraceValRecordsPerPeer

This parameter specifies the maximum number of Validation vtrace records that would be maintained. Increasing this number makes the vtrace feature use more space.

Command syntax

show ime serviceparam MaxVtraceValRecordsPerPeer

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime serviceparam MaxVtraceVapRecordsPerPeer

This parameter specifies the maximum number of VAP vtrace records that would be maintained. Increasing this number makes the vtrace feature use more space.

Command syntax

show ime serviceparam MaxVtraceVapRecordsPerPeer

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime serviceparam MaxVtraceTlsRecordsPerPeer

This parameter specifies the maximum number of TLS vtrace records that would be maintained. Increasing this number makes the vtrace feature use more space.

Command syntax

show ime serviceparam MaxVtraceTlsRecordsPerPeer

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime serviceparam MaxVtraceFetchRecordsPerPeer

This parameter specifies the maximum number of fetch records per peer, that vtrace maintains. Increasing this number makes the vtrace feature to use more space.

Command syntax

show ime serviceparam MaxVtraceFetchRecordsPerPeer

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime serviceparam MaxVtraceStoreRecordsPerPeer

This parameter specifies the maximum number of store records per peer that vtrace would maintain. Increasing this number makes the vtrace feature use more space.

Command syntax

show ime serviceparam MaxVtraceStoreRecordsPerPeer

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime serviceparam NetMaskForNATEnvironment

This parameter is used in a NAT environment to determine if outbound TCP/TLS connections are attempted to a remote IME Server, using its configured public or private IP address. The public and private IP addresses for an IME Server can be displayed.

Command syntax

show ime serviceparam NetMaskForNATEnvironment

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime serviceparam SdlTraceDataFlags

This parameter provides a bit mask for enabling tracing of SDL non-application-specific components, or for modifying the behavior of SDL tracing. Keep this parameter set to the default value, unless a Cisco support engineer instructs otherwise.

Command syntax

show ime serviceparam SdlTraceDataFlags

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime serviceparam SdlTraceDataSize

This command displays the number of bytes of raw SDL data that has been dumped into the SDL trace file, for each signal.

Command syntax

show ime serviceparam SdlTraceDataSize

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime serviceparam SdlTraceFlag

This parameter indicates whether the SDL traces are enabled. Valid values can be True or False.

Command syntax

show ime serviceparam SdlTraceFlag

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime serviceparam SdlTraceMaxFileSize

This parameter specifies the maximum number of Megabytes of space in each file, before the next file is started. You can update this parameter from the SDL Trace Configuration in Cisco Unified CM Serviceability.

Command syntax

show ime serviceparam SdlTraceMaxFileSize

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime serviceparam SdlTraceTotalNumFiles

This parameter specifies the maximum number of SDL trace files created, before the file count restarts. Old files are overwritten in a round-robin fashion, with the oldest file getting overwritten first. You can update this parameter from the SDL Trace Configuration in Cisco Unified CM Serviceability.

Command syntax

show ime serviceparam SdlTraceTotalNumFiles

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime serviceparam SdlTraceTypeFlags

This parameter provides an application-specific bit mask, that is used for the application tracing and signal tracing. Retain the default value of the parameter unless a Cisco support engineer instructs otherwise.

Command syntax

show ime serviceparam SdlTraceTypeFlags

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime serviceparam TLSMaxConnections

This parameter specifies the maximum number of TLS connections the server can have.

Command syntax

show ime serviceparam TLSMaxConnections

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime serviceparam TLSValidationThreshhold

This parameter specifies the maximum number of TLS connections that can be used on this server by the Cisco IME Service, for Validation.

Command syntax

show ime serviceparam TLSValidationThreshhold

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime software-config version

This command displays the contents of the software configuration table. This table contains instructions for upgrading software versions.

Command syntax

show ime software-config version [*versionnumber* | **all**]

Parameters

- *versionnumber* specifies software configuration for the version of interest.
- **all** displays the software configuration data for all versions.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime validation counters

This command displays information about the validation counters.

Command syntax

show ime validation counters

Parameters

None

Requirements

Command privilege level:0

Allowed during upgrade:Yes

Example

```
admin:show ime validation counters
DID Not Found in DHT     = 2
Route Sent       = 2
Original sRP attempts    = 2
sRP validation attempts  = 1
Total terminal VCR records       = 4


DHT Sent Message Counters
    DHT Reads.......................... = 1
    DHT Stores......................... = 180
    DHT Reads/Sec...................... = 0
    DHT Stores/Sec..................... = 0
    DHT Remove Reqs.................... = 0
    DHT Ping Reqs...................... = 1
    DHT Fetch Err...................... = 0
    DHT Store Err...................... = 0
    DHT Remove Err..................... = 0
    DHT Ping Err....................... = 0

DHT Received Message Counters
    DHT Fetch Reqs..................... = 1
    DHT Store Reqs..................... = 19620
    DHT Fetch/Sec...................... = 0
    DHT Store/Sec...................... = 0
    DHT Remove Req..................... = 0
    DHT Ping Reqs...................... = 1
    DHT Diag. Reqs..................... = 0
    DHT Diag./Sec...................... = 0

DHT Maintenance Counters
```

```
Mtce StoreRepls Sent.................. = 108
Mtce UpdateReqs Sent.................. = 50099
Mtce PingDhtReqs Sent................. = 83341
Mtce S-CDhtReqs Sent.................. = 8352
Mtce JoinDhtReqs Sent................. = 1
Mtce UpdateReqs Recv.................. = 49731
Mtce PingDhtReqs Recv................. = 82821
Mtce S-CDhtReqs Recv.................. = 12443
Mtce JoinDhtReqs Recv................. = 0
```

show ime validation details

This command displays all DiDs for validations that are discarded, failed-noroute, success, failed, pending, rate-limited, confirmation-required and remote-terminated.

Command syntax

show ime validation details [*public key* | **all**]

Parameters

- *public key* displays the DiDs for the specified public key
- **all** displays the DiDs for all public keys.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime validation DID

This command displays all DiDs for validations.

Command syntax

show ime validation DID [all]

Parameters

- **all** displays all the validations for DiDs.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime validation originating-aborted

This commands lists the most recent DiDs that did not validate because the DiD could not be retrieved from the DHT. Presence of a DiD in this list does not indicate a failure. The DiD may not be published by a IME server.

Command syntax

show ime validation discarded

Parameters

None

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime validation pending

This command displays the most recent validation-pending DiDs. Each pending DiD indicates that the number has successfully validated, but the IME server is waiting for sufficient entropy before passing the learned routes to Cisco Unified CM as successful validations.

Command syntax

show ime validation pending [*public key* | **all**]

Parameters

- *public key* displays the DiDs for the specified public key,
- **all** displays the DiDs for all public keys.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime validation summary

This command displays all the public keys with counters for discarded, failed-noroute, success, failed, pending, rate-limited, confirmation-required and remote-terminated validations.

Command syntax

show ime validation summary

Parameters

None

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime validation success

This command lists the most recent successfully validated DiDs. Each successfully validated DiD indicates that the learned route has been passed to the Cisco Unified CM.

Command syntax

show ime validation success [*public key* | **all**]

Parameters

- *public key* displays successfully validated DiDs for the specified public key,
- **all** displays successfully validated DiDs for all public keys.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime validation confirmation-required

This command displays the most recent validation-pending DiDs that are awaiting further validations.

Each confirmation-required DiD indicates that the number has successfully validated, but IME server is waiting for more successful validations to this same DiD since a previous validation failed.

Command syntax

show ime validation confirmation-required [*public key* | **all**]

Parameters

- *public key* displays DiDs that require confirmation for the specified public key.
- **all** displays DiDs that require confirmation for all public keys.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime validation terminating-aborted

This command displays the most recent remote-terminated DiDs. Each remote-terminated DiD indicates that a validation attempt was initiated to the given public key, but the validation failed because the terminating IME server could not find a matching call record or had too many overlapping call records to complete validation.

Command syntax

show ime validation remote-terminated [*public key* | **all**]

Parameters

- *public key* displays remote-terminated DiDs for the specified public key.

- **all** displays remote-terminated DiDs for all public keys.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime validation failed

This command lists the most recent validation failed DiDs. Each DiD failure indicates that a validation attempt was made to the given public key, but the validation failed due to mismatched VCR records.

Command syntax

show ime validation failed [*public key* | **all**]

Parameters

- *public key* displays DiDs on which validation failed for the specified public key.
- **all** displays DiDs on which validation failed for all public keys.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime validation route-discarded

This command displays the most recent DiDs that validated successfully, but failed to send to the Cisco Unified CM because a subsequent failed validation occurred.

Command syntax

show ime validation failed-to-send [*public key* | **all**]

Parameters

- *public key* displays failed-to-send DiDs for the specified public key.
- **all** displays failed-to-send DiDs for all public keys.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime validator config

This command displays validator configuration data.

Command syntax

show ime validator config {global | local}

Parameters

- **global** displays global validator configuration data.
- **local** displays local validator configuration data.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime vapserver

This command displays the vapserver entries that get administered on the server, and the ports they use, as well as other associated parameters (for example, authentication).

Command syntax

show ime vapserver [*vapservername* | **all**]

Parameters

- *vapservername* represents the vapserver to display.
- **all** specifies all vapservers will be shown.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime vapstatus summary

This command displays the registration status for the client specified by port number.

Command syntax

show ime vapstatus summary [*port* | **all**]

Parameters

- *port* specifies the client port number for which the summary will be displayed.
- **all** displays the summary of all clients.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime vapstatus subscriptions

Requirements

Command privilege level:0

Allowed during upgrade:Yes

Command syntax

show ime vapstatus subscriptions [*clientname* | **all**]

Parameters

- *clientname* displays the subscriptions/subscription IDs for the client specified.
- **all** displays the status of all clients.

show ime vapusercredentials

This command displays user credentials.

Command syntax

show ime vapusercredentials [*appusername* | **all**]

Parameters

- *appusername* represents the user for whom credentials should display.
- **all** specifies that all users credentials should display.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime voicerecord details

This command displays the voicerecord details.

Command syntax

show ime voicerecord details

Parameters

None

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime voicerecord summary

This command displays the voicerecord summary.

Command syntax

show ime voicerecord summary

Parameters

None

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show ime vservice

This command displays information about the Vservices that are published.

Command syntax

show ime vservice {details | summary}

details

summary

Parameters

- **details** displays details of the Vservices that are published
- **summary** displays summary information of the Vservices that are published.

