CLI Commands

- Delete Commands, on page 1
- File Commands, on page 4
- Run and Set commands, on page 11
- Show Commands, on page 48
- Unset Commands, on page 75
- Utils Commands, on page 77

Delete Commands

delete account

This command allows you to delete an administrator account.

Command Syntax

delete account *account-name*

Syntax Description

Parameters	Description
account-name	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.

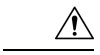
Command Syntax

delete dns *ip-address*

Syntax Description

Parameters	Description
ip-address	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 dscp

This command deletes a DSCP port tag.

Command Syntax

delete dscp *[port-tag]*

Syntax Description

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

Useage Guideline

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

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

Command Mode

Administrator (admin:)

delete ipsec

This command allows you to delete IPsec policies and associations.

Command Syntax

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

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

Syntax Description

Parameters	Description
policy-name	An IPsec policy.
association-name	An IPsec association

Requirements

Command privilege level: 1

Allowed during upgrade: No

delete process

This command allows you to delete a particular process.

Command Syntax

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

Syntax Description

Parameters	Description
process-id	The process ID number.
force	(Optional) Tells the process to stop.
terminate	(Optional) Tells the operating system to terminate the process.
crash	(Optional) Crashes the process and produces a crash dump.

Usage Guidelines

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

File Commands

file check

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

Command Syntax

file check *[detection-size-kb]*

Syntax Description

Parameters	Description
[detection-size-kb]	Specifies the minimum file size change that is required for the command to display the file as changed. Default value: 100 KB.

Usage Guidelines

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

Caution This command can affect system performance. We recommend that you use the command during off-peak hours.

Requirements

Command privilege level: 0

Allowed during upgrade: No

file delete

This command deletes one or more files.

Command Syntax

file delete {**activelog**|**inactivelog**|**install**} *directory/filename* [**detail**] [**noconfirm**]

Syntax Description

Parameters	Description
activelog	A log on the active side.
inactivelog	A log on the inactive side.
install	An installation log.
directory/filename	The path and filename of the files to delete. You can use the wildcard character (*) for "filename".
detail	(Optional) Shows a listing of deleted files with the date and time.
noconfirm	(Optional) 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.

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** |**inactivelog** |install } *directory/filename* [**detail**] [**hex**] [**recent**] [**regexp***expression*]

Syntax Description

Parameters	Description
activelog	A log on the active side.
inactivelog	A log on the inactive side.
install	An installation log
directory/filename	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.
detail	(Optional) Displays listing with the date and time.
hex	(Optional) Displays output in hexadecimal.
recent	(Optional) Displays the most recently modified file in the directory.
regexp *expression*	(Optional) Displays only the lines in the file that match the regular expression

Requirements

Command privilege level: 1 for logs

Allowed during upgrade: Yes

Example

This command dumps contents of file _cdrIndex.idx:

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

file get

This command sends a log to another system using SFTP.

Command Syntax

file get {**activelog** |**inactivelog** |**install**|**partBsalog**|**salog** } *directory/filename* [**reltime**|**abstime**] [**match**][**recurs**]

Syntax Description

Parameters	Description
activelog	A log on the active side.
inactivelog	A log on the inactive side.
install	An installation log.

Parameters	Description
partBsalog	The partBsalog log directory.
salog	The salog log directory.
directory/filename	the path to the files to delete. You can use the wildcard character (*) for filename as long as it resolves to one file.
abstime	(Optional) The absolute time period, specified as hh:mm:MM/DD/YY hh:mm:MM/DD/YY.
reltime	(Optional) The relative time period, specified as months|weeks| days| hours| minutes value.
match	(Optional) Match a particular string in the filename, specified as string value.
recurs	(Optional) Get all files, including subdirectories.

Usage Guidelines

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

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Examples

This command gets all files in the activelog operating system directory that match the string plat:

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

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

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

file list

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

Command Syntax

file list {**activelog**|**inactivelog**|**install**|**partBsalog**|**salog**} *directory/filename*[**page**|**detail**|**reverse**] [**date** | **size**]

Syntax Description

Parameters	Description
activelog	A log on the active side.
inactivelog	A log on the inactive side.

Parameters	Description
install	An installation log.
partBsalog	The partBsalog log directory.
salog	The salog log directory.
directory	The path to the directory to list. You can use a wildcard character (*) for directory as long as it resolves to one directory.
page	(Optional) Shows the output one screen at a time.
detail	(Optional) Shows a detailed listing with date and time.
reverse	(Optional) Reverse the sort direction.
date	(Optional) Sorts by date.
size	(Optional) Sorts by file size.

Requirements

Command privilege level: 1 for logs

Allowed during upgrade: Yes

Examples

This example lists operating system log files with details:

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

This example lists directories created for Emergency Responder logs:

```
file list activelog er/logs
```

This example lists Emergency Responder logs in a specified directory by size:

```
file list activelog er/logs size
```

file search

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

Command Syntax

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

Syntax Description

Parameters	Description
activelog	A log on the active side.

Parameters	Description
inactivelog	A log on the inactive side.
install	An installation log.
directory/filename	The path to the files to search. You can use the wildcard character (*) to represent all or part of the filename.
reg-exp	A regular expression.
abstime	(Optional) The files to search based on file creation time. Enter a start time and an end time.
days|**hours**|**minutes**	(Optional) The file age is in days, hours, or minutes.
ignorecase	(Optional) Ignores case when searching
reltime	(Optional) The files to search based on file creation time. Enter the age of files to search.
hh:mm:ss mm/dd/yyyy	(Optional) An absolute time, in the format hours:minutes:seconds month/day/year.
timevalue	(Optional) The age of files to search. The unit of this value is specified with the {**days** | **hours** | **minutes**} option.

Usage Guidelines

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

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

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Example

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

file tail

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

Command Syntax

file tail {**activelog** |**inactivelog** |**install** } *directory/filename*[**detail**] [**hex**] [**lines**]

Syntax Description

Parameters	Description
activelog	A log on the active side.
inactivelog	A log on the inactive side.
install	An installation log.
directory/filename	The path to the file to tail. You can use the wildcard character (*) for filename as long as it resolves to one file.
detail	(Optional) Long listing with date and time
hex	(Optional) Hexadecimal listing
lines	(Optional) Number of lines to display

Requirements

Command privilege level: 1 for logs

Allowed during upgrade: Yes

Example

This example tails the operating system CLI log file:

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

file view

This command displays the contents of a file.

Command Syntax

file view {**activelog**|**inactivelog**|**install**|**system-management-log**}*directory/filename*

Syntax Description

Parameters	Description
activelog	A log on the active side.
inactivelog	A log on the inactive side.
install	An installation log.
system-management-log	The contents of the Integrated Management Logs (IML).
directory/filename	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 er/logs/CERAdmin01.log
```

Run and Set commands

run sql

This command allows you to run an SQL command.

Command Syntax

run sql *sql_statement*

Syntax Description

Parameters	Description
sql_statement	The SQL command to run.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Examples

This example runs an SQL command:

```
run sql select * from cerserver
```

set account

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

Command Syntax

set account *name*

Syntax Description

Parameters	Description
name	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 is used to enable the user account if the account is disabled due to the password inactivity feature.

Password inactivity period is the number of days of inactivity after a password has expired before the account is disabled.

After entering this command, the user account is enabled with current system settings.The system settings are Password min days, Password Max days, Password inactivity period.

Command Syntax

set account enable *userid*

Syntax Description

Parameters	Description
userid	The name of the user account.

Example

This example runs a set account enable command:

```
set account enable test
Enabling the account 'test' with current settings....
.....
```

```
Successfully enabled account 'test'
```

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show accountlocking

This command shows the current account locking settings.

Command Syntax

show accountlocking

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

set accountlocking disable

This command disables accountlocking for the current administrator accounts.

Command Syntax

set accountlocking disable

Syntax Description

Parameters	Description
disable	Disable account locking.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

set accountlocking enable

This command enables accountlocking for the current administrator accounts.

Command Syntax

set accountlocking enable

Syntax Description

Parameters	Description
enable	Enable account locking.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

set accountlocking unlocktime

This command configures the unlock time for Emergency Responder OS administrator accounts in seconds. Acceptable values should be equal to or greater than 300 seconds, but less than 3600 seconds (60 mins).

Command Syntax

set accountlocking unlocktime *seconds*

Syntax Description

Parameters	Description
seconds	The unlocktime in seconds.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

set cert delete

This command deletes the certificate test.pem for the unit IPsec.

Command Syntax

set cert delete *[unit] [name]*

Syntax Description

Parameters	Description
unit	The name of the trust category.
name	The certificate file name.

Example

```
set cert
    delete ipsec test.pem
```

Requirements

Command privilege level: 1

Allowed during upgrade: No

set cert import

This command imports the certificate for a specific unit | trust.

Command Syntax

set cert import [*unit name*]

Syntax Description

Parameters	Description
unit name	The name of the unit or trust.

Example

The following example runs a set cert import command:

```
set cert
    import trust tomcat

Successfully regenerated certificate for tomcat.
Please restart services related to tomcat for the new certificate to become active.
```

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

set cert regen

This command regenerates the certificate for the unit.

Command Syntax

set cert regen [*name*]

Parameter

Name is unit name

Syntax Description

Parameters	Description
Name	The name of the unit.

Example

This example runs a set cert regen command:

