Set commands

- set account*, page 2
- set accountlocking*, page 3
- set alarm*, page 5
- set auditlog*, page 7
- set cert*, page 10
- set cli*, page 12
- set commandcount, page 13
- set csr gen, page 14
- set date, page 14
- set dscp*, page 15
- set hcs*, page 17
- set ipsec*, page 26
- set logging, page 27
- set network*, page 28
- set password*, page 42
- set session maxlimit, page 51
- set smtp, page 52
- set timezone, page 52
- set trace*, page 53
- set web-security, page 56
- set webapp session timeout, page 57
- set workingdir, page 58

set account*

set account enable

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

set account enable *user-id*

Syntax Description

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

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: No

set account name

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

set account name *name*

Syntax Description

Parameters	Description
name	Represents the username for the new account.

Command Modes

Administrator (admin:)

Usage Guidelines

After you enter the username, the system prompts you to enter the privilege level (0 or 1) and password for the new account. The privilege levels definitions are as follows:

Privilege level 0

Specifies an ordinary privilege level. Users with ordinary privileges can run CLI commands with privilege level 0 only.

Privilege level 1

Specifies an advanced privilege level. Users with advanced privileges can run CLI commands with privilege level 1 and below.

Note The administrator account that the system creates when Unified Communications Manager installs has a privilege level of 4. The administrator can run all commands in the CLI.

Requirements

Command privilege level: 0

Allowed during upgrade: No

set accountlocking*

set accountlocking

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

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

Syntax Description

Parameters	Description
enable	Enable account locking.
disable	Disable account locking.

Command Modes

Administrator (admin:)

Usage Guidelin

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

Requirements

set accountlocking count

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

set accountlocking count *attempts*

Syntax Description

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

Command Modes

Administrator (admin:)

Usage Guidelines

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

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

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

set accountlocking unlocktime

This command configures the unlock time for the current Unified Communications Manager admin accounts

set accountlocking unlocktime *seconds*

Syntax Description

Parameters	Description
seconds	Specifies the unlock time in seconds. Valid values: greater than 300 seconds, but less than 3600 seconds (60 minutes).

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

set alarm*

set alarm default

This command sets the alarm configuration to the factory defaults.

Command Syntax

set alarm default

Note The system prompts you for the service name.

Parameter

For a list of services, see the "Services on Cisco HCM-F" in the *Cisco Hosted Collaboration Mediation Fulfillment Planning Guide, Release 10.1(1)*.

Requirements

Command privilege level: 0

Allowed during upgrade No

set alarm remotesyslogserver

This command sets the alarm for the remote syslog server.

Command Syntax

set alarm remotesyslogserver

Note The system prompts you for the parameters.

Parameters

- remotesyslogserver specifies the name of the remote syslog server.
- For a list of services, see the *Cisco Hosted Collaboration Mediation Fulfillment Planning Guide, Release 10.1(1)*.

Requirements

Command privilege level: 0

Allowed during upgrade: No

set alarm status

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

Command Syntax

set alarm status

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

Parameters

Syntax Description

Parameters	Description
status	enable disable
monitor name	SDI SDL Event Log Sys Log

For a list of services, see the *Cisco Hosted Collaboration Mediation Fulfillment Planning Guide, Release 10.1(1)*.

Requirements

Command privilege level: 0

Allowed during upgrade: No

set alarm severity

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

Command Syntax

set alarm severity

Note The system prompts you for the severity, the monitor name and the service name.

Parameters

- severity
  - **Emergency**
  - **Alert**

- **Critical**
- **Error**
- **Warning**
- **Notice**
- **Informational**
- **Debug**

- monitor name
  - **SDI**
  - **SDL**
  - **Event_Log**
  - **Sys_Log**

- For a list of services, see the *Cisco Hosted Collaboration Mediation Fulfillment Planning Guide, Release 10.1(1)*.

Requirements

Command privilege level: 0

Allowed during upgrade: No

set auditlog*

set auditlog status

This command enables or disables the audit log.

Command Syntax

set auditlog status

Note The system prompts you for the parameters.

Parameters

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

Requirements

Command privilege level: 0

Allowed during upgrade: No

set auditlog purging

This command enables or disables audit log purging.

Command Syntax

set auditlog purging

Note The system prompts you for the parameters.