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 specifies 20.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show memory

This command displays information about the onboard memory.

Command Syntax

show memory

count

modules

module {*modulenumber* | **all**}

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.
- *modulenumber* specifies the module number to be displayed.
- **all** specifies that all modules will be displayed.

Parameters

None

show memory module [module number]

module number mandatory module number to be fetched or ALL

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show myself

This command displays information about the current account.

Command Syntax

show myself

Parameters

None

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show network

This command displays network information.

Command Syntax

show network

cluster

eth0 [**detail**]

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

route [**detail**]

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

ip_conntrack

max_ip_conntrack

dhcp eth0 status

all [**detail**]

Parameters

- **cluster** displays a list of the nodes in the network cluster.
- **eth0** specifies Ethernet 0.
- **failover** specifies Network Fault Tolerance information.
- **route** specifies network routing information.
- **status** specifies active Internet connections.
- **ip_conntrack** specifies ip_conntrack usage information.
- **max_ip_conntrack** specifies max_ip_conntrack information.
- **dhcp eth0 status** displays DHCP status information.
- **all** specifies all basic network information.

Options

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

Usage Guidelines

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

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Example

This example displays active Internet connections.

```
show network status
```

show network ipprefs

This command displays the list of ports that have been requested to be opened or translated in the firewall.

Command Syntax

ipprefs {all | enabled | public}

Parameters

all—Displays all incoming ports that may be used on the product.

enabled—Displays all incoming ports that are currently opened.

public—Displays all incoming ports that are currently opened for any remote client.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin:show network ipprefs public

Application  IPProtocol   PortValue    Type         XlatedPort   Status       Description
------------ ------------ ------------ ------------ ------------ ------------ ------------
sshd         tcp          22           public       -            enabled      sftp and ssh
access
tomcat       tcp          8443         translated   443          enabled      secure web
access
tomcat       tcp          8080         translated   80           enabled      web access
clm          udp          8500         public       -            enabled      cluster
manager
clm          tcp          8500         public       -            enabled      cluster
manager
ntpd         udp          123          public       -            enabled      network time
sync
snmpdm       udp          161          public       -            enabled      SNMP
ccm          tcp          2000         public       -            enabled      SCCP-SIG
ctftp        udp          6969         translated   69           enabled      TFTP access
to CUCM TFTP Server
ctftp        tcp          6970         public       -            enabled      HTTP access
to CUCM TFTP Server
admin:
```

show network ipv6

This command displays IPv6 network routes and network settings.

Note IPv6 is not supported in Cisco Unified Communications Manager Business Edition or Cisco Unity Connection.

Command Syntax

show network ipv6 {**route** | **settings**}

Parameters

route displays all IPv6 routes.

settings displays IPv6 network settings.

Command privilege level: 0

Allowed during upgrade: Yes

show open

This command displays open files and ports on the system.

Command Syntax

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*—Represents 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 age

This command displays the information about the configured password.

Command Syntax

show password

age - displays information about the configured password age parameters

expiry [minimum-age | maximum-age] - displays the configured password expiration parameters.

Parameters

None

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show password complexity character

This command displays the status of the password complexity as enabled or disabled.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

Command syntax

show password complexity character

Parameters

None

Usage Guidelines

When enabled, the passwords must adhere to the following guidelines:

- It must contain at least one lower-case character.
- It must contain at least one uppercase character.
- It must contain one digit.
- It must contain one special character.
- A password comprised of all adjacent characters on the keyboard will not be accepted.
- None of the previous ten passwords can be reused.
- The admin user password can be changed only once in 24 hours.

A violation of any of the above rules will result in a failure.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show password complexity length

This command displays the minimum length of Unified CM OS account passwords. The default specifies 6.

Command syntax

show password complexity length

Parameters

None

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show password history

This command displays the number of passwords that are maintained in the password history, for OS admin accounts.

Command syntax

show password history

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show password inactivity

This command displays the status of password inactivity.

Command syntax

show password inactivity

Parameters

None

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show perf counterhelp

This command displays the description of the specified perfmon counter.

Command syntax

show perf counterhelp *class-name counter-name*

Parameters

- *class-name* is mandatory and specifies the perf class name that contains the perf counter.
- *counter-name* is mandatory and specifies the perf counter name to display.

Usage Guidelines

If class-name or counter-name contains white space, *class-name* or *counter-name* should be included in double quotes.

Requirements

Command privilege level: 0

Allowed during upgrade:Yes

Example

```
admin:show perf counterhelp System "Total Threads"
==>perf counter (System -> Total Threads) has help text:
         * help text :
         - This represents the total number of threads on the system.
```

show perf list categories

This command displays all categories in the perfmon system.

Requirements

Command privilege level: 0

Allowed during upgrade:Yes

Command syntax

show perf list categories

Parameters

None

Example

```
admin:show perf list categories
==>list categories:
         ...
         - RISSystemAccess
         ...
```

show perf list classes

This command displays perfmon classes (objects).

Command syntax

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

Parameters

- **cat** *category* displays perfmon classes for the specified *category.*
- **detail** displays detailed information.

Usage Guidelines

If the category name contains white space, *category* should be included in double quotes.

Requirements

Command privilege level: 0

Allowed during upgrade:Yes

Example

```
admin:show perf list classes cat RISSystemAccess detail
==>list classes for category (RISSystemAccess) :
         * Display Name         Enum    ClassId
         - Process              1       0
         - Partition            2       32
         - Memory               3       58
         - Processor            4       106
         - Thread               5       124
         - IP                   6       130
         - TCP                  7       160
         - Network Interface    8       180
         - System               9       206
         - IP6                  10      222
```

show perf list counters

This command displays perfmon counters in a specified perfmon class.

Command syntax

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

Parameters

class-name is mandatory and specifies the perf class to display.

Options

detail displays detailed information.

Usage Guidelines

If the class-name contains white space, *class-name* should be included in double quotes.

Requirements

Command privilege level: 0

Allowed during upgrade:Yes

Example

```
admin:show perf list counters System detail
==>perf class (System) has counters:
         * Display Name                          CounterId
         - Allocated FDs                        208
         - Being Used FDs                       212
         - Freed FDs                            210
         - Max FDs                              214
         - Total CPU Time                       220
         - Total Processes                      216
         - Total Threads                        218
```

show perf list instances

This command displays perfmon instances of a specified perfmon class

Command syntax

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

Parameters

- *class-name* is mandatory and specifies the perf class to display.

Options

- **detail** displays detailed information.

Usage Guidelines

Requirements

Command privilege level: 0

Allowed during upgrade:Yes

If the class-name contains white space, *class name* should be included in double quotes.

Example

```
admin:show perf list instances Processor detail
==>perf class (Processor) has instances:
         * Instance Name        index
         - _Total                0
         - 0                     1
         - 1                     2
```

show perf query path

This command queries specific perfmon path(s).

Command syntax

show perf query path *path-spec*

Parameters

path-spec is mandatory and represents the perfmon query path to display.

If the perfmon class is instance-based, *path-spec* comprises:

*class-name(instance-name)\counter-name (*for example **“Processor(0)\System Percentage”**.)

If the perfmon class is not instance-ased (singleton), *path-spec* comprises:

class-name\counter-name (for example *“***System\Total CPU Time”**.)

Usage Guidelines

- If path-spec contains white space, it should be included in double quotes.
- You can query a maximum of five paths at the same time delimited by commas with no space after the comma (for example, *path-spec,path-spec*):

Requirements

Command privilege level: 0

Allowed during upgrade:Yes

Example

```
admin:show perf query path "Processor(0)\System Percentage,System\Total CPU Time"
- query path :
    Processor(0)\System Percentage = 0
    System\Total CPU Time = 56273840
    Processor(0)\System Percentage = 9
    System\Total CPU Time = 56274645
```

show perf query class

This command queries perfmon class(es) to display all instances and counter values of each instance.

Command syntax

show perf query class *class-name*

Parameters

class-name is mandatory and specifies the display name of the perfmon class.

Usage Guideline

- If *class-name* contains white space, it should be included in double quotes.
- You can query a maximum of five class-names at the same time delimited by commas with no space after the comma (for example, *class-name,class-name*):
- You can execute the **show perf list classes** command to display the list of perfmon class display names.

Requirements

Command privilege level: 0

Allowed during upgrade:Yes

Example

```
admin:show perf query class System,TCP
==>query class :

 - Perf class (System) has instances and values:
                    -> Allocated FDs                  = 66345
```

```
                    -> Being Used FDs                = 66345
                    -> Freed FDs                     = 0
                    -> Max FDs                       = 102535
                    -> Total CPU Time                = 56309336
                    -> Total Processes               = 96
                    -> Total Threads                 = 314

 - Perf class (TCP) has instances and values:
                    -> Active Opens                  = 151754
                    -> Attempt Fails                 = 0
                    -> Curr Estab                    = 37
                    -> Estab Resets                  = 131
                    -> In Segs                       = 3688813
                    -> InOut Segs                    = 7328568
                    -> Out Segs                      = 3639755
                    -> Passive Opens                 = 58152
                    -> RetransSegs                   = 45
```

show perf query counter

This command queries the specified counter to show the counter value of all instances.

Command syntax

show perf query counter *class-name* **counter-name** *counter-name*

Parameters

- *class-name* is mandatory and represents the perf class name that contains the perf counter.
- **counter-name** *counter-name* is mandatory and represents the perf counter name to display. A maximum of five counters can be queried at the same time.

Usage Guidelines

If class-name or counter-name contains white space, the name should be included in double quotes.

Requirements

Command privilege level: 0

Allowed during upgrade:Yes

Example

```
admin:show perf query counter System "Max FDs"

 - Perf class System(Max FDs) has values:
                    -> Max FDs                       = 102535

admin:show perf query counter System "Max FDs,Total Threads"

 - Perf class System(Max FDs,Total Threads) has values:
                    -> Max FDs                       = 102535
                    -> Total Threads                 = 324
```

show perf query instance

This command queries a particular instance to show all counter values. This command is not applicable for singleton perfmon class.

Command syntax

show perf query instance {*class-name*} **instance-name** *instance-name*

Parameters

- *class-name* is mandatory and represents the perf class name that contains the perf instance.
- **instance-name** *instance-name* is mandatory and represents the perf instance name to display.

Usage Guidelines

- If the class-name or instance-name contains white space, the name should be included in double quotes.
- A maximum of five instances can be queried at the same time delimited by a comma with no space after the comma.

Requirements

Command privilege level: 0

Allowed during upgrade:Yes

Example