```
set cert regen tomcat
Successfully regenerated certificate for tomcat.
Please restart services related to tomcat for the new certificate to become active.
```

Requirements

Command privilege level: 1

Allowed during upgrade: No

set cli pagination

For the current CLI session, this command turns automatic pagination on or off.

Command Syntax

set cli pagination {on | off}

Syntax Description

Parameters	Description
on	Turns pagination on.
off	Turns pagination off.

Requirements

Level privilege: 1

Command privilege: 1

Allowed during upgrade: No

Example

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

set cli session timeout

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

Command Syntax

set cli session timeout*minutes*

Syntax Description

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

Useage Guidelines

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

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

Command Mode

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

set commandcount

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

Command Syntax

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

Syntax Description

Parameters	Description
enable	Turns on command count.
disable	Turns off command count.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set csr gen

It regenerates the certificate for the unit name.

Command Syntax

set csr gen *name*

Syntax Description

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

Example

set csr gen tomcat

Successfully regenerated certificate for tomcat.

Please restart services related to tomcat for the new certificate to become active.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set date

This command sets the date on the system.

Command Syntax

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

Syntax Description

Parameters	Description
HH:mm:ss	Represents the time format (24 hours format).
MM/DD/YY	Represents the date format. This date format is also accepted: **MM/DD/YYYY**.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Example

To set date and time to 2:10:33 p.m. February 13, 2008:

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

set dscp

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

Command Syntax

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

Syntax Description

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

Command Mode

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

set dscp defaults

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

Command Syntax

set dscp defaults

Command Mode

Administrator (admin:)

Useage Guidelines

This command removes all non-default DSCP settings. The command **show dscp defaults** displays the factory default DSCP settings.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set dscp marking

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

Command Syntax

set dscp marking *port_tag value*

Syntax Description

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

Command Mode

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Useage Guidelines

The valid class names as defined by DSCP are:

- Class Selector: values CS0, CS1, CS2, CS3, CS5, CS6, CS7 The class selector (CS) values correspond to IP Precedence values and are fully compatible with IP Precedence.

- Expedited Forwarding: value EF EF PHB is ideally suited for applications such as VoIP that require low bandwidth, guaranteed bandwidth, low delay, and low jitter.
- Best Effort: value BE Also called default PHB, this value essentially specifies that a packet be marked with 0x00, which gets the traditional best-effort service from the network router.
- Assured Forwarding: values AF11, AF12, AF13, AF21, AF22, AF23, AF41, AF42, AF43 There are four types of Assured Forwarding classes, each of which has three drop precedence values. These precedence values define the order in which a packet is dropped (if needed) due to network congestion. For example, packets in AF13 class are dropped before packets in the AF12 class.

set ipsec

This command allows you to set IPSec policies and associations.

Command Syntax

set ipsec

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

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

Syntax Description

Parameters	Description
policy-name	An IPSec policy.
association-name	An IPSec association.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set logging

This command allows you to enable or disable logging.

Command Syntax

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

Syntax Description

Parameters	Description
enable	Turns on logging.
disable	Turns off logging.

Requirements

Command privilege level: 0

Allowed during upgrade: No

set network cluster publisher hostname

This command configures the cluster publisher hostname. Changing the hostname is possible only from the subscriber in a server group. This is supported when migrating from MCS to VMware platforms, but not in any other scenarios.

A temporary loss of network connectivity occurs while the network is being restarted with the new configuration.

Command Syntax

set network cluster publisher hostname *name*

Syntax Description

Parameters	Description
name	The hostname to be assigned.

set network cluster publisher ip

This command configures the cluster publisher IP address.

A temporary loss of network connectivity occurs while the network is being restarted with the new configuration.

Command Syntax

set network cluster publisher ***ip addr***

Syntax Description

Parameters	Description
ip addr	Specifies the ip address of the network cluster.

set network dhcp

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

Command Syntax

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

Syntax Description

Parameters	Description
eth0	Specifies Ethernet interface 0.
enable	This enables DHCP.
disable	This disables DHCP.
node_ip	The new static IP address for the server.
net_mask	The subnet mask for the server.
gateway_ip	The IP address of the default gateway.

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. We recommend that you restart all nodes whenever any IP address gets changed.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set network dns

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

Command Syntax

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

Syntax Description

Parameters	Description
ip-address	The IP address of the primary or secondary DNS server.

Usage Guidelines

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

Caution If you continue, this command causes a temporary loss of network connectivity. If you change the IP address of the DNS server, you must restart Cisco Tomcat. For more information, see utils service, on page 112.

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**]

Syntax Description

Parameters	Description
timeout	Sets the DNS request timeout.
seconds	The DNS timeout period, in seconds.
attempts	Sets the number of times to attempt a DNS request before quitting.
number	Specifies the number of attempts.
rotate	Causes the system to rotate among the configured DNS servers, distributing the load.

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*

Syntax Description

Parameters	Description
domain-name	The system domain that you want to assign.

Usage Guidelines

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

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

set network failover

This command enables and disables network fault tolerance.

Command Syntax

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

Syntax Description

Parameters	Description
enable	Enables network fault tolerance.
disable	Disables network fault tolerance.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set network gateway

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

Command Syntax

set network gateway *ip-address*

Syntax Description

Parameters	Description
ip-address	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 allows an administrator to set the network host name, change the IP address of the node, and restart the system.

Before attempting this command, the administrator should have a valid DRF backup.

Command Syntax

set network hostname *hostname*

Syntax Description

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

Command Mode

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Useage Guidelines

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

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

Example

```
admin:set network hostname
WARNING: Changing this setting will invalidate software license on this server. The license
 will have to be re-hosted.
Continue(y/n):
Continue (y/n)?y

ctrl-c: To quit the input.

*** W A R N I N G ***
Do not close this window without first canceling the command.

This command will automatically restart system services.
The command should not be issued during normal operating
hours.

=====================================================
Note: Please verify that the new hostname is a unique
name across the cluster and, if DNS services are
utilized, any DNS configuration is completed
before proceeding.
=====================================================

Security Warning : This operation will regenerate
all CUCM Certificates including any third party
signed Certificates that have been uploaded.

Enter the hostname:: app-lfwelty5
Would you like to change the network ip address at this time [yes]::


Warning: Do not close this window until command finishes.



ctrl-c: To quit the input.



*** W A R N I N G ***
=====================================================
Note: Please verify that the new ip address is unique
across the cluster.
=====================================================

Enter the ip address:: 106.1.34.154
Enter the ip subnet mask:: 255.0.0.0
Enter the ip address of the gateway:: 106.1.1.1
Hostname: app-lfwelty5
IP Address: 106.1.34.154
IP Subnet Mask: 255.0.0.0
Gateway: 106.1.1.1

Do you want to continue [yes/no]? yes
...
```

Note The administrator can change both the hostname and IP address by responding **yes**. To change just the hostname, respond **no**.

set network ip

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

Command Syntax

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

Syntax Description

Parameters	Description
eth0	Specifies Ethernet interface 0.
ip-address	The IP address that you want assign.
ip-mask	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 max_ip_contrack

This command sets the ip_conntrack_max value.

Command Syntax

set network max_ip_conntrack *ip_conntrack_max*

Syntax Description

Parameters	Description
ip_conntrack_max	Specifies the value for ip_conntrack_max.

set network mtu

This command sets the maximum MTU value.

Command Syntax

set network mtu *mtu_max*

Syntax Description

Parameters	Description
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 temporarily loses network connectivity.

Requirements

Level privilege: 1

Command privilege: 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 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**}}

Syntax Description

Parameters	Description
eth0	Specifies Ethernet interface 0.
auto	Specifies whether auto negotiation gets enabled or disabled.

Parameters	Description
speed	Specifies the speed of the Ethernet connection: 10 or 100 Mbps.
duplex	Specifies half-duplex or full-duplex.

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

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

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

set network ntp option

This command adds a noquery option to /etc/config file.

Command Syntax

set network ntp option noquery

set network pmtud

This command enables and disables path MTU discovery.

Command Syntax

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

Syntax Description

Parameters	Description
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 temporarily loses network connectivity.

Requirements

Level privilege: 1

Command privilege: 1

Allowed during upgrade: No

Example

This example runs the set network pmtud command.

```
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 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 use this command.

Command Syntax

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

Syntax Description

Parameters	Description
eth0	Specifies Ethernet interface 0.
ip-address	Specifies the IP address.
network-mask	Specifies the subnet mask.

Parameters	Description
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**}

Syntax Description

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

Usage Guidelines

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

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

set password

This command allows you to change the administrator password.

Command Syntax

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

Syntax Description

Parameters	Description
admin	Administrator.
security	Security.

Usage Guidelines

The system prompts you for the old and new passwords.

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.

To change a password:

1. Change the security password on the publisher server and then reboot the server.
2. Change the security password on all the subscriber servers to the same password that you created on the publisher server and restart the subscriber server to propagate the password change.

Note We recommend that you restart each server after the password is changed on that server.

Caution Failure to reboot the servers causes system service problems and problems with the Emergency Responder Administration on the subscriber servers.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set password age minimum

This command modifies the value of minimum password age for OS admin accounts in days.

Usage Guidelines

Acceptable values should be equal to or greater than 0 days but less or equal to 10 days.

Command Syntax

set password age minimum *days*

Syntax Description

Parameters	Description
days	The minimum password age in days.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

set password age maximum

This command modifies the value of maximum password age for Emergency Responder OS administration accounts in days.

Command Syntax

set password age maximum *days*

Usage Guidelines Acceptable values should be equal to or greater than 10 days but less than 3650 days (10 years).

Syntax Description

Parameters	Description
days	The maximum password age in days.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set password complexity character disable

This command disables password complexity. Changes take effect only at the next password change.

When disabled, the password created or changed after executing the command is no longer strong. The password does not need uppercase, lowercase, digit and special characters.

Command Syntax

set password complexity character disable

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

set password complexity character enable

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

When enabled, the passwords need to follow these guidelines:

- It must have at least one lowercase character.

- It must have at least one uppercase, one digit, and one special character.
- All of the adjacent characters on the keyboard are not accepted.
- Any of the previous ten passwords cannot be reused.
- The admin user password can only be changed once in 24 hours.
- A violation of any of the preceding rules results in a failure.