Parameters

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

Requirements

Command privilege level: 0

Allowed during upgrade: No

set auditlog logrotation

This command enables or disables the audit log log rotation.

Command Syntax

set auditlog logrotation

Note The system prompts you for the parameters.

Parameters

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

Requirements

Command privilege level: 0

Allowed during upgrade: No

set auditlog maxfilesize

This command sets the audit log maximum file size.

Command Syntax

set auditlog maxfilesize

Note The system prompts you for the parameters.

Parameters

size specifies an integer between 1 and 10.

Requirements

Command privilege level: 0

Allowed during upgrade: No

set auditlog maxnumfiles

This command sets the audit log maximum number of files count.

Command Syntax

set auditlog maxnumfiles

Note The system prompts you for the parameters.

Parameters

filecount specifies an integer between 1 and 10000.

Requirements

Command privilege level: 0

Allowed during upgrade: No

set auditlog remotesyslogseverity

This command sets the audit log remote syslog severity to the specified severity.

Command Syntax

set auditlog remotesyslogseverity

Note The system prompts you for the parameters.

Parameters

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

Requirements

Command privilege level: 0

Allowed during upgrade: No

set auditlog remotesyslogserver

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

Command Syntax

set auditlog remotesyslogserver

Note The system prompts you for the parameters.

Parameters

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

Requirements

Command privilege level: 0

Allowed during upgrade: No

set cert*

set cert delete

This command deletes a specific certificate file from the trust unit.

set cert delete *unit name*

Syntax Description

Parameters	Description
unit	Specifies the name of the trust category, as “own” or “trust”.
name	Certificate file name.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Example

```
admin:set cert delete cucm siptest.pem
```

set cert import

This command imports the specified certificate for the specified certificate type.

set cert import *type name* [*caCert*]

Syntax Description

Parameters	Description
type	Specifies the certificate type as “own” or “trust”.
name	Represents the unit name.
[*caCert*]	Represents the name of the CA certificate file name.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Example

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

set cert regen

This command regenerates the certificate for the specified unit.

set cert regen *name*

Syntax Description

Parameters	Description
name	Represents the unit name.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Example

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

set cli*

set cli pagination

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

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

Syntax Description

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

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

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

set cli session timeout

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

set cli session timeout *minutes*

Syntax Description

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

Command Modes

Administrator (admin:)

Usage Guidelines

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

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

set commandcount

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

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

Syntax Description

Parameters	Description
enable	Turns on command count.

Parameters	Description
disable	Turns off command count.

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

set csr gen

This command generates the csr for the unit name.

set csr gen *name*

Syntax Description

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

Command Modes Administrator (admin:)

Requirements

Example

```
admin:set csr gen tomcat
Successfully Generated CSR for tomcat.
```

Requirements

Command privilege level: 1

Allowed during upgrade: No

set date

This command changes the time and date on the server.

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

Syntax Description

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

Command Modes

Administrator (admin:)

Usage Guidelines

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

Requirements

Set Date and Time to 2:10:33 Pm April 13th 2012 Example

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

set dscp*

set dscp defaults

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

set dscp defaults

Command Modes

Administrator (admin:)

Usage Guidelines

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

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

set dscp

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

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

Syntax Description

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

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

set dscp marking

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

set dscp marking *port_tag value*

Syntax Description

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

Command Modes

Administrator (admin:)

Usage Guidelines

The valid class names as defined by DSCP are:

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

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

- Expedited Forwarding: value EF

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

- Best Effort: value BE

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

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

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

set hcs*

set hcs api-gateway-proxy global-address

This command configures the global address. When using a load balancer, you must configure the global address on the API Gateway Proxy to match the virtual IP address used by the load balancer.

Note This value can be set from any node in the cluster.

When the value is set on one node, it will propagate to the other nodes in the cluster automatically.

Command syntax

set hcs api-gateway-proxy global-address

Parameters

Hostname or IP address.

Note Leaving this parameter blank clears the setting.

Example

```
admin:set hcs api-gateway-proxy global-address 10.10.10.10
api-gateway-proxy global-address is 10.10.10.10

admin:set hcs api-gateway-proxy global-address
api-gateway-proxy global-address has been cleared
```

Requirements

Command privilege level: 1

Allowed during upgrade: No

set hcs api-gateway-proxy global-http-port

This command configures the global http port. When using the load balancer, you must configure the global http port on the API Gateway Proxy to match the non-secured port used by the load balancer.