```
admin:show perf query instance Processor 0,1

 - Perf class Processor(0,1) has values:
    0               -> % CPU Time                    = 22
    0               -> IOwait Percentage             = 1
    0               -> Idle Percentage               = 78
    0               -> Irq Percentage                = 0
    0               -> Nice Percentage               = 4
    0               -> Softirq Percentage            = 0
    0               -> System Percentage             = 14
    0               -> User Percentage               = 3
    1               -> % CPU Time                    = 22
    1               -> IOwait Percentage             = 1
    1               -> Idle Percentage               = 78
    1               -> Irq Percentage                = 0
    1               -> Nice Percentage               = 3
    1               -> Softirq Percentage            = 0
    1               -> System Percentage             = 13
    1               -> User Percentage               = 5
```

show process

This command displays information about processes that run on the system.

Syntax

show process

list [**file** *filename*] [**detail**]

load [**cont**] [**clear**] [**noidle**] [**num** *number*] [**thread**] [**cpu** | **memory**| **time**] [**page**]

name *process* [**file** *filename*]

open-fd *process-id* [**,** *process-id2*]

pid *pid* [**file** *file-name*]

search *regexp* [**file** *filename*]

user *username* [**file** *filename*]

using-most cpu [*number*] [**file** *filename*]

using-most memory [*number*] [**file** *filename*]

Parameters

- **list** displays a list of all the processes and critical information about each process and visually indicates the child-parent relationships between the processes.
- **load** displays the current load on the system.
- **name** displays the details of processes that share the same name and indicates their parent-child relationship.
- **open-fd** lists the open file descriptors for a comma-separated list of process IDs.
- **search** searches for the pattern that the regular expression *regexp* specifies in the output of the operating system-specific process listing.
- **user** *username* retrieves details of processes that share the user name and displays parent-child relationship.
- **using-most cpu** displays a list of the most CPU-intensive processes.
- **using-most memory** displays a list of the most memory-intensive processes.

Options

- **file** *filename*—Outputs the results to the file that is specified by *filename*
- **detail**—Displays detailed output
- **cont**—Repeats the command continuously
- **clear**—Clears the screen before displaying output
- **noidle**—Ignore the idle/zombie processes
- **num** *number*—Displays the number of processes that are specified by *number*. The default number of processes equals 10. Set *number* to **all** to display all processes.
- **thread**—Displays threads
- [**cpu | memory | time**]—Sorts output by CPU usage, memory usage, or time usage. The default specifies to sort by CPU usage.
- **page**—Displays the output in pages
- *process*—Specifies the name of a process
- *pid*—Specifies the process ID number of a process
- *regexp*—Represents a regular expression
- *number*—Specifies the number of processes to display. The default specifies 5.
- *username*—(mandatory) Specifies the username.
- **vm**—Displays the virtual memory of the process.

show registry

This command displays the contents of the registry.

Command syntax

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

Parameters

- **system** represents the registry system name.
- **component** represents the registry component name.
- *name* the name of the parameter to display.
- **page** pauses the output.

Usage Guidelines

If the name of the parameter that you want to display is 'page', and you want to page the output, use the following command:

show registry system component page page

Example

```
admin:show registry cm dbl/sdi
system = cm
   component = dbl/sdi
      tracelevel=127
      enable=1
      outputdebugstringflag=0
      numminutes=1440
      tracefile=/var/log/active/cm/trace/dbl/sdi/dbl.log
      numfiles=250
      numlines=10000
```

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show risdb list

This command displays the list of tables supported in Realtime Information Service(RIS) database.

Command syntax

show risdb list [**file** *filename*]

Parameters

file *filename* specifies the file into which the output goes.

Usage Guidelines

- The file gets saved in platform/cli/filename.txt.
- *filename* should not contain the "." character.
- If the specified file already exists, it will be renamed.

Example

```
admin: show risdb list file TableList
```

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show risdb query

This command displays the contents of the Realtime Information Service(RIS) database.

Command syntax

show risdb query [*tablename*] [*tablename*] **file** *filename*

Parameters

- *tablename* is mandatory and represents the name of the tables or tables that are listed when **show risdb list** command is run.
- *filename* represents the name of the file to which the output should be sent.

Usage Guidelines

- The file will be saved in platform/cli/filename.txt.
- *filename* should not contain the "." character.
- If the specified file already exists it will be renamed.

Example

```
admin: show risdb query genalarm file genalarmtable
```

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show risdc serviceparam RisClientTimeout

This parameter specifies the time, in seconds, that a RIS client will wait for a reply from the Cisco RIS Data Collector service. The RIS Data Collector service running on each node internally, distributes 90 percent of the value specified in this parameter.

Command syntax

show risdc serviceparam RisClientTimeout

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show risdc serviceparam RisCleanupTimeOftheDay

This parameter specifies the time of the day that the RIS database will be cleaned up to remove any unused, old device information. During this time, the NumofRegistrationAttempts performance counters for all devices are reset to 0.

Command syntax

show risdc serviceparam RisCleanupTimeOftheDay

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show risdc serviceparam RisSystemAccessMaxProcessesThreads

This parameter specifies the maximum number of processes and threads that can run on a machine. If the total number of processes and threads running on the machine exceeds this maximum number, SystemAccess sends the TotalProcessesThreadsExceededThresholdStart alarm.

Command syntax

show risdc serviceparam RisSystemAccessMaxProcessesThreads

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show risdc serviceparam RisTLCThrottleEnable

This parameter enables or disables the throttling behavior of Trace and Log Central.

Command syntax

show risdc serviceparam RisTLCThrottleEnable

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show risdc serviceparam RisTLCIOThrottleLimit

This parameter specifies the system IOWait percentage that TLC throttles toward.

Command syntax

show risdc serviceparam RisTLCIOThrottleLimit

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show risdc serviceparam RisTLCCPUThrottleLimit

This parameter specifies the system CPU utilization percentage that TLC throttles towards.

Command syntax

show risdc serviceparam RisTLCCPUThrottleLimit

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show risdc serviceparam RisTLCThrottlePollRate

This parameter specifies the minimum delay in milliseconds between IO wait and CPU usage polls, for the purpose of trace collection throttling.

Command syntax

show risdc serviceparam RisTLCThrottlePollRate

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show risdc serviceparam RisTLCSFTPKeepaliveDelay

This parameter specifies the maximum number of times an SFTP transfer will be paused, in order to prevent time-outs.

Command Syntax

show risdc serviceparam RisTLCSFTPKeepaliveDelay

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show risdc serviceparam RisTSEnableLogging

This parameter determines whether collecting and logging of troubleshooting perfmon data is enabled (True), or disabled (False).

Command Syntax

show risdc serviceparam RisTSEnableLogging

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show risdc serviceparam RisTSPollingInterval

This parameter specifies the polling rate for troubleshooting perfmon data, in seconds.

Command Syntax

show risdc serviceparam RisTSPollingInterval

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show risdc serviceparam RisTSFileSize

This parameter specifies the maximum file size in megabytes, for each troubleshooting perfmon log file, before the next file is started. If the Maximum File Size is set to a large number, you should reduce the Maximum Number of Files.

Command Syntax

show risdc serviceparam RisTSFileSize

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show risdc serviceparam RisTSTotalNumberFiles

This parameter specifies the maximum number of troubleshooting perfmon log files that are saved on the disk. If the *Maximum Number of Files* is set to a large number, you should reduce the *Maximum File Size*.

Command Syntax

show risdc serviceparam RisTSTotalNumberFiles

Requirements

Command privilege level:0

Allowed during upgrade:Yes

show smtp

This command displays the name of the SMTP host.

Command Syntax

show snmp

Parameters

None

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show stats io

This command displays system IO statistics.

Command Syntax

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

Options

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

Note The file option saves the information to platform/cli/*filename*.txt. Ensure that the file name does not contain the "." character.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show status

This command displays basic platform status.

Command Syntax

show status

Usage Guidelines

This command displays the following basic platform status:

- Host name

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

Requirements

Command privilege level: 0

show tech all

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

Command Syntax

show tech all [**page**] [**file** *filename*]

Options

- **page**—Displays one page at a time.
- **file** *filename*—Outputs the information to a file.

Note The file option saves the information to platform/cli/*filename*.txt. Ensure that the file name does not contain the "." character.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show tech network

This command displays network aspects of the server.

Command Syntax

show tech network

all [**page**] [**search** *text*] [**file** *filename*]

hosts [**page**] [**search** *text*] [**file** *filename*]

interfaces [**page**] [**search** *text*] [**file** *filename*]

resolv [**page**] [**search** *text*] [**file** *filename*]

routes [**page**] [**search** *text*] [**file** *filename*]

sockets {**numeric**}

Parameters

- **all** displays all network tech information.
- **hosts** displays information about hosts configuration.
- **interfaces** displays information about the network interfaces.
- **resolv** displays information about hostname resolution.
- **routes** displays information about network routes.
- **sockets** displays the list of open sockets.

Options

- **page**—Displays one page at a time.
- **search** *text*—Searches the output for the string that *text* specifies. Be aware that the search is case insensitive.
- **file** *filename*—Outputs the information to a file.
- **numeric**—Displays the numerical addresses of the ports instead of determining symbolic hosts. This parameter is equivalent to running the Linux shell command netstat [-n] command.

Usage Guidelines

The **file** option saves the information to platform/cli/*filename*.txt. Ensure that the file name does not contain the "." character.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show tech system

The show tech system command gets updated as described in this section. This command displays system aspects of the server.

Command Syntax

show tech system

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

bus [**page**] [**file** *filename*]

hardware [**page**] [**file** *filename*]

host [**page**] [**file** *filename*]

kernel modules [**page**] [**file** *filename*]

software [**page**] [**file** *filename*]

tools [**page**] [**file** *filename*]

Parameters

- **all** displays all the system information.
- **bus** displays information about the data buses on the server.
- **hardware** displays information about the server hardware.

- **host** displays information about the server.
- **kernel modules** lists the installed kernel modules.
- **software** displays information about the installed software versions.
- **tools** displays information about the software tools on the server.

Options

- **page**—Displays one page at a time.
- **file** *filename*—Outputs the information to a file.

Usage Guidelines

The **file** option saves the information to platform/cli/*filename*.txt. Ensure that the file name does not contain the "." character.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show tech runtime

This command displays runtime aspects of the server.

Command Syntax

show tech runtime

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

cpu [**page**] [**file** *filename*]

disk [**page**] [**file** *filename*]

env [**page**] [**file** *filename*]

memory [**page**] [**file** *filename*]

Parameters

- **all** displays all runtime information.
- **cpu** displays CPU usage information at the time the command is run.
- **disk** displays system disk usage information.
- **env** displays environment variables.
- **memory** displays memory usage information.

Options

- **page**—Displays one page at a time.
- **file** *filename*—Outputs the information to a file.

Usage Guidelines

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

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show timezone

This command displays time zone information.

Command Syntax

show timezone

config

list [**page**]

Parameters

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

Note Although the list of available time zones includes **Factory**, Cisco Unified Communications Manager does not support the **Factory** time zone.

Options

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

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show trace

This command displays the trace configuration for the specified service.

Command syntax

show trace

Usage Guidelines

The system prompts you for the service name. Service names comprise:

- **cdpmib**
- **servm**
- **syslogmib**
- **Cisco AMC Service**
- **Cisco Audit Event Service**
- **Cisco DRF Local**

- **Cisco DRF Master**
- **Cisco IME Configuration Manager**
- **Cisco IME Service**
- **Cisco Log Partition Monitoring Tool**
- **Cisco RIS Data Collector**
- **Cisco RTMT Web Service**
- **Cisco RisBean Library**
- **Cisco Trace Collection Service**

Enter **all** to display the trace configurations of all the services.

Requirements

Command privilege level: 0

Allowed during upgrade:Yes

show tracelevels

This command displays the allowed trace levels for the specified service name.

Command syntax

show tracelevels

Usage Guidelines

The system prompts you for the service name. Service names comprise:

- **cdpmib**
- **servm**
- **syslogmib**
- **Cisco AMC Service**
- **Cisco Audit Event Service**
- **Cisco DRF Local**
- **Cisco DRF Master**
- **Cisco IME Configuration Manager**
- **Cisco IME Service**
- **Cisco Log Partition Monitoring Tool**
- **Cisco RIS Data Collector**
- **Cisco RTMT Web Service**
- **Cisco RisBean Library**
- **Cisco Trace Collection Service**

Requirements

Command privilege level:0

Allowed during upgrade:Yes

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

show version

Be aware that this command displays the software version on the active or inactive partition.

Command Syntax

show version

active

inactive

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show web-security

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

Command Syntax

show web-security

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show workingdir

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

Command Syntax

show workingdir

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Unset Commands

- unset network dns options, page 119
- unset network ipv6 static_address, page 119

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 as 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.

unset network ipv6 static_address

This command unsets the ipv6 static address.

Command syntax

unset network ipv6 static_address [**reboot**]

Parameters

- **reboot** causes the server to reboot the server after the changes get applied.

Example