Command Syntax

set password complexity character enable

Requirements

Command privilege level: 1

Allowed during upgrade: No

set password complexity minimum-length

This command modifies the value of minimum password length for Unified CM OS accounts.

Command Syntax

set password complexity minimum-length *length*

Syntax Description

Parameters	Description
length	The minimum password length.

Useage Guidelines

Acceptable values should be equal to or greater than 6. Use this command only after enabling the character complexity of passwords.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set password expiry maximum-age

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

Command Syntax

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

Syntax Description

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

set password expiry minimum-age enable

This command enables minimum password expiry for OS accounts.

Usage Guidelines This command sets the value of minimum password age to 1 day (24 hrs) for OS administration accounts.

Command Syntax

set password expiry minimum-age enable.

set password expiry minimum-age disable

This command is used to disable minimum password aging for OS accounts.

This means passwords for OS admin accounts can be changed at any interval.

Command Syntax

set password expiry minimum-age disable

set password expiry user maximum-age disable

This command disables password expiry for a particular OS account.

Command Syntax

set password expiry user maximum-age disable *userid*

Syntax Description

Parameters	Description
userid	The name of account for which to disable maximum password age settings.

set password expiry user maximum-age enable

This command enables maximum password expiry for a particular OS account.

Command Syntax

set password expiry user maximum-age enable *userid*

Syntax Description

Parameters	Description
userid	The name of account for which to enable maximum password age settings.

set password expiry user minimum-age disable

This command disables minimum password age settings for a particular OS account.

Command Syntax

set password expiry user minimum-age disable *userid*

Syntax Description

Parameters	Description
userid	The account for which to disable minimum password age settings.

set password expiry minimum-age enable

This command enables minimum password age for a particular OS account.

Command Syntax

set password expiry user minimum-age enable *userid*

Syntax Description

Parameters	Description
userid	The account for which to enable minimum password age settings.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

set password history

This command sets the number of passwords to maintain in history.

Command Syntax

set password history *number*

Syntax Description

Parameters	Description
number	The number of passwords to maintain in history.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

set password inactivity disable

This command disables the password inactivity for the OS accounts.

Command Syntax

set password inactivity disable

set password inactivity enable

This command enables the password inactivity for the OS accounts with the default value set as 10 days.

Command Syntax

set password inactivity enable

set password inactivity period

This command sets the password inactivity for the OS accounts with the configured value.

Command Syntax

set password inactivity period *days*

Syntax Description

Parameters	Description
days	The number of days for which to set inactivity. Acceptable values are 1 to 99 days.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

set password user admin

This commands sets a new administration password.

Command Syntax

set password user admin

Example

This example runs the set password user admin command:

```
set password user admin
Please enter the old password :********
Please enter the new password:********
re-enter new password to confirm:********
```

Requirements

Command privilege level: 1

Allowed during upgrade: No

set password user security

This command sets a new platform security password.

Command Syntax

set password user security

Example

This example runs the set password user security command:

```
set password user security
Please enter the password:********
re-enter the password to confirm: ********
```

Requirements

Command privilege level: 1

Allowed during upgrade: No

set session maxlimit

This command sets the upper limit for concurrent sessions.

Command Syntax

set session maxlimit *[value]*

Syntax Description

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

Command Mode

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

set smtp

This command sets the SMTP server hostname.

Command Syntax

set smtp *hostname*

Syntax Description

Parameters	Description
hostname	The SMTP server name.

Requirements

Command privilege level: 0

Allowed during upgrade: No

set timezone

This command changes the system time zone.

Command Syntax

set timezone *timezone*

Usage Guidelines

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

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

Syntax Description

Parameters	Description
timezone	The new timezone.

Requirements

Command privilege level: 0

Allowed during upgrade: No

Example

This example sets the time zone to Pacific time:

```
set timezone Pac
```

set tls min-version

This command sets the minimum version of Transport Layer Security (TLS) protocol.

Note

- The system automatically restarts after you set the minimum TLS version.
- You need to configure the minimum TLS version for each node.

Command Syntax

set tls min-version *tls minVersion*

Syntax Description

Parameters	Description
tls minVersion	Type any one of the following options to set the minimum TLS version. • 1.0 • 1.1 • 1.2

Command Modes

Administrator (admin:)

Usage Guidelines

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Emergency Responder

Example

```
admin: set tls min-version 1.1
```

This command results in setting the minimum TLS version to 1.1 to all secured interfaces. If you have custom applications that make secure connection to the system, then make sure the applications support the TLS version that you have selected to configure. See *Cisco Unified Reporting Administration Guide* to make sure the endpoints in your deployment support this feature.

Warning This will set the minimum TLS to 1.1 and the server will reboot.

Do you want to continue (Yes or No)? Yes

The minimum TLS version is set to 1.1 successfully.

The system restarts in few minutes.

set tls resumption-timeout

This command sets the number of seconds after which the TLS resumption will not work and the sessions will be invalid.

Command Syntax

set tls resumption-timeout *set tls resumption-timeout*

Syntax Description

Parameters	Description
seconds	Enter a value up to 3600 seconds to configure. After the configured value, the TLS sessions are invalid.

Command Modes Administrator (admin:)

Usage Guidelines

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Emergency Responder

set tls trace

From the release 12.0 onwards, you can enable or disable the TLS tracing for services. Currently, Tomcat is the only supported device. You can use the CLI commands to view the reasons of connection failure of TLS connections to Cisco Emergency Responder.

set tls trace disable

This CLI command disables the TLS tracing for a service.

Note After you disable the TLS trace for a service, the service automatically gets restarted. During the restart process, any functionality related to the service will be not reachable.

Command Syntax

set tls trace disable *service*

Syntax Description

Parameters	Description
service	Specifies the service that you use to disable TLS tracing.

Command Modes Administrator (admin:)

Usage Guidelines

Requirements

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:set tls trace disable tomcat
```

Warning This disables the tls trace for Tomcat service and the Tomcat service is automatically restarted.

You must restart the Cisco Tomcat service for the changes to take effect. This will disconnect the active web sessions and all applications on this node will be unavailable until the service restarts. The service restart takes several minutes to complete.

Continue (Y/N)? Y

Successfully disabled tls trace for tomcat.

The Tomcat service will restart.

set tls trace enable

This CLI command enables the TLS tracing for a service.

Note After you enable the TLS trace for a service, the service automatically gets restarted. During the restart process, any functionality related to the service will be not reachable.

Command Syntax

set tls trace enable *service*

Syntax Description

Parameters	Description
service	Specifies the service that you use to enable TLS tracing.

Command Modes Administrator (admin:)

Usage Guidelines

Requirements

Command privilege level: 1

Allowed during upgrade: No

Example

```
admin:set tls trace enable tomcat
```

Warning This enables the tls trace for Tomcat service and the Tomcat service is automatically restarted.

You must restart the Cisco Tomcat service for the changes to take effect. This will disconnect the active web sessions and all applications on this node will be unavailable until the service restarts. The service restart takes several minutes to complete.

Continue (Y/N)? Y

Successfully enabled tls trace for tomcat.

The Tomcat service will restart.

set trace

This command sets trace activity for the specified task.

Command Syntax

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

Syntax Description

Parameters	Description
tname	The task for which you want to enable or disable traces.
enable Error	Sets task trace settings to the error level.
enable Special	Sets task trace settings to the special level.
enable State_Transition	Sets task trace settings to the state transition level.
enable Significant	Sets task trace settings to the significant level.
enable Entry_exit	Sets task trace settings to the entry_exit level.
enable Arbitrary	Sets task trace settings to the arbitrary level.
enable Detailed	Sets task trace settings to the detailed level.
disable	Disables the task trace settings.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set web-security

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

Command Syntax

set web-security *orgunit orgname locality state* [*country*] [*alternate-host-name*]

Usage Guidelines

When you set an *alternate-host-name* parameter with the **set web-security** command, self-signed certificates for Tomcat contains the Subject Alternate Name extension with the alternate host name specified. CSR for Emergency Responder contains Subject Alternate Name Extension with the alternate host name included in the CSR.

Syntax Description

Parameters	Description
orgunit	The organizational unit.
orgname	The organizational name.
locality	The organization location.
state	The organization state.
country represents	The organization country.
alternate-host-name	(Optional) Specifies an alternate name for the host when you generate a web-server (Tomcat) certificate.

Requirements

Command privilege level: 0

Allowed during upgrade: No

set webapp session timeout

This command sets a timeout period for the web application session of Cisco Emergency Responder and logs off the user on expiry.

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

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

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

Command Syntax

set webapp session timeout *minutes*

Syntax Description

Parameters	Description
minutes	Specifies the time, in minutes, that can elapse before a web application times out and logs off the user. • • Default value: 30 minutes

Command Mode

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

set workingdir

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

Command Syntax

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

Syntax Description

Parameters	Description
activelog	Sets the working directory for active logs.
inactivelog	Sets the working directory for inactive logs.
install	Sets the working directory for installation logs.
directory	The current working directory.

Requirements

Command privilege level: 0 for logs

Allowed during upgrade: Yes

Show Commands

show account

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

Command Syntax

show account

Requirements

Command privilege level: 4

Allowed during upgrade: Yes

show cert

This command displays certificate contents and certificate trust lists.

Command Syntax

Table 1: Available Commands

Command	Result
show cert list {**own** | **trust**}	This command displays certificate trust lists.
show cert own *filename*	This command displays certificate contents.
show cert trust *filename*	This command displays certificate contents.

Syntax Description

Parameters	Description
filename	The name of the certificate file.
own	Specifies owned certificates.
trust	Specifies trusted certificates.
list	Specifies a certificate trust list.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Example

This command displays own certificate trust lists:

```
show cert list own
```

show cli pagination

This command displays the status of the automatic CLI pagination.

Command Syntax

show cli pagination

Requirements

Level privilege: 0

Command privilege: 0

Allowed during upgrade: Yes

Example

The following example runs the show cli pagination command:

```
admin: show cli paginationAutomatic Pagination: Off.
```

show cli session timeout

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

Command Syntax

show cli session timeout

Command Mode

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show csr list

This command displays the selected CSR file.

Command Syntax

show csr list ***type***

Example

This example runs a show csr list command:

```
show csr list own

tomcat/tomcat.csr

Vipr-QuetzalCoatl/Vipr-QuetzalCoatl.csr
```

show ctl

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

Command Syntax

show ctl

show date

This command shows the system date.

Command Syntax

show date

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show diskusage

This command displays information about disk usage on the server.

Command Syntax

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

Syntax Description

Parameters	Description
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.

Parameters	Description
install	Displays disk usage information about the install directory.
tmp	Displays disk usage information about the tmp directory.
filename *filename*	(Optional)Saves the output to a file specified by a filename. These files are stored in the platform/cli directory. To view saved files, use the **file view activelog** command.
directory	(Optional)Displays only the directory sizes.
sort	(Optional)Sorts the output based on file size. File sizes are displayed in 1024-byte blocks.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show dscp all

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

Command Syntax

show dscp all

Command Mode

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: No

show dscp defaults

This command displays the default factory DSCP settings. These values take effect if the **set dscp defaults** command is executed.

Command Syntax

show dscp defaults

Command Mode

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: No

show dscp marking

This command displays the current DSCP traffic markings for a particular DSCP value.

Command Syntax

show dscp marking *value*

Syntax Description

Parameters	Description
value	DSCP value. You can enter the name of a well-known DSCP class, or a numeric value in decimal or hexadecimal format. Precede hexadecimal values with 0x or 0X.

Useage Guidelines

The valid class names as defined by DSCP are:

- Class Selector: values CSO, CS1, CS2, CS3, CS5, CS6 CS7 The class selector (CS) values correspond to IP Precedence values and are fully compatible with IP Precedence.
- Expedited Forwarding: value EF EF PHB is ideally suited for applications such as VoIP that require low bandwidth, guaranteed bandwidth, low delay, and low jitter.
- Best Effort: value BE Also called default PHB, this value essentially specifies that a packet be marked with 0x00, which gets the traditional best-effort service from the network router.
- Assured Forwarding: values AF11, AF12, AF13, AF21, AF22, AF23, AF41, AF42, AF43 There are four types of Assured Forwarding classes, each of which has three drop precedence values. These precedence values define the order in which a packet is dropped (if needed) due to network congestion. For example, packets in AF13 class are dropped before packets in the AF12 class.

Command Mode

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show dscp status

This command displays the current DSCP traffic markings.

Command Syntax

show dscp status {**enabled**|**disabled**}

Syntax Description

Parameters	Description
enabled	Filters the output to show only DSCP traffic markings that are enabled. If you do not specify a status, this filter is the default option.
disabled	Filters the output to show only DSCP traffic markings that are disabled.

Command Mode

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: No

show environment

This command displays information about the server hardware.

Command Syntax

show environment {**fans** |**power-supply** |**temperatures**}

Syntax Description

Parameters	Description
fans	Displays information gathered by fan probes.
power-supply	Displays information gathered by power supply probes.
temperatures	Displays information gathered by temperature probes.

show hardware

This command displays the following information about the platform hardware.

Command Syntax

show hardware

Usage Guidelines

This command displays the following information about the platform hardware:

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

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show ipsec

This command displays information about IPsec policies and associations.

Command Syntax

Table 2: Available Commands

Command	Result
show ipsec information *policy_group| policy_name*	This command displays detailed information about the specified ipsec policy.
show ipsec policy_group	This command displays all the ipsec policy group on the node.
show ipsec policy_name*policy_group*	This command displays the list of ipsec policy names that exist in the specified policy group.
show ipsec status	

Syntax Description

Parameters	Description
information	Displays the association details and status for the policy.
status	Displays the status of all IPsec tunnels that are defined in the system.
policy_group	The name of a specific IPsec policy.

Requirements

Command privilege level: 1

Allowed during upgrade: yes

Example

This example displays IPsec policies:

```
show ipsec policy
```

show logins

This command displays recent logins to the server.

Command Syntax

show logins *number*

Syntax Description

Parameters	Description
number	The number of most recent logins to display. The default is 20.

show memory

This command displays information about the server memory.

Command Syntax

show memory{**count**| **module**[**ALL** | *module_number*]| **size**}

Syntax Description

Parameters	Description
ALL	Displays information about all installed memory modules.
module_number	Specifies the memory module to display.
count	(Optional)Displays the number of memory modules on the system.
module	(Optional)Displays detailed information about each memory module.
size	(Optional)Displays the total amount of memory.

show myself

This command displays information about the current account.

Command Syntax

show myself

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show network

This command displays network information.

Command Syntax

Table 3: Available Commands

Command	Result
show networkall [**detail**]	This command shows network information for listening and non-listening sockets.
show networketh0 [**detail**]	This command shows network information for ethernet 0.
show networkfailover [**detail**] [**page**]	This command shows Network Fault Tolerance information.
show networkroute [**detail**]	This command shows network routing information.
show network status [**detail**] [**listen**] [**process**] [**all**] [**nodns**] [**search stext**]	This command shows active internet connections.
show network ip_conntrack	This command shows ip_conntrack usage information.
show network max_ip_conntrack	This command shows max_ip_conntrack information.
show network dhcp eth0 status	This command shows DHCP status information.
show network cluster	This command lists nodes in the network cluster.
show network ipprefs{**all** |**enabled**| **public**	This command shows the list of ports that have been requested to be opened or translated in the firewall.
show network ntp	
show network failover[**detail**][**page**]	This command shows Network Fault Tolerance information.

Command	Result
show network ipv6{**route**| **settngs**}	This command shows IPv6 network routes and network settings.

Syntax Description

Parameters	Description
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	(Optional)Displays additional information.
detail	(Optional)Displays more detailed additional information.
page	(Optional)Displays information one page at a time.
listen	(Optional)Displays only listening sockets.
process	(Optional)Displays the process ID and name of the program to which each socket belongs.
all	(Optional)Displays both listening and nonlistening sockets.
nodns	(Optional)Displays numerical addresses without any DNS information.
search stext	(Optional)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 cluster

This command lists nodes in the network cluster.

Command Syntax

show network cluster

Command Mode

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

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}

Syntax Description

Parameters	Description
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

Level privilege: 0

Command privilege: 0

Allowed during upgrade: Yes

Example

The following example shows show the network ipprefs command:

```
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:
```

set network ntp option

This command adds a noquery option to /etc/config file.

Command Syntax

set network ntp option noquery

show open

This command displays open files and ports on the system.

Syntax Description

Table 4: Available Commands

Command	Result
show open files [**all**] [**process** *processID*] [**regexp** *reg_exp*]	This command shows open files on the system.
show open ports [**all**] [**regexp** *reg_exp*]	This command shows all open ports on the system.

Syntax Description

Parameters	Description
files	displays open files on the system.
ports	displays open ports on the system.
all	(Optional)Displays all open files or ports.
process	(Optional)Displays open files that belong to the specified process.
processID	(Optional)Specifies a process.
regexp	(Optional)Displays open files or ports that match the specified regular expression.

Parameters	Description
reg_exp	(Optional)A regular expression.

show packages

This command displays the name and version for installed packages.

Command Syntax

show packages {**active**| **inactive**} *name* [**page**]

Syntax Description

Parameters	Description
active	Specifies active packages.
inactive	Specifies inactive packages.
name	The package name. To display all active or inactive packages, use the wildcard character (*).
page	(Optional)Displays the output one page at a time.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show password expiry maximum-age

This command displays the configured password expiration parameters.

Command Syntax

show password expiry maximum-age

show password expiry minimum-age

This command displays the configured password expiration parameters.

Command Syntax

show password expiry minimum-age

show password expiry user maximum-age

This command displays the configured password expiration parameters for a particular OS user.

Command Syntax

show password expiry user maximum-age userid

show password expiry user minimum-age

This command displays the configured password expiration parameters for a particular OS user.

Command Syntax

show password expiry user minimum-age userid

show password history

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

Password inactivity is the number of days of inactivity after a password has expired before the account is disabled.

Command Syntax

show password inactivity

Example