Note This value can be set from any node in the cluster.

When the value is set on one node, it will propagate to other nodes in the cluster automatically.

Command syntax

set hcs api-gateway-proxy global-http-port

Parameters

http port number

Note Leaving this parameter blank clears the setting.

Example

```
admin:set hcs api-gateway-proxy global-http-port 8089
api-gateway-proxy global-http-port is set to 8089
admin:set hcs api-gateway-proxy global-http-port
api-gateway-proxy global-http-port has been cleared
```

Requirements

Command privilege level: 1

Allowed during upgrade: No

set hcs api-gateway-proxy global-https-port

This command configures the global https port. When using the load balancer, you must configure the global https port on the API Gateway Proxy to match the SSL port used by the load balancer (default 443).

Note This value can be set from any node in the cluster.

When the value is set on one node, it will propagate to other nodes in the cluster automatically.

Command syntax

set hcs api-gateway-proxy global-https-port

Parameters

https port number

Note Leaving this parameter blank clears the setting.

Example

```
admin:set hcs api-gateway-proxy global-https-port 8088
api-gateway-proxy global-https-port is set to 8088
admin:set hcs api-gateway-proxy global-https-port
api-gateway-proxy global-https-port has been cleared
```

Requirements

Command privilege level: 1

Allowed during upgrade: No

set hcs cluster node

This command adds a node to the cluster or updates a node on the cluster. This command can only be executed on the primary node (HCS application node).

Note It is important to specify the actual hostname of the node in order to correctly add the node to the cluster. If you do not use the actual hostname, you may overwrite an existing entry.

Command syntax

set hcs cluster node

Parameters

- **Node Type :** the type of node to set, either “app” for an HCS application node or “ws” for an HCS Web Services node. Since application nodes are automatically added to the cluster when installed, there is no method to add an application node.
- **Server Hostname:** the hostname of the node.
- **IP address:** the IP address of the node.

Example

```
admin:set hcs cluster node
Enter Node Type: ws
Enter Server Hostname: vm-csf-hcmf-ws
Enter IP address[10.81.55.170]:
Node successfully added to the cluster
```

Error messages

`Not an authorized node to add nodes. Has to be an App Node`

This command can only be executed on the primary node (HCS application node).

`Duplicate node exists. Cannot create the node`

A node with the same hostname and IP address already exists in the cluster.

Requirements

This command can only be executed on the primary node (HCS application node).

Command privilege level: 1

Allowed during upgrade: No

Note **show hcs cluster verify detailed** must be executed after running **set hcs cluster config** in order to verify the cluster configuration.

set hcs hlm audit-interval

This setting determines interval (in hours) that HLM should perform an audit to verify its license integrity.

Command syntax

set hcs hlm audit-interval [hours]

Parameters

hours: must be between 4 and 24.

Example

```
admin:set hcs hlm audit-interval 1
HLM Audit Interval (Hours) must fall between 4 and 24
admin:set hcs hlm audit-interval 4
HLM Audit Interval (Hours) has been updated to '4'
admin:set hcs hlm audit-interval 24
HLM Audit Interval (Hours) has been updated to '24'
admin:set hcs hlm audit-interval 18
HLM Audit Interval (Hours) has been updated to '18'
admin:set hcs hlm audit-interval 30
HLM Audit Interval (Hours) must fall between 4 and 24
```

Requirements

Command privilege level: 1

Allowed during upgrade: No

set hcs hlm license-report-retention-days

This setting determines the number of days that Cisco HCS License Manager should retain any generated license report files.

Command syntax

set hcs hlm license-report-retention-[days]

Parameters

days: must be between 1 and 120.

Example

```
admin:set hcs hlm license-report-retention-days 0
HLM License Report Retention (Days) must fall between 1 and 120
admin:set hcs hlm license-report-retention-days 1
HLM License Report Retention (Days) has been updated to '1'
```

Requirements

Command privilege level: 1

Allowed during upgrade: No

set hcs hlm disk-space

This command determines the maximum size (in megabytes) of the HCS License Manager report repository disk space.

Command syntax

set hcs hlm disk-space [Size of report repository]

Parameters

Size of report repository: The size of the report repository.