```
admin:unset network ipv6 static_address
***   W A R N I N G   ***
The Server must be rebooted for these changes to take effect.
Please make sure that you reboot this server.


IPv6 static address was removed.
```

Requirements

Command privilege level:1

Allowed during upgrade:No

Utils Commands

- utils auditd, page 122
- utils ime certenrollment enroll, page 122
- utils ime enroll, page 123
- utils ime fetch did, page 123
- utils ime license file install, page 124
- utils ime license file list, page 124
- utils ime license file report, page 125
- utils ime license file view, page 125
- utils ime reset peerid, page 125
- utils core active, page 126
- utils core inactive list, page 126
- utils core inactive analyze, page 126
- utils create report, page 127
- utils csa disable, page 127
- utils csa enable, page 128
- utils csa status, page 128
- utils diagnose, page 128
- utils disaster_recovery backup local, page 129
- utils disaster_recovery backup tape, page 129
- utils disaster_recovery backup network, page 130
- utils disaster_recovery cancel_backup, page 130
- utils disaster_recovery device add, page 131
- utils disaster_recovery device delete, page 131
- utils disaster_recovery device list, page 132
- utils disaster_recovery restore local, page 132
- utils disaster_recovery restore tape, page 133
- utils disaster_recovery restore network, page 133
- utils disaster_recovery schedule, page 133
- utils disaster_recovery show_backupfiles tape, page 135
- utils disaster_recovery show_backupfiles network, page 136
- utils disaster_recovery show_registration, page 136
- utils disaster_recovery show_tapeid, page 136
- utils disaster_recovery status, page 137
- utils fior, page 137
- utils firewall ipv4, page 138
- utils firewall ipv6, page 139

- utils iostat, page 139
- utils iothrottle, page 140
- utils iothrottle threshold low, page 140
- utils iothrottle threshold clear, page 141
- utils iothrottle threshold status, page 141
- utils netdump client, page 141
- utils netdump server, page 142
- utils network arp, page 143
- utils network capture eth0, page 144
- utils network host, page 145
- utils network ipv6, page 145
- utils network ping, page 146
- utils network traceroute, page 146
- utils ntp, page 147
- utils ntp restart, page 147
- utils ntp server add, page 147
- utils ntp server delete, page 149
- utils ntp server list, page 150
- utils ntp start, page 151
- utils ntp status, page 151
- utils ntp server add, page 153
- utils ntp server delete, page 154
- utils ntp server list, page 155
- utils raid disk maintenance, page 156
- utils remote_account, page 156
- utils service, page 157
- utils service list, page 158
- utils snmp, page 158
- utils snmp get 3, page 159
- utils snmp walk 3, page 159
- utils snmp config inform 3 add, page 160
- utils snmp config inform 3 delete, page 161
- utils snmp config inform 3 list, page 162
- utils snmp config inform 3 update, page 162
- utils snmp config mib2 add, page 163
- utils snmp config mib2 delete, page 163
- utils snmp config mib2 list, page 164
- utils snmp config mib2 update, page 164

- utils snmp config trap 3 add, page 164
- utils snmp config trap 3 update, page 165
- utils snmp config trap 3, page 165
- utils snmp config trap 3 list, page 166
- utils snmp config user 3 add, page 166
- utils snmp config user 3 delete, page 167
- utils snmp config user 3 list, page 167
- utils snmp config user 3 update, page 167
- utils snmp test, page 168
- utils system, page 169
- utils system boot, page 169
- utils system upgrade, page 169

utils auditd

This command enables, disables, and provides the status of audit logging. When enabled, the system monitors and records user actions in both Cisco Unified Communications Manager and Cisco Unified Serviceability.

Cisco recommends that you retrieve the audit log by using the Real Time Monitoring Tool, but you can also retrieve it by using the CLI.

Command Syntax

utils auditd {enable | disable | status}

Parameters

- **enable**—Turns on audit logging.
- **disable**—Turns off audit logging.
- **status**—Displays whether audit logging is on or off.

utils ime certenrollment enroll

This command enrolls with GoDaddy WebService, to obtain the GoDaddy CA signed certficate for Cisco IME Server.

Command Syntax

utils ime certenrollment enroll

Requirements

Command privilege level:0

Allowed during upgrade:Yes

Example:

```
admin:utils ime certenrollment enroll
```

```
Congratulations, Cisco IME Certificate Enrollment Successful
```

utils ime enroll

This command communicates with GoDaddy WebService to obtain the GoDaddy CA signed certficate for the ime server

Command syntax

utils ime enroll

Parameters

None

```
ime Certificate Enrollment Successful
```

Requirements

Command privilege level:0

Allowed during upgrade:Yes

Example

```
admin:utils ime enroll
```

utils ime fetch did

This command indicates whether or not the DID was found in the DHT or not.

If a DID is found, that means it was published by a IME server somewhere on the network.

Command syntax

utils ime fetch *did*

Parameters

did specifies the number you want to look for in the system.

Example

utils ime fetch did +3035551001

This command will return either:

- DID not found (indicating DID is not stored in the DHT).
- or it will return the peer id that is storing that DID in the DHT.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

utils ime license file install

This command install license files.

Command syntax

utils ime license file install *file-name*

Parameters

- *file-name* represents the name of the license file, which has already been uploaded.

Usage Guidelines

This command assumes that the user has uploaded the license file on the system in the SFTP license directory. When this command is executed it looks into this directory and then installs the file.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

utils ime license file list

This command lists all the installed license files.

Command syntax

utils ime license file list

page

detail

reverse

date

size

Parameters

- **page** paginates the list.
- **detail** displays detailed information about the license files.
- **reverse** displays the license files in reverse chronological order.
- **date** displays the license files in chronological order.
- **size** displays license files in order of size.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

utils ime license file report

This command allows the user to view random number, signature, and peer ID count information, which gets used to obtain the certificate for the IME server.

Command syntax

utils ime license file report

Parameters

None

Requirements

Command privilege level:0

Allowed during upgrade:Yes

utils ime license file view

This command displays the contents of certain license file.

Command syntax

utils ime license file view *file-name*

Parameters

- *file-name* represents the name of the licence file, that has already been installed.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

utils ime reset peerid

This command resets the peerID.

Command syntax

utils ime reset peerid *peerID*

Parameters

- *peerID* specifies the peerID to be reset.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

utils core active

This command affects existing core files.

Command syntax

utils core active

list

analyze *core_file_name*

Parameters

- **list** displays the existing core files.
- **analyze** displays the stack trace for the specified core file.

Options

- *core_file_name* name of core file from which to get stack trace.

Requirements

Command privilege level:1

Allowed during upgrade:Yes

utils core inactive list

This command displays a list of core files.

Command Syntax

utils core inactive list

Parameters

None

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

utils core inactive analyze

This command displays backtrace for the specified core file. A list of core files can be obtained via the **utils core inactive list** command.

Command Syntax

utils core inactive analyze *core_file_name*

Parameter

core_file_name (mandatory) specifies the name of the core file from which to get a stack trace.

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.
- **csa** collects all the files required for CSA diagnostics and assembles them in 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 disable

This command stops Cisco Security Agent (CSA).

Command Syntax

utils csa disable

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils csa enable

This command enables Cisco Security Agent (CSA).

Command Syntax

utils csa enable

Usage Guidelines

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

Caution You must restart the system after you start CSA.ca

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils csa status

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

Command Syntax

utils csa status

Usage Guidelines

The system indicates whether CSA is running.

Requirements

Command privilege level: 0

Allowed during upgrade: No

utils 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.
- *module_name* specifies the name of a diagnostics module.

Requirements

Command privilege level: 0

Allowed during upgrade: No

utils disaster_recovery backup local

This command invokes the backup and creates the tar file on the local drive.

Command syntax

utils disaster_recovery backup local *featurelist device_name*

Parameters

- *featurelist* is mandatory and comprises a comma-separated feature list to backup.
- *device_name* is mandatory and specifies the name of the backup device to be added.

Usage Guidelines

Use **utils disaster_recovery show_registration** to display the list of registered features.

Use **utils disaster_recovery device list** to display the configured device list.

Requirements

Command privilege level:1

Allowed during upgrade:No

Example