```
show password inactivity
Password Inactivity: Enabled and is currently set to 10
    days
```

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show process

This command displays information about processes running on the system.

Syntax

Command	Result
show processlist [**file** filename] [**detail**]	This command displays a list of all the processes and critical information about each process and visually indicates the child-parent relationships between the processes.
show processload [**cont**] [**clear**] [**noidle**] [**num** *number*] [**thread**] [**cpu** | **memory**| **time**] [**page**]	This command displays the current load on the system.
show process name *process* [**file** *filename*]	This command displays the details of processes that share the same name and indicates their parent-child relationship.
show process open-fd *process-id* [**,** *process-id2*]	This command lists the open file descriptors for a comma-separated list of process IDs.
show process search *regexp* [**file** *filename*]	This command searches for the pattern that the regular expression regexp specifies in the output of the operating system-specific process listing.
show process using-most cpu [*number*] [**file** *filename*]	This command displays a list of the most CPU-intensive processes.
show process using-most memory [*number*] [**file** *filename*]	This command displays a list of the most memory-intensive processes.
show process pid *pid*[**file** *filename*]	This command displays a list of PIDs.
show process user *username* [**file** *filename*]	This command retrieves details of processes that share the user name and displays parent-child relationship.
show process using most	This command lists the most intensive processes.

Syntax Description

Parameters	Description
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.

Parameters	Description
open-fd	lists the open file descriptors for a comma-separated list of process IDs.
search	searches for the pattern specified by the regular expression regexp in the output of the operating system-specific process listing.
using-most cpu	displays a list of the most CPU-intensive processes.
using-most memory	displays a list of the most memory-intensive processes.
file*filename*	(Optional)Outputs the results to the file specified by the filename.
detail	(Optional)Displays the detailed output.
cont	(Optional)Repeats the command continuously.
clear	(Optional)Clears the screen before displaying output.
noidle	(Optional)Ignores the idle/zombie processes.
num number	(Optional)Displays the number of processes specified by number. The default number of processes is 10. Set number to **all** to display all processes.
thread	(Optional)Displays threads.
[**cpu** | **memory** | **time**]	(Optional)Sorts output by CPU usage, memory usage, or time usage. The default is to sort by CPU usage.
page	(Optional)Displays the output in pages.
process	(Optional)Specifies the name of a process.
process-id	(Optional)Specifies the process ID number of a process.
regexp	(Optional)A regular expression.
number	(Optional)The number of processes to display. The default is 5.
pid	Specifies the process ID number of a process.
username	Specifies the username.

show session maxlimit

This command shows the upper limit for concurrent SSH sessions.

Command Syntax

show session maxlimit

Command Mode

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show smtp

This command displays the name of the SMTP host.

Command Syntax

show snmp

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show stats io

This command displays system I/O statistics.

Command Syntax

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

Syntax Description

Parameters	Description
kilo	Displays statistics in kilobytes.
detail	Displays detailed statistics on every available device on the system and overrides the kilo option.
page	Displays one page at a time.
file *filename*	Outputs the information to a file.

Useage Guidelines

The file option saves the information to

`platform/cli/filename.txt.`

The filename cannot contain the "." character.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show status

This command displays basic platform status.

Command Syntax

show status

Usage Guidelines

This command displays the following basic platform status:

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

Requirements

Command privilege level: 0

show tech all

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

Command Syntax

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

Syntax Description

Parameters	Description
page	Displays one page at a time.
file*filename*	Outputs the information to a file.

Useage Guidelines

The file option saves the information to

`platform/cli/filename.txt.`

The file name cannot contain the "." character.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show tech database

This command creates a CSV file of the entire database.

Command Syntax

show tech database {**dump**| **sessions**}

Syntax Description

Parameters	Description
dump	Creates a CSV file of the entire database.
sessions	Redirects the session and SQL information of the present session IDs to a file.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show tech database dump

This command creates a CSV file of the entire database.

Command Syntax

show tech database dump

show tech dbintegrity

This command displays the database integrity.

Command Syntax

show tech dbintegrity

show tech dbinuse

This command displays the database in use.

Command Syntax

show tech dbinuse

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show tech dbschema

This command displays the database schema in a CSV file.

Command Syntax

show tech dbschema

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show tech dbstateinfo

This command displays the state of the database.

Command Syntax

show tech dbstateinfo

show tech network

This command displays network aspects of the server.

Command Syntax

Command	Result
show tech network	
show tech network [**page**] [**file** *filename*]	This command displays network tech information for a page.
show tech network all [**page**] [**search** *text*] [**file** *filename*]	This command displays all network tech information.

Command	Result
show tech network hosts [**page**] [**search** *text*] [**file** *filename*]	This command displays information about hosts configuration.
show tech network interfaces [**page**] [**search** text] [**file** *filename*]	This command displays information about the network interfaces.
show tech network resolv [**page**] [**search** *text*] [**file** *filename*]	This command displays information about hostname resolution.
show tech network routes [**page**] [**search** *text*] [**file** *filename*]	This command displays information about network routes.
show tech network sockets {**numeric**}	This command displays the list of open sockets.

Syntax Description

Parameters	Description
all	displays all network technical 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.
page	(Optional)Displays one page at a time.
search *text*	(Optional)Searches the output for the string specified by text. The search is not case sensitive.
file *filename*	(Optional)Outputs the information to a file.
numeric	(Optional)Displays the numerical addresses of the ports instead of determining symbolic hosts. It is equivalent to running the Linux **netstat [-n]** shell command.

Usage Guidelines

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

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show tech prefs

This command displays all preferences files for Emergency Responder and its database.

Usage Guidelines This information is written to a file, which can be viewed subsequently using the **file view** CLI.

Command Syntax

show tech prefs

show tech runtime

This command displays server runtime.

Command Syntax

show tech runtime {**all** | **cpu**| **disk**| **env**| **memory**} [**page**] [**file** *filename*]

Syntax Description

Parameters	Description
all	Displays all runtime information.
cpu	Displays CPU usage information at the time the command is run.
disk	Displays system disk usage information.
env	Displays environment variables.
memory	Displays memory usage information.
page	Displays one page at a time.
file *filename*	Outputs the information to a file.

Usage Guidelines The **file** option saves the information to

`platform/cli/filename.txt.`

The file name cannot contain the "." character.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show tech systables

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

Command Syntax

show tech systables

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show tech system

This command displays the system aspects of the server.

Command Syntax

show tech system {**all**| **bus**| **hardware**| **host**| **kernel**| **software**| **tools**} [**page**] [**file** *filename*]

Syntax Description

Parameters	Description
all	Displays all of 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	Lists the installed kernel modules.
software	Displays information about the installed software versions.
tools	Displays information about the software tools on the server.
page	Displays one page at a time.
file *filename*	Outputs the information to a file.

Usage Guidelines

The **file** option saves the information to

`platform/cli/filename.txt`

. The file name cannot contain the "." character.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show tech table

This command displays the contents of the specified database table.

Command Syntax

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

Syntax Description

Parameters	Description
table_name	The name of the table to display.
page	Displays the output one page at a time.
csv	Sends the output to a comma separated values file.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show tech version

This command displays the version of the installed components.

Command Syntax

show tech version [**page**]

Syntax Description

Parameters	Description
page	Displays the output one page at a time.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show timezone

This command displays time zone information.

Command Syntax

show timezone{**config**| **list** [**page**] }

Syntax Description

Parameters	Description
config	Displays the current time zone settings.
list	Displays the available time zones.
page	Displays the output one page at a time.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show tls trace

This command shows the status of TLS trace for a service.

Command Syntax

show tls trace *service*

Syntax Description

Parameters	Description
service	Represents the TLS tracing status of a service. It is a mandatory parameter.

Command Modes Administrator (admin:)

Usage Guidelines

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Emergency Responder

show tls min-version

This command shows the minimum configured version of Transport Layer Security (TLS) protocol.

Command Syntax

show tls min-version

Command Modes Administrator (admin:)

Usage Guidelines

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Emergency Responder

Example

```
admin:show tls min-version
```

The configured TLS minimum version is 1.0.

show tls resumption-timeout

This command shows the TLS session resumption timeout.

Command Syntax

show tls resumption-timeout

Command Modes

Administrator (admin:)

Usage Guidelines

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Emergency Responder

show trace

This command displays trace information for a particular task.

Command Syntax

show trace [*task_name*]

Syntax Description

Parameters	Description
task_name	The name of the task for which you want to display the trace information.

Useage Guidelines

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

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Example

This example displays trace information for CDP.

```
show trace cdps
```

show ups status

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

Command Syntax

show ups status

Usage Guidelines

This command only can provide a complete status on 7835-H2 and 7825-H2 servers.

show version

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

Command Syntax

show version {**active**| **inactive**}

Syntax Description

Parameters	Description
active	Displays the version running on the active partition.
inactive	Displays the version on the inactive partition.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show webapp session timeout

This command displays the webapp session timeout value, which is the amount of time, in minutes, that can elapse before a web application times out and logs off the user.

Command Syntax

show webapp session timeout

Command Mode

Administrator (admin:)

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

Command Mode

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Unset Commands

unset ipsec

This command allows you to disable IPsec policies and associations.

Command Syntax

Command	Result
unset ipsec policy {**ALL** | *policy-name*}	

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

Syntax Description

Parameters	Description
policy-name	The name of an IPsec policy.
association-name	The name of an IPsec association.

Requirements

Command privilege level: 1

Allowed during upgrade: No

unset network

This command unsets DNS options.

Command Syntax

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

Syntax Description

Parameters	Description
timeout	Sets the wait time before the system considers a DNS query failed to the default.
attempts	Sets the number of DNS attempts to make before failing to the default.
rotate	Sets the method for selecting a name server to the default. This affects how loads are distributed across name servers.

Usage Guidelines

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

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

unset network domain

This command unsets the domain name and restarts the server.

Command Syntax

unset network domain

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Utils Commands

utils auditd

This command starts, stops, and provides the status of the system auditing service.

Command Syntax

utils auditd {**enable**|**disable**|**status**}

Syntax Description

Parameters	Description
enable	Enables the collection of audit logs. When enabled, the system monitors and records user actions as well as Linux events such as the creation and removal of users, as well as the editing and deleting of files.
disable	Disables the collection of audit logs.
status	Displays the status of audit log collection. Cisco recommends that you retrieve the audit log by using the Real-Time Monitoring Tool, but you can also retrieve it by using the CLI.

Command Mode

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Useage Guidelines

After the service has been enabled, it monitors and logs activity on the system. Be aware that the system auditing service logs a lot of information. Care must be taken not to overfill the disk.

utils core list

This command lists all existing core files.

Command Syntax

utils core{**active**| **inactive**} **list**

utils core analyze

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

Command Syntax

utils core analyze *core file name*

Syntax Description

Parameters	Description
core file name	Specifies the name of a core file.

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

utils create report

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

Command Syntax

utils create report {**hardware**| **platform**| **csa**}

Syntax Description

Parameters	Description
hardware	Creates a system report containing disk array, remote console, diagnostic, and environmental data.
platform	Collects all of the platform configuration files into a TAR file.
csa	Collects all the files required for CSA diagnostics and assembles them into 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, to get the report use the command **file get activelog platform/log/***filename*, where *filename* is the report filename that is displayed after the command completes.

Requirements

Level privilege: 1

Command privilege level: 0

Allowed during upgrade: Yes

utils create report database

Collects all log files needed for database troubleshooting.

Command Syntax

Utils create report database.

Example