Example

```
admin:set hcs hlm disk-space 1
HLM Disk Space (Megabytes) has been updated to '1'
```

Requirements

Command privilege level: 1

Allowed during upgrade: No

set hcs jmsconfig

This command retrieves the JMS Broker configuration from the supplied IP address. The supplied IP address should be an application node with this node the cluster table. This command is meant to restore JMS Connectivity after the IP/Hostname has been changed on the application node.

After an IP/Hostname change, **set hcs jmsconfig**, **set hcs sdrconfig** and **set hcs appnodeconfig** should only be run if **set hcs cluster config** is attempted first.

After running **set hcs cluster config**, the admin can verify the cluster configuration using **show hcs cluster verify detailed**. If **show hcs cluster verify detailed** still indicates problems, **set hcs jmsconfig**, **set hcs sdrconfig** and **set hcs appnodeconfig** can be used to restore the cluster configuration.

set hcs version could also be used after an IP/Hostname change or a WS node upgrade (L2 or Refresh-Upgrade) or after a WS node install. If the WS node completes the upgrade (or install) and the **show hcs cluster nodes** does not show the WS node's actual version, **set hcs cluster version** can be used to update the APP node's record for the WS node's version.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set hcs link auto-primecollab-linkage

This setting determines whether or not HCS Fulfillment Service attempts to automatically associate a Prime Collaboration with a Customer in SDR. When this setting is enabled, and a new Customer is added to SDR, the service searches for the Prime Collaboration with the lowest device utilization that is beneath the customer and device warning thresholds, which is linked to the new Customer. When this setting is disabled, no such automatic linking occurs.

Command Syntax

set hcs link auto-primecollab-linkage {**enable** | **disable**}

Parameters

- **enable** turns on the set hcs link auto-primecollab-linkage.
- **disable** turns off the set hcs link auto-primecollab-linkage.

set hcs link auto-vm-linkage

This command determines whether or not Cisco Hosted Collaboration Mediation Link Service will attempt to automatically associate a virtual machine with an Application Instance in SDR. When this command is enabled, the service will look for a match between the virtual machine's guest OS hostname and the hostname of the Network Address associated with the Application Instance. If there is a match, the virtual machine links to the Application Instance. When this command is disabled, no such automatic behavior is attempted.

Command Syntax

set hcs link auto-vm-linkage {**enable** | **disable**}

Parameters

- **enable** turns on the hcs link auto-vm-linkage.
- **disable** turns off the hcs link auto-vm-linkage.

Requirements

Command privilege level: 0

Allowed during upgrade: No

set hcs ipa require-vcenter-certificate

The IPA service can be set for each vCenter connection.

This setting defaults to false and can only be set for the entire service, not a specific vCenter.

Before enabling this setting, ensure that the necessary certificates are in the HCM-F tomcat trust store for each vCenter.

Without a certificate, IPA will fail to connect to the vCenter and will display an error message. After changing the setting to enable vCenter certificates, the IPA service must be restarted to ensure that all open vCenter sessions are reopened with certificates.

If the setting is changed to disabled, a restart is not necessary unless it is essential that all sessions not use vCenter certificates. As a general practice, restarting the service after either change is the best way to ensure that all IPA vCenter sessions use the same type of authentication.

Command Syntax

set hcs ipa require-vcenter-certificate {**enable** | **disable**}

Parameters

- **enable** turns on the vcenter require-certificate for each vCenter connection
- **disable** turns off the vcenter require-certificate for each vCenter connection

Requirements

Command privilege level: 0

Allowed during upgrade: No

set hcs postinstall

This command completes the postinstallation setup after an HCS application or Web Services node has been installed or upgraded.

Before executing this command on a WS node, ensure that you have added the node to the cluster on the application node. See **set hcs cluster node**.

Command syntax

set hcs postinstall

Parameters

- **Primary Node IP Address**: the hostname or IP address of the primary node (application node). This parameter is only displayed when executing the command on the WS node.
- **Primary Node Password**: the password on the primary node (application node). You must enter the administrator user password as it is configured in the primary node. This parameter is only displayed when executing the command on the WS node.