```
admin:utils disaster_recovery backup local VIPR localdevice
Backup initiated successfully.Please run 'utils showstatus backup' command to see the
status.
```

utils disaster_recovery backup tape

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

Command Syntax

utils disaster_recovery backup tape *featurelist tapeid*

Parameters

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

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

utils disaster_recovery backup network

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

Command Syntax

utils disaster_recovery backup network *featurelist path servername username*

Parameters

- *featurelist* specifies the list of features to back up, separated by commas.
- *path* represents the location of the backup files on the remote server.
- *servername* represents the IP address or host name of the server where you stored the backup files.
- *username* represents the username that is needed to log in to the remote server.

Usage Guidelines

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

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

utils disaster_recovery cancel_backup

This command cancels the ongoing backup job.

Command Syntax

utils disaster_recovery cancel_backup *confirm*

Usage Guidelines

After you enter the command, you must confirm that you want to cancel the backup. Enter **Y** to cancel the backup or any other key to continue the backup.

Example

```
admin:utils disaster_recovery cancel_backup yes
Cancelling backup...
Backup cancelled successfully.
```

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

utils disaster_recovery device add

This command adds:

- backup tape device
- backup local device
- backup network device.

Command Syntax

utils disaster_recovery device add

local *device_name Number_of_backups*

network *device_name path server_name username Number_of_backups*

tape *device_name tapeid*

Parameters

- *device_name*—name of the backup device to be added
- *path*—path to retrieve backup device from this location
- *server_name*—hostname of the server where the backup file needs to be stored
- *username*—user id to connect to the remote machine
- *Number_of_backups*—Number of backups to be stored on the local or the network directory (default value is 2)
- *tapeid*

Requirements

Command privilege level: 1

Allowed during upgrade: No

Examples:

```
admin:utils disaster_recovery device add local localBackup 3

admin:utils disaster_recovery device add network networkDevice /root
10.77.31.116 root 3

admin:utils disaster_recovery device add tape tapeDevice /dev/nst0
```

utils disaster_recovery device delete

This command deletes the specified device.

Command syntax

utils disaster_recovery device delete [*device_name*|*]

Parameters

- *device_name* is mandatory and specifies the name of the device to be deleted.

Usage Guidelines

This command deletes all the existing devices except for the ones associated to a schedule.

Requirements

Command privilege level:1

Allowed during upgrade:No

utils disaster_recovery device list

This command display the device name, device type and device path for all the backup device.

Command syntax

utils disaster_recovery device list

Parameters

None

Requirements

Command privilege level:1

Allowed during upgrade:Yes

utils disaster_recovery restore local

This command invokes the restore and takes the tar file from network drive.

Command syntax

utils disaster_recovery restore local *restore_server tarfilename device_name*

Parameters

- *restore_server* is mandatory and represents the hostname of the server to be restored.
- *tarfilename* is mandatory and specifies the file that will get restored (without the file extension, for example: 2008-01-21-18-25-03).
- *device_name* is mandatory and specifies the name of the backup device to be added.

Usage Guidelines

Use **utils disaster_recovery device list** to display the configured device list.

Requirements

Command privilege level:1

Allowed during upgrade:No

Example

```
admin:utils disaster_recovery restore local SW075B-CM11 2008-01-21-18-25-03 localdevice
Restore initiated successfully.Please run 'utils showstatus restore' command to see the
status.
```

utils disaster_recovery restore tape

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

Command syntax

utils disaster_recovery restore tape *server tarfilename tapeid*

Parameters

- *server* specifies the hostname of the server that you want to restore.
- *tarfilename* specifies the name of the file to restore.
- *tapeid* specifies the name of the tape device from which to perform the restore job.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

utils disaster_recovery restore network

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

Command Syntax

utils disaster_recovery restore network *restore_server tarfilename path servername username*

Parameters

- *restore_server* specifies the hostname of the server that you want to restore.
- *tarfilename* specifies the name of the file to restore.
- *path* represents the location of the backup files on the remote server.
- *servername* represents the IP address or host name of the server where you stored the backup files.
- *username* represents the username that is needed to log in to the remote server.

Usage Guidelines

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

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

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

Requirements

Command privilege level:1

Allowed during upgrade:No

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.
```

utils disaster_recovery show_backupfiles local

Command syntax

utils disaster_recovery show_backupfiles local backup|restore

Parameters

- *directory*—name of the local backup/restore directory

Requirements

Command privilege level:1

Allowed during upgrade:Yes

Example:

```
admin:utils disaster_recovery show_backupfiles local backup/restore
2009-05-14-21-12-00
2009-05-16-21-12-00
```

utils disaster_recovery show_backupfiles tape

This command retrieves information of backup files available on tape.

Command syntax

utils disaster_recovery show_backupfiles tape *tapeid*

Parameters

- *tapeid* is mandatory and specifies the tape from which to display backup files.

Usage Guidelines

To display the list of tape IDs, execute the **utils disaster_recovery show_tapeid** command.

Requirements

Command privilege level:1

Allowed during upgrade:Yes

Example

```
admin:utils disaster_recovery show_backupfiles tape /dev/nst0
20050426181203853
```

utils disaster_recovery show_backupfiles network

This command retrieves information about backup files available on the network drive.

Command syntax

utils disaster_recovery show_backupfiles network *path servername userid*

Parameters

- *path* is mandatory and specifies the path to the backupfiles location.
- *servername* is mandatory and specifies the server IP address/hostname where the backup file is stored.
- *userid* is mandatory and specifies the user ID used to connect to the remote machine.

Requirements

Command privilege level:1

Allowed during upgrade:Yes

Example

```
admin:utils disaster_recovery show_backupfiles network /usr/local/ 10.77.31.55
administrator
Please enter password to connect to network server 10.77.31.55:****
20050426181203855
20050426181203853
20050426181203857
```

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.
- **[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 firewall ipv4

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 IPv6 firewall. If you do not enter the *time* parameter, this command disables the firewall for 5 minutes.
- **enable** turns on the IPv6 firewall.
- **list** displays the current configuration of the firewall.
- **status** displays the current status of the firewall.
- *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 firewall ipv6

This commands sets options and displays status for the IPv6 network firewall.

Note IPv6 is not supported in Cisco Unified Communications Manager Business Edition or Cisco Unity Connection.

Command Syntax

utils firewall ipv6

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 IPv6 firewall. If you do not enter the *time* parameter, this command disables the firewall for 5 minutes.
- **enable** turns on the IPv6 firewall.
- **list** displays the current configuration of the firewall.
- **status** displays the current status of the firewall.
- *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 iostat

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

Command Syntax

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

Parameters

- *interval* represents the value in seconds between two iostat readings (mandatory if you specify the number of iterations)
- *iterations* represents the number of iostat iterations to be performed (mandatory if you specify an interval)
- *filename* redirects the output to a file

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils iothrottle

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

Command Syntax

utils iothrottle {enable | disable | status}

Parameters

- **enable** turns on the I/O throttling enhancements. When enabled, I/O throttline enhancements lower the impact of upgrades on an active system.
- **disable** turns off the I'O throttling enhancements. This could adversely affect the system during upgrades.
- **status** displays the status of I/O throttling enhancements.

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils iothrottle threshold low

This command modifies the low iowait threshold used by the iowait monitor tool during upgrades.

Command syntax

utils iothrottle threshold low *value*

Parameters

- *value* is mandatory and specifies a value between 10 and 35.

Usage Guideline

Do not use this tool without Cisco Support supervision.

Requirements

Command privilege level:1

Allowed during upgrade:No

utils iothrottle threshold clear

This command clears the low iowait threshold that got configured via the **utils iothrottle threshold low** command.

Command syntax

utils iothrottle threshold clear

Usage Guidelines

Do not use this tool without Cisco Support supervision.

Requirements

Command privilege level:1

Allowed during upgrade:No

utils iothrottle threshold status

This command displays the current custom iowait threshold set by the **utils iothrottle threshold low** command.

Command syntax

utils iothrottle threshold status

Usage Guideline

Do not use this tool without Cisco Support supervision.

Requirements

Command privilege level:1

Allowed during upgrade:Yes

utils netdump client

This command configures the netdump client.

Command Syntax

utils netdump client

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

status

stop

Parameters

- **start** starts the netdump client.

- **status** displays the status of the netdump client.
- **stop** stops the netdump client.
- *ip-address-of-netdump-server* specifies the IP address of the netdump server to which the client will send diagnostic information.

Usage Guidelines

If a kernel panic crash occurs, the netdump client sends diagnostic information about the crash to a netdump server.

Requirements

Command privilege level: 0

Allowed during upgrade: No

utils netdump server

This command configures the netdump server.

Command Syntax

utils netdump server

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

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

list-clients

start

status

stop

Parameters

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

Usage Guidelines

If a kernel panic crash occurs, a netdump-enabled client system sends diagnostic information about the crash to the netdump server.

The netdump diagnostic information gets stored in the following location on the netdump server: *crash/*. The subdirectories whose names comprise a client IP address and a date contain netdump information.

You can configure each Cisco Unified Communications Operating System server as both a netdump client and server.

If the server is on another Cisco Unified Communications Operating System server, only the kernel panic trace signature gets sent to the server; otherwise, an entire core dump gets sent.

Requirements

Command privilege level: 0

Allowed during upgrade: No

Parameters

- **list** lists the contents of the address resolution protocol table.
- **set** sets an entry in the address resolution protocol table.
- **delete** deletes an entry in the address resolution table.
- *host* represents the host name or IP address of the host to add or delete to the table.
- *address* represents the MAC address of the host to be added. Enter the MAC address in the following format: XX:XX:XX:XX:XX:XX.

Options

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

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils network arp

This command lists the contents of the Address Resolution Protocol table.

Command syntax

utils network arp

list [**host** *hostname*][*options*]

Command privilege level: 0

Allowed during upgrade:Yes

set host *addr*

Command privilege level:1

Allowed during upgrade:No

delete *host*

Command privilege level:1

Allowed during upgrade:Yes

Options

- *host* (optional) specifies host you want to list/set/delete.
- *hostname* (optional) the hostname of the specified host.