```
admin:utils create report database
Created /var/log/active/cm/log/informix/[hostname]_db_report_Oct_27_11_13_10 for log
collection...
Collecting database logs, please be patient...
Collecting message logs (ccm.log) and assert failure files (af files)...
Collecting ris and ats files...
Collecting DB Replication logs...
Collecting DB install logs...
Collecting dblrpc and dbmon logs...
Collecting CDR information...
COMPLETED! Database report created successfully...
To retrieve the [hostname]_db_report_Oct_27_11_13_10.tar, use CLI command:
  file get activelog cm/log/informix/[hostname]_db_report_Oct_27_11_13_10.tar
To delete the [hostname]_db_report_Oct_27_11_13_10.tar, use CLI command:
  file delete activelog cm/log/informix/[hostname]_db_report_Oct_27_11_13_10.tar
```

utils configapisecurehttp

This command enables secure http for UCAT service(ConfigAPI).

Command Syntax

Command	Result
utils configapisecurehttp enable	This command when enabled, UCAT(ConfigAPI) connections are allowed only over secure http.
utils configapisecurehttp disable	This command when disabled, non-secure http UCAT(ConfigAPI) connections are allowed.
utils configapisecurehttp status	Displays the enabled or disabled status of the command.

Usage Guidelines We recommend that you enable the `configapisecurehttp` when the FIPS mode or Enhanced Security Mode is enabled on the Cisco Emergency Responder server.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

utils dbreplication dropadmindb

This command drops the Informix syscdr database on any server in the cluster.

Command Syntax

utils dbreplication dropadmindb

Usage Guidelines You should run this command only if database replication reset or cluster reset fails and replication cannot be restarted.

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: No

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

utils dbreplication status

This command displays the status of database replication. Use this command only on the first publisher server of a cluster.

Command Syntax

utils dbreplication status

utils dbreplication stop

This command stops the automatic setup of database replication. Run this command on subscriber and publisher servers before executing the CLI command **utils dbreplication reset** or **utils dbreblication clusterreset**. You can run this command on the subscriber servers simultaneously, before you run it on the publisher server.

Command Syntax

utils dbreplication stop {*nodename*| **all**}

Syntax Description

Parameters	Description
nodename	Specifies the name of the node on which to stop the automatic setup of database replication.
all	Stops database replication on all nodes.

Command Mode

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: No

utils dbreplication repair

This command repairs database replication.

Command Syntax

utils dbreplication repair

utils dbreplication reset

This command resets and restarts database replication.

Command Syntax

utils dbreplication reset

Usage Guidelines

You must restart the Emergency Responder Subscriber node from CUOS Administration or using the CLI command **utils system restart** after executing **utils dbreplication reset** command. See **help utils dbreplication reset** CLI command for more details.

utils diagnose

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

Command Syntax

utils diagnose {**fix**| **list**| **module**| **test**| **version**} *[module_name]*

Syntax Description

Parameters	Description
fix	Runs all diagnostic commands and attempts to fix problems.
list	Lists all available diagnostic commands.
module	Runs a single diagnostic command or group of commands and attempts to fix problems.
test	Runs all diagnostic commands but does not attempt to fix problems.
version	Displays the diagnostic framework version.
module_name	The name of a diagnostics module.

utils diagnose test

This command enables you to run all diagnostic commands but does not attempt to fix any problems.

Command Syntax

utils diagnose test

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*]

Syntax Description

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

Usage Guidelines

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

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

utils disaster_recovery cancel_backup

This command cancels the ongoing backup job.

Command Syntax

utils disaster_recovery cancel_backup

Usage Guidelines

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

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

utils disaster_recovery device add network

This command adds the backup network device.

Command Syntax

utils disaster_recovery device add network *device_name path server_name/ip_address username* [*Number_of_backups*]

Syntax Description

Parameters	Description
device_name	The name of the backup device to be added.
path	The path to retrieve backup device from this location.
server_name/ip_address	The hostname or IP address of the server where the backup file needs to be stored.
username	the user ID to connect to remote machine
Number_of_backups	(Optional)The number of backups to store on Network Directory(default 2).

Example

Use the following example when running the utils disaster_recovery device add network command:

```
utils disaster_recovery device add network
networkDevice /root 10.77.31.116 root 3
```

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils disaster_recovery device delete

This command deletes the device.

Command Syntax

utils disaster_recovery device delete *device_name*|*

Syntax Description

Parameters	Description
device_name	The name of the device to be deleted.
*	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 shows the device name, device type, and device path for all the backup devices.

Command Syntax

utils disaster_recovery device list

Example

The following example shows how to run this command:

```
utils disaster_recovery device list
sftpdevice                NETWORK              10.77.31.116 : /root
tapedevice                TAPE                 /dev/nst0
localdevice               LOCAL                /common/drfbackup
```

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

utils disaster_recovery estimate_tar_size

estimate_tar_size help:

This command provides the estimated size of last successful backup from SFTP/Local device.

Syntax Description

Parameters	Description
Name of the tar	This will give the tar file name through which the size can be estimated.

Example

```
admin:utils disaster_recovery estimate_tar_size CER
Estimated tar size successfully: Estimated size of backup for selected feature(s) is 42.52
 MB.
```

utils disaster_recovery history

This command shows the history of a previous backup or restore

Command Syntax

utils disaster_recovery history *operation*

Syntax Description

Parameters	Description
operation	The name of an operation such as backup or restore.

Example

The following example shows how to run this command:

```
utils disaster_recovery history backup
Tar Filename: Backup Device: Completed On: Result: Backup Type: Features Backed Up:
2009-10-30-14-53-32.tar TAPE  Fri Oct 30 14:55:31 CDT 2009   ERROR    MANUAL
2009-12-10-10-30-17.tar TAPE  Thu Dec 10 10:35:22 CST 2009   SUCCESS  MANUAL
CDR_CAR,CCM
```

utils disaster_recovery jschLogs

This command enables and disables detailed JSch logging.

Example

```
drfCliCommand: JSch detailed logging enabled.
Restart DRS Master and Local Agent in this machine for the changes to take effect.
```

```
drfCliCommand: JSch detailed logging disabled.
Restart DRS Master and Local Agent in this machine for the changes to take effect.
JSch logs deleted successfully.
```

utils disaster_recovery schedule add

This command adds the configured schedules.

Command Syntax

utils disaster_recovery schedule add *schedulename devicename featurelist datetime frequency*

Syntax Description

Parameters	Description
schedulename	The name of the scheduler.
devicename	The name of the device for which scheduling is done.
featurelist	The comma-separated feature list to back up.
datetime	The date when the scheduler is set. The format is (yyyy/mm/dd-hh:mm) 24-hr clock.
frequency	The frequency at which the scheduler is set to receive a backup. For example: ONCE, DAILY, WEEKLY and MONTHLY .

Example

The following example show how to run this command:

```
utils disaster_recovery schedule add schedulename devicename featurelist
datetime frequency
Schedule has been saved successfully.
```

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

utils disaster_recovery schedule delete

This command deletes the specified schedule.

Command Syntax

utils disaster_recovery schedule delete *schedulename*|*

Syntax Description

Parameters	Description
schedulename	The name of the schedule that needs to be deleted.
*	Deletes all of the existing schedules.

Example

The following example shows how this command is run:

```
utils disaster_recovery schedule delete schedule1|
Schedules deleted successfully.
```

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils disaster_recovery schedule disable

This command disables the specified schedule.

Command Syntax

utils disaster_recovery schedule disable *schedulename*

Syntax Description

Parameters	Description
schedulename	The name of the schedule that needs to be disabled.

Example

The following example shows how to run this command:

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils disaster_recovery schedule enable

This command enables the specified schedule.

Command Syntax

utils disaster_recovery schedule enable *schedulename*

Syntax Description

Parameters	Description
schedulename	The name of the schedule that needs to be enabled.

Example

The following example shows how to run this command:

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils disaster_recovery schedule list

This command displays all the of configured schedules.

Command Syntax

utils disaster_recovery schedule list

Requirements

Command privilege level: 1

Allowed during upgrade: No

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*

Syntax Description

Parameters	Description
restore_server	Specifies the hostname of the server that you want to restore.
tarfilename	Specifies the name of the file to restore.

Parameters	Description
path	Represents the location of the backup files on the remote server.
servername	Represents the IP address or host name of the server where you stored the backup files.
username	Represents the username that is needed to log in to the remote server.

Usage Guidelines

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

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

utils disaster_recovery show_backupfiles tape

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

Command Syntax

utils disaster_recovery show_backupfiles tape *tapeid*

Syntax Description

Parameters	Description
tapeid	Represents the ID of an available tape device.

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils disaster_recovery show_backupfiles network

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

Command Syntax

utils disaster_recovery show_backupfiles network *path servername username*

Syntax Description

Parameters	Description
path	Represents the location of the backup files on the remote server.
servername	The IP address or host name of the server where you stored the backup files.
username	The username that is needed to log in to the remote server.

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils disaster_recovery show_registration

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

Command Syntax

utils disaster_recovery show_registration *hostname*

Syntax Description

Parameters	Description
hostname	The server that you want to display registration information.

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*

Syntax Description

Parameters	Description
operation	The name of the ongoing operation: backup or restore.

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils EnhancedSecurityMode

This command allows you to change and check Enhanced Security Mode status on a particular node.

Command Syntax

Command	Result
utils EnhancedSecurityMode	This command allows you to change and check Enhanced Security Mode status on a particular node. When the system is enabled for Enhanced Security Mode, the system implements a set of strict security and risk management controls that allow your system to comply with Enhanced Security Mode guidelines.
utils EnhancedSecurityMode disable	Run this command to disable a cluster node for Enhanced Security Mode.
utils EnhancedSecurityMode enable	Run this command to enable a cluster node for Enhanced Security Mode.
utils EnhancedSecurityMode status	Run this command to verify if Enhanced Security Mode is enabled.

Syntax Description

Parameters	Description
disable	Deactivates Enhanced Security Mode and prompts disabling of FIPS mode.
enable	Activates Enhanced Security Mode and prompts for enabling FIPS mode. If FIPS is enabled, then Enhanced Security Mode will be activated.
status	Displays the status of Enhanced Security Mode.

Usage Guidelines

FIPS mode must be enabled before you enable Enhanced Security Mode. If you haven't already enabled FIPS, you will be prompted to enable it when you attempt to enable Enhanced Security Mode.

Confirm that your phones support SHA-512. Enhanced Security Mode compliance requires this level of encryption for digital signatures. Legacy phones that do not support SHA-512 encryption will not work after you configure the system to use SHA-512.

Do not run this command on all nodes simultaneously.

Requirements

Command privilege level: 0

Allowed during upgrade: No

utils fior

This command allows you to monitor the I/O on the server.

Usage Guidelines The file I/O reporting service provides a kernel-based daemon for collecting file I/O per process.

Command Syntax

Command	Result
utils fior	This command allows you to monitor the I/O on the server. The File I/O Reporting service provides a kernel-base daemon for collecting file I/O per process.
utils fior disable	
utils fior enable	
utils fior list [**start**=*date-time*] [**stop**=*date-time*]	This command displays a list of the I/O events for all processes.
utils fiorstart	
utils fior status	
utils fior stop	
utils fior top *number* [**read** | **write** | **read-rate** | **write-rate]** [**start**=*date-time*] [**stop**=*date-time*]	This command displays a list of I/O statistics for I/O bound processes at the time that you run this command.

Syntax Description

Parameters	Description
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.

Parameters	Description
start	Starts a previously stopped file I/O reporting service. The service remains in a started state until it is manually stopped or the machine is rebooted.
status	Displays the status of the file I/O reporting service.
stop	Stops the file I/O reporting service. The service remains in a stopped state until it is manually started or the machine is rebooted.
top	Displays a list of top processes that create file I/O. This list can be sorted by the total number of bytes read, the total number of bytes written, the rate of bytes read, or the rate of bytes written.
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 used to sort the list of the top processes.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

utils fips

Caution FIPS mode is only supported on releases that have been through FIPS compliance. Be warned that FIPS mode should be disabled before you upgrade to a non-FIPS compliance version of Cisco Emergency Responder.

For information about which releases are FIPS compliant and to view their certifications, see the *FIPS 140* document at http://www.cisco.com/web/strategy/government/security_certification/net_business_benefit_seccert_fips140.html.

This command enables, disables, or displays the status of FIPS 140-2 mode. FIPS 140-2 mode is disabled by default; only an administrator can enable FIPS.

Command Syntax

utils fips {**enable**|**disable**|**status**}

Syntax Description

Parameters	Description
enable	Activates FIPS 140-2 mode.
disable	Deactivates FIPS 140-2 mode.
status	Displays the status of FIPS 140-2 mode.

Command Modes

Administrator (admin:)

Usage Guidelines

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

Consider the following information before you enable FIPS 140-2 mode:

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

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

Consider the following information before you disable FIPS 140-2 mode: In multiple server groups, each server must be disabled separately; FIPS mode is not disabled group-wise but on a per server basis.

Requirements

Command privilege level: 0

Allowed during upgrade: No

utils firewall

This command manages the firewall on the node.

Command Syntax

Command	Result
utils firewall {**enable** |**disable***[time]*}	This commands enables and disables firewall.
utils firewall list	This commands displays the current configuration of the firewall.
utils firewall status	This command displays the current status of the IPv4 firewall.

Syntax Description

Parameters	Description
disable	Disables the firewall.
time	The duration for which the firewall is disabled, in one of these formats: • [0–1440]**m** to specify a duration in minutes. • [0–24]**h** to specify a duration in hours. • [0–23]**h**[0–60]**m** to specify a duration in hours and minutes. • If you do not specify a time, the default is 5 minutes.
list	The current firewall configuration.
status	The status of the firewall.

Usage Guidelines

When the firewall is disabled, you must enter the URL of the Cisco Unified Communications Manager server in the following format to log into the web interface:

https://*server***:8443/**

where *server* is the server name or IP address of the server.

Disabling the firewall is not recommended.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils firewall ipv4

This command enables and disables IPv4 firewall.

Command Syntax

utils firewall ipv4 {**enable**|**disable**|*[time]*}

Syntax Description

Parameters	Description
enable	Turns on the IPv4 firewall.
disable	Turns off the IPv4 firewall. If you do not enter the time parameter, this command disables the firewall for 5 minutes.

Parameters	Description
[time]	(Optional) Sets the duration for which the firewall is to be disabled in the following formats: • Minutes: 0–1440m • Hours: 0–23h • Hours and minutes: 0–23h 0–60m

Command Mode

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils firewall ipv4 debug

This command turns IPv4 firewall debugging on or off. If you do not enter a time parameter, this command turns on debugging for 5 minutes.

Command Syntax

utils firewall ipv4 debug {**off**| *[time]*}

Syntax Description

Parameters	Description
off	Enables the collection of audit logs. When enabled, the system monitors and records user actions as well as Linux events such as the creation and removal of users, as well as the editing and deleting of files.
[time]	(Optional) Disables the collection of audit logs.

Command Mode

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils firewall ipv4 list

This command displays the current configuration of the IPv4 firewall.

Command Syntax

utils firewall ipv4 list

Command Mode

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils firewall ipv4 status

This command displays the current status of the IPv4 firewall.

Command Syntax

utils firewall ipv4 status

Command Mode

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils filebeat

This command uses the filebeat client to upload logs from the Cisco Emergency Responder server to the external logstash server.

Command Syntax

utils filebeat {**config** |**enable**|**disable**|**status**}

Syntax Description

Parameters	Description
config	Allows you to enter the logstash server details. You can enable the filebeat service if the logstash server is reachable by choosing one of the following log types: • Platform audit logs(/var/log/active/audit/vos/vos-audit.log) • Remote Support logs(/var/log/active/audit/vos/remote_activity.log_*)
enable	Enables the filebeat service, and the selected logs are uploaded to an external logstash server if service is active else, you can also restart the service.
disable	Disables the filebeat service.
status	Displays the active status of the filebeat service.

Command Mode

Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: Yes

Usage Guidelines After the service has been enabled, the selected logs will be uploaded to the external logstash server.

Warning Warning: There may loss of data when the service is restarted.

utils import config

This command imports all configuration settings found on the platformConfig.xml file and then reboots the system.

Command Syntax

utils import config

utils iostat

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

Command Syntax

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

Syntax Description

Parameters	Description
interval	The value in seconds between two iostat readings (mandatory if you specify the number of iterations).
interations	The number of iostat iterations to be performed (mandatory if you specify an interval).
filename	Redirects the output to a file.

Requirements

Level privilege: 0

Command privilege: 1

Allowed during upgrade: No

utils iothrottle enable

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

Command Syntax

utils iothrottle enable

utils iothrottle disable

This command disables I/O throttling enhancements.

Usage Guidelines This could adversely affect the system during upgrades.

Command Syntax

utils iothrottle disable

utils iothrottle status

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

Command Syntax

utils iothrottle status

utils network arp

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

Command Syntax

Command	Result
utils network arplist [**host** *host*] [**page**] [**numeric**]	This command lists the contents of the Address Resolution Protocol table.
utils network arpset {*host*} {*address*}	This command sets an entry in the Address Resolution Protocol table.
utils network arpdelete *host*	This command deletes an entry in the Address Resolution Protocol table.

Syntax Description

Parameters	Description
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.
page	Displays the output one page at a time.
numeric	Displays hosts as dotted IP addresses.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils network capture eth0

This command captures IP packets on the specified Ethernet interface.

Command Syntax

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

Syntax Description

Parameters	Description
eth0	Specifies Ethernet interface 0.
page	(Optional)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	(Optional)Displays hosts as dotted IP addresses.
file fname	(Optional)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	(Optional)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	(Optional)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	(Optional)Specifies the source address of the packet as a host name or IPV4 address.
dest addr	(Optional)Specifies the destination address of the packet as a host name or IPV4 address.
port num	(Optional)Specifies the port number of the packet, either source or destination.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils network connectivity

This command verifies the server's network connection to the publisher server. It is only valid on a subscriber server.

Command Syntax

utils network connectivity

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils network connectivity output

This command verifies the node network connection to the first node in the cluster. It is for Cisco Emergency Responder Subscriber only.

Command Syntax

utils network connectivity output

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**]

Syntax Description

Parameters	Description
hostname	The host name or IP address that you want to resolve.
server-name	(Optional)Specifies an alternate domain name server.
page	(Optional)Displays the output one screen at a time.
detail	(Optional)Displays a detailed listing.
srv	(Optional)Displays DNS SRV records.

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*]

Syntax Description

Parameters	Description
destination	The hostname or IP address of the server that you want to ping.

Parameters	Description
count	(Option)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 traceroute *destination*

Syntax Description

Parameters	Description
destination	The hostname or IP address of the server to which you want to send a trace.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils ntp

This command displays the NTP status or configuration.

Command Syntax

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

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils ntp restart

This command restarts the NTP service.

Command Syntax

utils ntp restart

Parameters

None

Requirements

Level privilege: 0

Command privilege: 0

Allowed during upgrade: Yes

utils ntp server add

The command adds up to 5 specified NTP servers.

Usage Guidelines

norestart results in the NTP service not being restarted after adding the servers.

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

Command Syntax

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

Usage Guidelines

Note the following:

- Mandatory parameter: at least one NTP server to add.
- Optional parameters: up to four more ntp servers and the norestart option.

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 2

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 3

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 4

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 5

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 6

Adding inaccessible server without norestart

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

Example 7

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 must be restarted for the changes to take effect.
```