Example on an HCS application node

```
admin:set hcs postinstall
PostInstall configuration will run after you acknowledge to a server
re-boot
Is it ok to undergo a reboot of the system?
Continue (y/n)?
```

Example on a HCS Web Services node

```
admin:set hcs postinstall
Enter Primary Node IP Address: 10.81.55.203
Enter Primary Node Password: **********
PostInstall configuration will run after you acknowledge to a server
re-boot
Is it ok to undergo a reboot of the system?
Continue (y/n)?
```

Error messages

```
The node was not found in the cluster. This is because the configured
hostname and ip for this node must match a node entry in the cluster of
the primary node or the primary node is not available at the moment
```

You must add an HCS WS node to the primary node using the **set hcs cluster node** command.

Requirements

For a Web Services (WS) node, ensure that you have added the WS node to the cluster on the application node. See **set hcs cluster node**.

set hcs sdrconfig

This command, if run on the application node, compares the hostname and IP Address from local network configuration to the SDR's configuration files. If there's a mismatch, the SDR configuration files are updated with the values from the platform. The CLI also prompts the user for the option to reboot. If there is no change detected, there is no reboot.

On a WS node, this command retrieves the SDR configuration from the supplied IP address. This command is meant to restore SDR Connectivity after the IP/Hostname has been changed on the application node.

set hcs ucsmsync require-ucsm-certificate

This command controls whether the UCSMSync service needs to verify the security certificate of the UCS Managers that it connects to. If the value is set to Enable, any UCS Manager that the Cisco HCS UCSMSync service connects to needs to have its public certificate uploaded to the Cisco HCM-F platform. If the value is set to Disable, the Cisco HCS UCSMSync service does not check the UCS Manager's certificate when they are connected. Use the command **set cert import** to upload the certificate.

Command Syntax

set hcs ucsmsync require-ucsm-certificate {**enable** | **disable**}

Parameters

- **enable** turns on the ucsmsync require-ucsm-certificate.
- **disable** turns off the ucsmsync require-ucsm-certificate.

Note The command is set to Disable by default.

After you set the parameter to Enable, you must restart the UCSMSync service. If the setting is changed to Disable, a restart is not necessary unless no sessions can use UCS Manager certificates. As a general practice, restarting the service after either change is the best way to ensure that all UCS Manager sessions use the same type of authentication.

Requirements

Command privilege level: 0

Allowed during upgrade: No

set hcs vcentersync require-vcenter-certificate

This command controls whether VCenterSync service needs to verify the security certificate of the vCenters that it connects to. If the value is set to Enable, then the vCenters that the Cisco HCS VCenter Sync Service connects to needs to have its public certificate uploaded to the Cisco HCM-F platform. If the value is set to Disable, then the Cisco HCS VCenter Sync Service does not check the vCenter's certificate when they are connected. Use the command **set cert import** to upload the certificate.

Command Syntax

set hcs vcentersync require-vcenter-certificate {**enable** | **disable**}

Parameters

- **enable** turns on the vcentersync require-vcenter-certificate.
- **disable** turns off the vcentersync require-vcenter-certificate.

Requirements

Command privilege level: 0

Allowed during upgrade: No

set hcs version

This command is meant to fix disparity between actual installed HCS software version and what is being reported in the cluster table. Running this command will update the cluster table on the with the HCS version of the node this command was run from.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Example

```
admin:set hcs version
Version successfully updated to: 10.0.0.98030-1 in the Cluster Table.
```

set ipsec*

set ipsec policy_group

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

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

Syntax Description

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

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

set ipsec policy_name

This command enables the specified ipsec policy.

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

Syntax Description

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

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

set logging

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

set logging {**enable| disable**}

Syntax Description

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

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: No

set network*

set network dhcp eth0

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

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

Syntax Description

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

Command Modes

Administrator (admin:)

Usage Guidelin

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

set network dns

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

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

Syntax Description

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

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

set network dns options

This command sets DNS options.

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

Syntax Description

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

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

set network domain

This command sets the domain name for the system.