- *options* (optional) *page*, *numeric*
  - *page* pauses output.
  - *numeric* shows hosts as dotted IP addresses.
- *addr* (mandatory) the hardware address (MAC) of the host.

  Format XX:XX:XX:XX:XX:XX

  Format XX:XX:XX:XX:XX:XX

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 ipv6

This command displays information about a specified IPv6 address or hostname.

Command syntax

utils network ipv6

ping {*IPv6-address* | *hostname*} [*count*]

traceroute {*IPv6-address* | *hostname*}

host {*IPv6-address* | *hostname*}

Parameters

- **ping** pings the specified IPv6 address or hostname.
- **traceroute** traceroutes the specified IPv6 address or hostname.

- **host** looks up the specified IPv6 address or hostname.
- *IPv6-address* specifies the IPv6 address about which to get information.
- *hostname* specifies the hostname about which to get information.
- *count* specifies the number of ICMPv6 message that will get exchanged. Default specifies 4.

Usage Guidelines

The hostname must resolve to a valid IPv6 address.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

utils network ping

This command allows you to ping another server.

Command Syntax

utils network ping *destination* [*count*]

Parameters

- *destination* represents the hostname or IP address of the server that you want to ping.

Options

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

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils network traceroute

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

Command Syntax

utils network tracert *destination*

Parameters

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

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils ntp

This command displays the NTP status or configuration.

Command Syntax

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

Note To avoid potential compatibility, accuracy, and network jitter problems, the external NTP servers that you specify for the primary node should be NTP v4 (version 4). If you are using IPv6 addressing, external NTP servers must be NTP v4.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils ntp restart

This command restarts the NTP service.

Command Syntax

utils ntp restart

Parameters

None

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils ntp server add

The command adds up to 5 specified NTP servers.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

Command syntax

utils ntp server add *s1* [*s2 s3 s4 s5*] [**norestart**]

Parameters

- at least one (and up to 5) ntp server to add.
- **norestart** results in the NTP service not being restarted after the server gets added.

Usage Guidelines

If the norestart parameter gets used, an explicit restart of the NTP service is required for the changes to take effect.

Example: Adding servers with incorrect command line parameters

```
------------------------------------------------------------
admin:utils ntp server add s1 s2 s3 s4 s5 s6 s7 s8
Incorrect number of parameters entered for add
usage: utils ntp server add s1 [s2 s3 s4 s5] [norestart]
admin:
```

Example: Adding using norestart without specifying a server

```
------------------------------------------------------------
admin:utils ntp server add norestart
At least one NTP server must be specified for add operation.
usage: utils ntp server add s1 [s2 s3 s4 s5] [norestart]
```

Example: Adding servers without norestart

```
----------------------------------------
admin:utils ntp server add clock1.cisco.com clock2.cisco.com
clock1.cisco.com :  added successfully.
clock2.cisco.com :  added successfully.
Restarting NTP on the server.
```

Example: Adding servers that are already added, without norestart

```
------------------------------------------------------------
admin:utils ntp server add clock1.cisco.com clock2.cisco.com
clock1.cisco.com : [The host has already been added as an NTP server.]
clock2.cisco.com : [The host has already been added as an NTP server.]
admin:
```

Example: Adding server to self without norestart

```
-----------------------------------------------
admin:utils ntp server add bglr-ccm26
bglr-ccm26 : [This server cannot be added as an NTP server.]
admin:
```

Example: Adding inaccessible server without norestart

```
-------------------------------------------------------
admin:utils ntp server add clock3.cisco.com
clock3.cisco.com : [ Inaccessible NTP server. Not added. ]
admin:
```

Example: Adding servers with norestart

```
-------------------------------------
admin:utils ntp server add ntp01-syd.cisco.com ntp02-syd.cisco.com clock.cisco.com
norestart
ntp01-syd.cisco.com :  added successfully.
ntp02-syd.cisco.com :  added successfully.
clock.cisco.com :  added successfully.
The NTP service will need to be restarted for the changes to take effect.
```

Example: Adding servers when 5 are already configured

```
-------------------------------------------------
admin:utils ntp server add clock3.cisco.com
The maximum permissible limit of 5 NTP servers is already configured.
admin:
```

utils ntp server delete

This command deletes NTP servers.

Command syntax

utils ntp server delete

Parameters

None

Usage Guidelines

When you execute this command, you have the option to delete any configured NTP server or all of them. After you enter your choice, you have the option to restart the NTP service. If you choose No, the NTP service does not restart after deleting the server(s).

If you choose not to restart the NTP service, an explicit restart of the NTP service is required for the changes to take effect.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

Example: Deleting servers with incorrect command line parameters

```
------------------------------------------------------------
admin:utils ntp server delete clock1.cisco.com clock2.cisco.com
Incorrect number of optional parameters entered for delete
usage: utils ntp server delete
admin:
```

Example: Deleting single server with ntp restart

```
-----------------------------------------------
admin:utils ntp server delete
1: clock1.cisco.com
2: clock2.cisco.com
3: ntp01-syd.cisco.com
4: ntp02-syd.cisco.com
5: clock.cisco.com
a: all
q: quit

Choice: 1

Restart NTP (y/n): y

clock1.cisco.com will be deleted from the list of configured NTP servers.
Continue (y/n)?y

clock1.cisco.com :  deleted successfully.
Restarting NTP on the server.
admin:
```

Example: Deleting all servers without ntp restart

```
------------------------------------------------
admin:utils ntp server delete
1: clock1.cisco.com
2: clock2.cisco.com
3: ntp01-syd.cisco.com
4: ntp02-syd.cisco.com
5: clock.cisco.com
a: all
q: quit

Choice: a

Restart NTP (y/n): n

This will result in all the configured NTP servers being deleted.
Continue (y/n)?y

clock1.cisco.com :  deleted successfully.
clock2.cisco.com :  deleted successfully.
ntp01-syd.cisco.com :  deleted successfully.
ntp02-syd.cisco.com :  deleted successfully.
clock.cisco.com :  deleted successfully.
The NTP service will need to be restarted for the changes to take effect.
admin:
```

Example: Deleting all servers when no servers are configured

```
------------------------------------------------------------
admin:utils ntp server delete
There are no NTP servers configured to delete.
admin:
```

utils ntp server list

This command displays a list of the configured ntp servers.

Command syntax

utils ntp server list

Parameters

None

Requirements

Command privilege level:0

Allowed during upgrade:Yes

Example: Listing servers with incorrect command line parameters

```
------------------------------------------------------------------
admin:utils ntp server list all
Incorrect optional parameter entered for list
usage: utils ntp server list
admin:
```

Example: Listing servers

```
------------------------
```

```
admin:utils ntp server list
clock1.cisco.com
clock2.cisco.com
ntp01-syd.cisco.com
ntp02-syd.cisco.com
clock.cisco.com
admin:
```

Example: Listing servers when no servers are configured

```
------------------------------------------------------
admin:utils ntp server list
There are no NTP servers configured.
```

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

Command privilege level: 0

Allowed during upgrade: Yes

utils ntp status

This command displays the current status of NTP.

Command Syntax

utils ntp status

Parameters

None

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Example

```
admin:utils ntp status
ntpd (pid 18705) is running...
```

```
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 127.127.1.0     LOCAL(0)        10 l   12   64  377    0.000    0.000   0.004
+171.68.10.80    10.81.254.131    2 u  331 1024  377   35.201   -0.498   0.673
*10.81.254.131   .GPS.            1 u  356 1024  377   64.304   -0.804   0.638


synchronised to NTP server (10.81.254.131) at stratum 2
   time correct to within 37 ms
   polling server every 1024 s

Current time in UTC is : Thu Feb 12 22:33:43 UTC 2009
Current time in America/Los_Angeles is : Thu Feb 12 14:33:43 PST 2009

The 'remote' column lists the remote NTP servers.  The local hardware clock is
configured as 127.127.1.0 and is always shown, even when not active.

The leftmost column below the 'remote' column header has the following meaning:
  " " discarded due to high stratum and/or failed sanity checks
  "+" a candidate NTP server and included in the final selection set
  "*" selected for synchronization

Any other values indicate the NTP server is not being used for synchronization.
Other possible values are:
  "x" designated false ticker (is an invalid NTP server)
  "." culled from the end of the candidate list (is considered non viable)
  "-" discarded
  "#" selected for synchronization, but has high delay, offset or jitter

The 'refid' column indicates the remote's time source.  "LOCAL(0)" applies to
the local hardware clock.  ".INIT." means initialization has not yet succeeded.

The 'st' column is the stratum of the remote NTP server.  16 is a invalid
stratum value meaning "this server is not considered a time provider".
This can be for various reasons, the most common reasons are "time provider not
synchronized", "configured source does not exist" or "ntp server not running".

The 'when' column indicates how many seconds ago the remote was queried.

The 'poll' column indicates the polling interval in seconds.  E.G., '64' means
the remote is being polled every 64 seconds.  The shortest interval NTP uses
is every 64 seconds and the longest is 1024 seconds.  The better a NTP source
is rated over time, the longer the interval.

The 'reach' column indicates the trend of reachability tests in octal, where
each digit, when converted to binary represents whether a particular poll was
successful (binary 1) or unsuccessful (binary 0).  E.G., '1' means only one
poll has been done thus far and it was successful.  '3' (= binary 11) means the
last 2 polls were successful.  '7' (= binary 111) means the last 3 polls were
successful.  '17' (= binary 1 111) means the last 4 polls were successful.
'15' (= binary 1 101) means the last 2 polls were successful, the poll prior to
that was unsuccessful, and the poll prior to that was successful.

When a poll is done for the active NTP server selected for synchronization is
done, a time correction using that NTP server's time is also done.

The delay, offset and jitter are the round-trip delay, dispersion, and jitter
in seconds.

"At stratum #" shown below the table shows the stratum of this host's NTP
server, which will be one higher than that of the currently active NTP server
being used for synchronization.
```

utils ntp server add

The command adds a maximum of 5 specified NTP server(s).

Command syntax

utils ntp server add s1 [s1 | s2 | s3 | s4 | s5] [**norestart**]

Parameters

- **norestart** causes the NTP service to not restart after adding the server(s).