Example 8

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
```

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils ntp server delete

The command deletes any configured NTP server or all of them.

Usage Guidelines

After the user enters their choice, they are prompted if they would like to restart the NTP service.

Answering No results in the NTP service not being restarted after deleting the servers.

Note If the user chooses not to restart the NTP service, an explicit restart of the NTP service is required for the changes to take effect.

Command Syntax

utils ntp server delete

Example 1

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 2

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 is deleted from the list of configured NTP servers.
Continue (y/n)?y
clock1.cisco.com:  deleted successfully.
Restarting NTP on the server.
admin:
```

Example 3

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 results 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 must be restarted for the changes to take effect.
admin:
```

Example 4

Deleting all servers when no servers are configured

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

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils ntp server list

The command lists the configured NTP servers.

Command Syntax

utils ntp server list

Example 1

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 2

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 3

Listing servers when no servers are configured

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

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

utils ntp start

This command starts the NTP service, if it is not already running.

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

Command Syntax

utils ntp start

Requirements

Level privilege: 0

Command privilege: 0

Allowed during upgrade: Yes

utils os kerneldump

This command configures kerneldump to provide a kernel crash dumping mechanism. The kernel captures the dump to the local disk, in case of a kernel crash.

Note The netdump commands have been removed from release 8.6(1) and have been replaced with the kerneldump commands.

Command Syntax

utils os kerneldump {**enable**|**disable**}

Useage Guidelines

If a kernel crash occurs, the capture kernel dumps the core on the local disk of the server. The primary kernel reserves 128MB of physical memory that the capture kernel uses to boot. The kerneldump uses the **kexec** command to boot into a capture kernel whenever the kernel crashes.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Example

```
admin: utils os kerneldump enable
***************WARNING******************
Enabling kerneldump requires system reboot
Would you like to boot the machine (y/n):y
kerneldump enable operation succeeded
System going for a reboot
```

utils os kerneldump ssh

This command enables, disables, or displays the status of an external SSH server.

Command Syntax

utils os kerneldump ssh {**enable**|**disable**|**status**}

Syntax Description

Parameters	Description
enable	Configures an external SSH server as a kerneldump server to kernel dumps.
disable	Removes support of the external SSH server that is configured to collect kernel dumps.
status	Indicates whether an external SSH server is configured or not, to collect kernel dumps.

Useage Guidelines

If external SSH server has the kerneldump service enabled and a kernel crash occurs, the capture kernel dumps the core on the external server that is configured to collect the dump.Enabling and disabling kerneldump require a system reboot for the changes to come into effect.

Command Mode

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Example

```
admin: utils os kerneldump ssh disable 10.77.31.60
Disabling kerneldump requires system reboot
Would you like to continue (y/n): y
kerneldump disable operation succeeded
System going for a reboot
```

utils os secure

This command is used to specify the level of security provided by selinux.

Command Syntax

utils os secure {**enforce** |**permissive**|**status**}

Useage Guidelines

The selinux does not handle rate limiting. Rate limiting is handled by ipprefs and ip tables.

Command Mode

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils remote_account

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

Command Syntax

Command	Result
utils remote_account status	This command allows you to check the status of a remote account.
utils remote_account enable	This command allows you to enable a remote account.
utils remote_account disable	This command allows you to disable a remote account.
utils remote_account create *username life*	This command creates a remote account.

Syntax Description

Parameters	Description
username	The name of the remote account. The username can contain only lowercase characters and must be more than six-characters long.

Parameters	Description
life	The life of the account in days. After the specified number of day, the account expires.

Usage Guidelines

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

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Example

```
utils remote_account status
```

utils reset_application_ui_administrator_name

This command resets the application user interface administrator name.

Command Syntax

utils reset_application_ui_administrator_name

Command Mode

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils reset_application_ui_administrator_password

This command resets the application user interface administrator password.

Command Syntax

utils reset_application_ui_administrator_password

Command Mode

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils service

This command stops, starts, or restarts a service.

Command Syntax

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

Syntax Description

Parameters	Description
service-name	The name of the service that you want to stop or start: • System NTP • System SSH • Cisco IDS • Cisco Tomcat • Cisco Database Layer Monitor • Cisco Emergency Responder • Cisco Phone Tracking Engine • Cisco DB Replicator • CER Provider • Cisco CDP • Cisco CDP Agent • Cisco Certificate Expiry Monitor • Cisco DRF Local • Cisco DRF Master • Cisco Tomcat • Host Resources Agent • MIB2 Agent • SNMP Master Agent • System Application Agent
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**]

Syntax Description

Parameters	Description
page	(Option)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]*	This interactive command gets the SNMP data using the specified version for the specified MIB OID.
utils snmphardware-agents [**status** | **restart**]	This command affects the SNMP agents on the server.
utils snmptest	
utils snmpwalk *version community ip-address object [file]*	This interactive commands walks through the SNMP MIB.

Syntax Description

Parameters	Description
get	Displays the value of the specified SNMP object.
hardware-agents status	Displays the status of the hardware agents on the server.
hardware-agents	Stops all SNMP agents provided by the hardware vendor.

Parameters	Description
hardware-agents restart	Restarts the hardware agents on the server.
test	Tests the SNMP host by sending sample alarms to local syslog and remote syslog.
walk	Walks the SNMP MIB, starting with the specified SNMP object.
version	Specifies the SNMP version. Possible values are 1 or 2c.
community	Specifies the SNMP community string.
ip-address	Specifies the IP address of the server. Enter 127.0.0.1 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 config 1/2c community-string

This interactive command adds, deletes, lists or updates a community string.

Command Syntax

utils snmp config 1/2c community-string {**add**|**delete** |**list**|**update**}

Syntax Description

Parameters	Description
add	Adds a new community string.
delete	Deletes a community string.
list	Lists all community strings.
update	Updates a community string.

Useage Guidelines

The system prompts you for the parameters.

The SNMP Master Agent service is restarted for configuration changes to take effect. Do not abort command after execution until restart is complete. If the command is aborted during service restart, verify service status

of SNMP Master Agent by using **utils service list**. If service is down, start it by using **utils service start SNMP Master Agent** .

Command Mode

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils snmp config 3 user

This interactive command affects v3 user configuration.

Command Syntax

utils snmp config 3 user {**add**|**delete**|**list**|**update**}

Syntax Description

Parameters	Description
add	Adds a new v3 user with the v3 authentication and privacy passwords.
delete	Deletes the configuration information for an existing v3 user.
list	Lists the v3 users currently configured.
update	Updates configuration information for an existing v3 user.

Useage Guidelines

The system prompts you for the parameters.

Command Mode

Administrator (admin:)

Requirements

Command privilege level:1

Allowed during upgrade: Yes

utils snmp config mib2

This command affects the Mib2 configuration information.

Command Syntax

utils snmp config mib2 {**add**|**delete**|**list**|**update**}

Syntax Description

Parameters	Description
add	Adds the Mib2 configuration information.
delete	Deletes the Mib2 configuration information.
list	Lists the Mib2 configuration information.
update	Updates the Mib2 configuration information.

Useage Guidelines

The system prompts you for the parameters.

Command Mode

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

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 prompts you for the parameters]

Example

```
If you run snmp walk on a leaf in the MIB you basically get what you would
get with 'utils snmp get ...' command. Here is the sample walk
output we are getting 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
.....
```

If you provide an IP address of a remote host the command is executed on that remote host. You have to provide the IP address, not the domain name.

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils snmp get 3

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

Command Syntax

utils snmp get 3

[system prompts you for the parameters]

Usage Guidelines

If you use this command on a specific OID (leaf) in the MIB, you will get the value of the MIB. 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

If you provide an IP address of a remote host, the command is executed on that remote host. You have to provide the IP address not the domain name.

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils system

This command restarts the system on the same partition, restarts the system on the inactive partition, or shuts down the system.

Command Syntax

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

Syntax Description

Parameters	Description
restart	Restarts the system.
shutdown	Shuts down the system.
switch-version	Switches to the product release installed on the inactive partition.

Usage Guidelines The **utils system shutdown** command has a 5-minute timeout. If the system does not shut down within 5 minutes, the command gives you the option of doing a forced shutdown.

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**}

Syntax Description

Parameters	Description
console	Redirects the system boot output to the console.
serial	Redirects the system boot output to the COM1 (serial port 1).
status	Displays the where the serial boot output currently gets sent.

Requirements

Level privilege: 1

Command privilege: 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**}

Syntax Description

Parameters	Description
cancel	Cancels the active upgrade.
initiate	Starts a new upgrade wizard or assumes control of an existing upgrade wizard. The wizard prompts you for the location of the upgrade file.
status	Displays the status of an upgrade.

Usage Guidelines

To upgrade the system, follow these steps:

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

utils vmtools status

This command shows the version of the currently running VMware Tools.

Command Syntax

utils vmtools status

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils vmtools upgrade

This command updates the currently installed VMware Tools to the latest version required by the ESXi host for that VM.

Command Syntax

utils vmtools upgrade