Usage Guidelines

If **norestart** gets used, an explicit restart of the NTP service is required for the changes to take effect.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

Example: Attempting to add servers with incorrect command line parameters

```
------------------------------------------------------------
admin:utils ntp server add s1 s2 s3 s4 s5 s6 s7 s8
Incorrect number of parameters entered for add
usage: utils ntp server add s1 [s2 s3 s4 s5] [norestart]
admin:
```

Example: Attempting to add a server using norestart without specifying a server

```
------------------------------------------------------------
admin:utils ntp server add norestart
At least one NTP server must be specified for add operation.
usage: utils ntp server add s1 [s2 s3 s4 s5] [norestart]
```

Example: Adding servers without norestart

```
---------------------------------------
admin:utils ntp server add clock1.cisco.com clock2.cisco.com
clock1.cisco.com :  added successfully.
clock2.cisco.com :  added successfully.
Restarting NTP on the server.
```

Example: Adding servers that are already added, without norestart

```
------------------------------------------------------------------
admin:utils ntp server add clock1.cisco.com clock2.cisco.com
clock1.cisco.com : [The host has already been added as an NTP server.]
clock2.cisco.com : [The host has already been added as an NTP server.]
admin:
```

Example: Adding server to self without norestart

```
-----------------------------------------------
admin:utils ntp server add bglr-ccm26
bglr-ccm26 : [This server cannot be added as an NTP server.]
admin:
```

Example: Adding inaccessible server without norestart

```
-------------------------------------------------
admin:utils ntp server add clock3.cisco.com
clock3.cisco.com : [ Inaccessible NTP server. Not added. ]
```

```
admin:
```

Example: Adding servers with norestart

```
------------------------------------
admin:utils ntp server add ntp01-syd.cisco.com ntp02-syd.cisco.com clock.cisco.com
norestart
ntp01-syd.cisco.com :  added successfully.
ntp02-syd.cisco.com :  added successfully.
clock.cisco.com :  added successfully.
The NTP service will need to be restarted for the changes to take effect.
```

Example: Adding servers when 5 are already configured

```
-------------------------------------------------
admin:utils ntp server add clock3.cisco.com
The maximum permissible limit of 5 NTP servers is already configured.
admin:
```

utils ntp server delete

This command deletes configured NTP servers.

Command syntax

utils ntp server delete

Parameters

None

Usage Guidelines

This command results in the option to delete a configured NTP server or all of them. When you choose the server to delete, you get prompted to indicate if you want to restart the NTP service. If you choose no, the NTP service does not get restarted after the server gets deleted.

If you chose not to restart the NTP service, an explicit restart of the NTP service is required for the changes to take effect.

Requirements

Command privilege level:0

Allowed during upgrade:Yes

Example: Deleting servers with incorrect command line parameters

```
-------------------------------------------------------------
admin:utils ntp server delete clock1.cisco.com clock2.cisco.com
Incorrect number of optional parameters entered for delete
usage: utils ntp server delete
admin:
```

Example: Deleting single server with ntp restart

```
-----------------------------------------------
admin:utils ntp server delete
1: clock1.cisco.com
2: clock2.cisco.com
3: ntp01-syd.cisco.com
4: ntp02-syd.cisco.com
5: clock.cisco.com
```

```
a: all
q: quit

Choice: 1

Restart NTP (y/n): y

clock1.cisco.com will be deleted from the list of configured NTP servers.
Continue (y/n)?y

clock1.cisco.com :  deleted successfully.
Restarting NTP on the server.
admin:
```

Example: Deleting all servers without ntp restart

```
------------------------------------------------
admin:utils ntp server delete
1: clock1.cisco.com
2: clock2.cisco.com
3: ntp01-syd.cisco.com
4: ntp02-syd.cisco.com
5: clock.cisco.com
a: all
q: quit

Choice: a

Restart NTP (y/n): n

This will result in all the configured NTP servers being deleted.
Continue (y/n)?y

clock1.cisco.com :  deleted successfully.
clock2.cisco.com :  deleted successfully.
ntp01-syd.cisco.com :  deleted successfully.
ntp02-syd.cisco.com :  deleted successfully.
clock.cisco.com :  deleted successfully.
The NTP service will need to be restarted for the changes to take effect.
admin:
```

Example: Deleting all servers when no servers are configured

```
------------------------------------------------------------
admin:utils ntp server delete
There are no NTP servers configured to delete.
admin:
```

utils ntp server list

The command displays a list of the configured ntp servers.

Command syntax

utils ntp server list

Parameters

None

Requirements

Command privilege level:0

Allowed during upgrade:Yes

Example: Listing servers with incorrect command line parameters

```
------------------------------------------------------------
admin:utils ntp server list all
Incorrect optional parameter entered for list
usage: utils ntp server list
admin:
```

Example: Listing servers

```
------------------------
admin:utils ntp server list
clock1.cisco.com
clock2.cisco.com
ntp01-syd.cisco.com
ntp02-syd.cisco.com
clock.cisco.com
admin:
```

Example: Listing servers when no servers are configured

```
-----------------------------------------------------
admin:utils ntp server list
There are no NTP servers configured.
admin:
```

utils raid disk maintenance

This command affects scheduled software RAID service.

Command syntax

utils raid disk maintenance [**disable | enable | status**]

Parameters

- **disable** - stops the scheduled software RAID service.
- **enable** - schedules the weekly disk verify utility on software RAID equipped servers. This utility will run at 4:22 AM Sunday mornings.
- **status** - displays the status of the weekly scheduled software RAID disk verify service.

Usage guidelines

Cisco recommends that you keep this feature enabled as a best practice to ensure drive health.

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 service

This command stops, starts, or restarts a service.

Command Syntax

utils service

start *service-name*

stop *service-name*

restart *service-name*

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

Parameters

- *service-name* represents the name of the service that you want to stop or start:
  - System NTP
  - System SSH
  - Service Manager
  - A Cisco DB
  - Cisco Tomcat
  - Cisco Database Layer Monitor
  - Cisco Unified Serviceability
- **auto-restart** causes a service to automatically restart.

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils service list

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

Command Syntax

utils service list [**page**]

Options

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

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils snmp

This command manages SNMP on the server.

Command Syntax

utils snmp

get *version community ip-address object* [*file*]

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

test

walk *version community ip-address object* [*file*]

Parameters

- **get** gets the SNMP data using the specified version(1 or 2c), for the specified MIB OID.
- **hardware-agents status** displays the status of the hardware agents on the server.
- **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 the SNMP MIB using the specified version(1 or 2c), starting with the specified MIB OID.

- *version* specifies the SNMP version. Possible values include 1 or 2c.
- *community* specifies the SNMP community string.
- *ip-address* specifies the IP address of the server. Enter 127.0.0.0 to specify the local host. You can enter the IP address of another node in the cluster to run the command on that node.
- *object* specifies the SNMP Object ID (OID) to get.
- *file* specifies a file in which to save the command output.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

utils snmp get 3

This command gets the SNMP data for the specified MIB OID.

Command Syntax

utils snmp get 3

[system will prompt you for the parameters]

Requirements

Command privilege level: 1

Allowed during upgrade: No

Usage Guidelines

- To get the value of a MIB, run this command on a specific OID (leaf) in the MIB.
- To execute this command on a remote host, provide the IP address of a remote host. Ensure that you provide the IP address of the remote host and not the domain name.

Example:

Following is the snmp get output of system uptime:

```
iso.3.6.1.2.1.25.1.1.0 = Timeticks: (19836825) 2 days, 7:06:08.25
```

utils snmp walk 3

This command is used to walk the SNMP MIB starting with the specified OID.

Command Syntax

utils snmp walk 3

[system will prompt you for the parameters]

Requirements

Command privilege level: 1

Allowed during upgrade: No

Usage Guidelines

- If you run snmp walk on a leaf in the MIB, output is same as that of the **utils snmp get** command.
- To execute this command on a remote host, provide the IP address of a remote host. Ensure that you provide the IP address of the remote host and not the domain name.

Example

Here is the sample walk output for the OID 1.3.6:

```
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"
iso.3.6.1.2.1.2.2.1.2.2 = STRING: "eth0"
iso.3.6.1.2.1.2.2.1.2.3 = STRING: "eth1"
iso.3.6.1.2.1.2.2.1.3.1 = INTEGER: 24
iso.3.6.1.2.1.2.2.1.3.2 = INTEGER: 6
iso.3.6.1.2.1.2.2.1.3.3 = INTEGER: 6
iso.3.6.1.2.1.2.2.1.4.1 = INTEGER: 16436
iso.3.6.1.2.1.2.2.1.4.2 = INTEGER: 1500
iso.3.6.1.2.1.2.2.1.4.3 = INTEGER: 1500
iso.3.6.1.2.1.2.2.1.5.1 = Gauge32: 0
iso.3.6.1.2.1.2.2.1.5.2 = Gauge32: 100000000
iso.3.6.1.2.1.2.2.1.5.3 = Gauge32: 10000000
iso.3.6.1.2.1.2.2.1.6.1 = Hex-STRING: 00 00 00 00 00 00
iso.3.6.1.2.1.2.2.1.6.2 = Hex-STRING: 00 16 35 5C 61 D0
iso.3.6.1.2.1.2.2.1.6.3 = Hex-STRING: 00 16 35 5C 61 CF
iso.3.6.1.2.1.2.2.1.7.1 = INTEGER: 1
```

utils snmp config inform 3 add

This command adds a new v3 inform notification destination that is associated with a configured v3 username.

Command syntax

utils snmp config inform 3 add {*ipaddress*} {*portno*} {*username*} {*authprotocol*} {*authpassphrase*} {*privprotocol*} {*privpassphrase*} {*accessprivilege*} {*engineId*}

Parameters

- *ipaddress* is mandatory and specifies the IP address of the notification destination

Note Do not specify the IP address of the server you are on.

- *portno* is mandatory and represents the port number.

- *username* is mandatory and represents the v3 user-name. A new inform user gets created. Check **utils snmp config user 3 list** for using existing inform users.
- *authprotocol* is mandatory and represents the authentication protocol (SHA).
- *authpassphrase* is mandatory and represents the authentication protocol pass phrase (minimum 8 characters).
- *privprotocol* [**AES128 | AES192 | AES256**] is mandatory and represents the privacy protocol.
- *privpassphrase* is mandatory and represents the privacy protocol pass phrase (minimum 8 characters).
- *accessprivilege[***ReadWriteNotify | NotifyOnly | ReadNotifyOnly**] is mandatory and represents the access privilege.
- *engineId* is mandatory and represents the remote engine ID of the server to which Inform is to be sent.

Note Do not specify engine ID of the server you are on.

Requirements

Command privilege level: 1

Allowed during upgrade:No

Example

```
utils snmp config inform 3 add 10.77.31.26 162 testuser SHA authpass AES128 privpass
ReadWriteNotify 00:00:00:63:00:00:00:a1:0a:4d:1f:1a
```

utils snmp config inform 3 delete

This command deletes the configuration information for an existing v3 inform notification destination.

Command syntax

utils snmp config inform 3 delete {*ipaddress*}{*portno*}{*username*}{*deletuserconf*}

Parameter

- *ipaddress* is mandatory and specifies the IP address of the notification destination.
- *portno* is mandatory and specifies the port number.
- *username* is mandatory and specifies the v3 user-name that is associated with the inform.
- *deletuserconf* [**Y** or **N**] is mandatory and specifies confirmation for deleting the old user.

Requirements

Command privilege level: 0

Allowed during upgrade:No

Example

```
utils snmp config inform 3 delete 10.77.31.26 162 testuser Y
```

utils snmp config inform 3 list

This command lists the v3 inform notifications currently configured

Command syntax

utils snmp config inform 3 list

Parameters

None

Requirements

Command privilege level: 0

Allowed during upgrade:No

utils snmp config inform 3 update

This command updates the configuration information for an existing v3 inform notification destination.

Command syntax

utils snmp config inform 3 update {*ipaddress*} {*oldportno*} {*newportno*} {*oldusername*} {*newusername*} {*deletuserconf*} {*authprotocol*} {*authpassphrase*} {*privprotocol*} {*privpassphrase*} {*accessprivilege*} {*engineId*}

Parameters

- *ipaddress* is mandatory and specifies the IP address of the notification destination.
- *oldportno* is mandatory and represents the old port number.
- *newportno* is mandatory and represents the new port number.
- *oldusername* is mandatory and represents the v3 user-name that is currently associated with the inform.
- *newusername* is mandatory and represents the v3 user-name that is to be newly associated with inform.
- *deletuserconf* [**Y** or **N**] is mandatory and represents confirmation for deleting the old user.
- *authprotocol* is mandatory and represents the authentication protocol (SHA).
- *authpassphrase* is mandatory and represents the authentication protocol pass phrase (minimum 8 characters).
- *privprotocol* [**AES128 | AES192 | AES256**] is mandatory and represents the privacy protocol.
- *privpassphrase* is mandatory and represents the privacy protocol pass phrase (minimum 8 characters).
- *accessprivilege* [**ReadWriteNotify | NotifyOnly | ReadNotifyOnly**] is mandatory.
- *engineId* is mandatory and represents the remote engine ID, of the server to which Inform is to be sent.

Note Do not specify engine ID of the server you are on.

Requirements

Command privilege level: 0

Allowed during upgrade:No

Example

```
utils snmp config inform 3 update 10.77.31.26 162 6162 testuser testuser1 Y SHA authpass
AES128 privpass ReadWriteNotify 00:00:00:63:00:00:00:a1:0a:4d:1f:1a
```

utils snmp config mib2 add

This command adds mib2 configuration information (for example, system contact and system location).

Command syntax

utils snmp config mib2 add *SysContact SysLocation*

Parameter

- *SysContact* is mandatory and represents the mib2 system contact information.
- *SysLocation* is mandatory and represents the mib2 system location information.

Requirements

Command privilege level: 1

Allowed during upgrade:No

Example

```
utils snmp config mib2 add cisco india
```

utils snmp config mib2 delete

This command deletes the mib2 configuration information (for example, system contact and system location).

Command syntax

utils snmp config mib2 delete

Parameters

None

Requirements

Command privilege level: 1

Allowed during upgrade:No

Example

```
utils snmp config mib2 delete cisco india
```

utils snmp config mib2 list

This command lists the mib2 configuration information (for example, system contact and system location).

Command syntax

utils snmp config mib2 list

Parameter

None

Requirements

Command privilege level: 1

Allowed during upgrade:No

Example

```
utils snmp config mib2 list cisco india
```

utils snmp config mib2 update

This command updates the mib2 configuration information (for example, system contact and system location.)

Command syntax

utils snmp config mib2 update SysContact SysLocation

Parameters

- *SysContact* is mandatory and represents the mib2 system contact information.
- *SysLocation* is mandatory and represents the mib2 system location information.

Requirements

Command privilege level: 1

Allowed during upgrade:No

Example

```
utils snmp config mib2 update cisco india
```

utils snmp config trap 3 add

This command adds a new v3 trap notification destination that is associated with a configured v3 username.

Command syntax

utils snmp config trap 3 add {*ipaddress*} {*portno*} {*username*}

Parameters

- *ipaddress* is mandatory and represents the IP address of the notification destination.
- *portno* is mandatory and represents the port number.
- *username* is mandatory and represents the v3 user-name.

Requirements

Command privilege level: 1

Allowed during upgrade:No

Example

```
utils snmp config trap 3 add 10.77.31.26 162 testuser
```

utils snmp config trap 3 update

This command updates the configuration information for an existing v3 trap notification destination.

Command syntax

utils snmp config trap 3 update {*ipaddress*} {*oldportno*} {*newportno*} {*oldusername*} {*newusername*}

Parameters

- *ipaddress* is mandatory and specifies the IP address of the notification destination.
- *oldportno* is mandatory and represents the old port number.
- *newportno* is mandatory and represents the new port number.
- *oldusername* is mandatory and represents the v3 user-name that is currently associated with the trap.
- *newusername* is mandatory and represents the v3 user-name that is to be newly associated with the trap.

Requirements

Command privilege level: 0

Allowed during upgrade:No

Example

```
utils snmp config trap 3 update 10.77.31.26 162 6162 testuser testuser1
```

utils snmp config trap 3

This command deletes the configuration information for an existing v3 trap notification destination

Command syntax

utils snmp config trap 3 delete {*ipaddress*} {*portno*} {*username*}

Parameters

- *ipaddress* is mandatory and specifies the IP address of the notification destination.

- *portno* is mandatory and specifies the port number.
- *username* is mandatory and specifies the v3 user-name that is associated with the trap.

Requirements

Command privilege level: 0

Allowed during upgrade:No

Example

```
utils snmp config trap 3 delete 10.77.31.26 162 testuser
```

utils snmp config trap 3 list

This command displays the v3 trap notifications currently configured

Command syntax

utils snmp config trap 3 list

Parameters

None

Requirements

Command privilege level: 0

Allowed during upgrade:No

utils snmp config user 3 add

This command adds a new v3 user with the v3 authentication and privacy passwords.

Command syntax

utils snmp config user 3 add {*username*} {*authprotocol*} {*authpassphrase*} {*privprotocol*} {*privpassphrase*} {*accessprivilege*} [*ipaddress1 ipaddress2*]

Parameters

- *username* is mandatory and specifies the v3 username.
- *authprotocol* is mandatory and specifies the authentication protocol (SHA).
- *authpassphrase* is mandatory and specifies the authentication protocol pass phrase (minimum 8 characters).
- *privprotocol* **[AES128 | AES192 | AES256]** is mandatory and specifies the privacy protocol.
- *privpassphrase* is mandatory and specifies the privacy protocol pass phrase (minimum 8 characters).
- *accessprivilege* **[ReadOnly | ReadWrite | ReadWriteNotify | NotifyOnly | ReadNotifyOnly | None]** is mandatory and specifies the access privilege.

Options

- *ipaddress1* specifies the IP addresses from which to accept packets. Default specifies to accept packets from all hosts.

- *ipaddress2* specifies the IP addresses from which to accept packets from. Default specifies to accept packets from all hosts.

Requirements

Command privilege level: 1

Allowed during upgrade:No

Example

```
utils snmp config user 3 add testuser SHA authpass AES128 privpass ReadWriteNotify
10.77.31.26 10.77.31.29
```

utils snmp config user 3 delete

Command syntax

utils snmp config user 3 delete *username*

Parameter

*username*is mandatory and represents the v3 username.

Requirements

Command privilege level: 0

Allowed during upgrade:No

Example

```
utils snmp config user 3 delete testuser
```

utils snmp config user 3 list

This command lists the v3 users currently configured.

Command syntax

utils snmp config user 3 list

Parameters

None

Requirements

Command privilege level: 0

Allowed during upgrade:No

utils snmp config user 3 update

This command updates the configuration information for an existing v3 user

Command syntax

utils snmp config user 3 update {*username*} {*authprotocol*} {*authpassphrase* {*privprotocol*} {*privpassphrase*} {*accessprivilege*} [*ipaddress1 ipaddress2*]

Parameters

- *username* is mandatory and specifies the v3 username.
- *authprotocol* is mandatory and specifies the authentication protocol (SHA).
- *authpassphrase* is mandatory and specifies the authentication protocol pass phrase (minimum 8 characters).
- *privprotocol* [**AES128 | AES192 | AES256]** is mandatory and specifies the privacy protocol.
- *privpassphrase* is mandatory and specifies the privacy protocol pass phrase (minimum 8 characters).
- *accessprivilege* [**ReadOnly | ReadWrite | ReadWriteNotify | NotifyOnly | ReadNotifyOnly | None]** is mandatory and specifies the access privilege.

Options

- *ipaddress1* specifies the IP addresses from which to accept packets. Default specifies to accept packets from all hosts.
- *ipaddress2* specifies the IP addresses from which to accept packets from. Default specifies to accept packets from all hosts.

Requirements

Command privilege level: 0

Allowed during upgrade:No

Example

```
utils snmp config user 3 update testuser SHA authpass AES128 privpass ReadWriteNotify
10.77.31.26 10.77.31.29
```

utils snmp test

This command sends snmp test sample alarms to local syslog, remote syslog and SNMP trap.

Command syntax

utils snmp test

Parameters

None

Requirements

Command privilege level: 0

Allowed during upgrade:Yes

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 provides a 5-minute timeout. If the system does not shut down within 5 minutes, the command gives you the option of doing a forced shutdown.

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils system boot

This commands redirects where the system boot output gets sent.

Command Syntax

utils system boot {console | serial | status}

Parameters

- **console** redirects the system boot output to the console.
- **serial** redirects the system boot output to the COM1 (serial port 1).
- **status** displays the where the serial boot output will currently get sent.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

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 {initiate | cancel | status}

Parameters

- **cancel** cancels the active upgrade.
- **initiate** starts a new upgrade wizard or assumes control of an existing upgrade wizard. The wizard prompts you for the location of the upgrade file.
- **status** displays the status of an upgrade.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

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

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Cisco Product Security Overview

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)