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

Note Reboot the servers one at a time in order for the phones to register correctly. For more information about changing the domain name, see *Changing the IP Address and Hostname for Cisco Unified Communications Manager*.

set network domain [*domain-name*]

Syntax Description

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

Command Modes

Administrator (admin:)

Usage Guidelines

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

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

set network failover

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

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

Syntax Description

Parameters	Description
ena	Enables Network Fault Tolerance.
dis	Disables Network Fault Tolerance.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

set network gateway

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

set network gateway *addr*

Syntax Description

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

Command Modes

Administrator (admin:)

Usage Guidelines

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

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

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. Additionally, before attempting a Hostname (or Hostname and IP address) change, the administrator should perform the following:

- verify the cluster configuration does not have any configuration problems by executing **show hcs cluster verify detailed**
- update the cluster configuration by executing **set hcs cluster config**
- validate the cluster configuration by executing **show hcs cluster verify detailed**

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 Modes

Administrator (admin:)

Usage Guidelines

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

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

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 eth0

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

Before attempting this command, the administrator should have a valid DRF backup. Additionally, before attempting an IP address change, the administrator should perform the following:

- verify the cluster configuration does not have any configuration problems by executing **show hcs cluster verify detailed**
- update the cluster configuration by executing **set hcs cluster config**
- validate the cluster configuration by executing **show hcs cluster verify detailed**

set network ip eth0 *addr mask gw*

Syntax Description

Parameters	Description
eth0	Specifies Ethernet interface 0.
addr	Represents the IP address that you want to assign.
mask	Represents the IP mask that you want to assign.
gw	Represents the IP default gw that you want to assign.

Command Modes

Administrator (admin:)

Usage Guidelines

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

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

set network ipv6 dhcp

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

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

Syntax Description

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

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

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

set network ipv6 gateway

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

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

Syntax Description

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

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

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

set network ipv6 service

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

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

Syntax Description

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

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

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

set network ipv6 static_address

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

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

Syntax Description

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

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

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

set network max_ip_conntrack

This command sets the ip_conntrack_max value.

set network max_ip_conntrack *ip_conntrack_max value*

Syntax Description

Parameters	Description
ip_conntrack_max value	Specifies the value for ip_conntrack_max. **Note** The value of ip_conntrack_max cannot be less than 65536.

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Example

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

set network mtu

This command sets the maximum MTU value.

set network mtu *mtu_max*

Syntax Description

Parameters	Description
mtu_max	Specifies the maximum MTU value. The system default MTU value equals 1500. **Caution** When packets on UDP port 8500 that have the DF bit set are exchanged between nodes, if there is any policy on the WAN router to clear the DF bit and fragment large packets, this may cause dbreplication issues.

Command Modes

Administrator (admin:)

Usage Guidelines

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

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

Example

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

set network nic eth0

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

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

Syntax Description

Parameters	Description
eth0	Specifies Ethernet interface 0.
auto	Specifies whether auto negotiation gets enabled or disabled.
speed	Specifies whether the speed of the Ethernet connection: 10 or 100 Mb/s.

Parameters	Description
duplex	Specifies half-duplex or full-duplex.

Command Modes Administrator (admin:)

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

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

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

set network pmtud state

This command enables and disables Path MTU Discovery.

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

Syntax Description

Parameters	Description
enable	Enables Path MTU Discovery.
disable	Disables Path MTU Discovery.

Command Modes Administrator (admin:)

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

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

Example

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

set network restore

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

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

Syntax Description

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

Command Modes

Administrator (admin:)

Usage Guidelines

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

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

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Example

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

set network status eth0

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

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

Syntax Description

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

Command Modes

Administrator (admin:)

Usage Guidelines

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

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

set password*

set password age

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

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

Syntax Description

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

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

set password change-at-login

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

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

Syntax Description

Parameters	Description
disable	This does not force users to change their password.

Parameters	Description
enable	This forces users to change their password when they sign in to the system the next time.
userid	Specifies the affected user account.

Command Modes

Administrator (admin:)

Usage Guidelines

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

Requirements

Command privilege level: 4

Allowed during upgrade: No

set password complexity character

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

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

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

Syntax Description

Parameters	Description
disable	This turns off password complexity for character types.
enable	This turns on password complexity for character types. **Note** When you disable password complexity, you also turn off **password character difference**, **password character max-repeat**, and **password history**.

Parameters	Description
num-char	This specifies the number of characters required from each of the four character sets: lowercase, uppercase, numbers, and special characters. • Value range: 0-8 • Default value: 1

Command Modes

Administrator (admin:)

Usage Guidelines

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

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

set password complexity character difference

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

set password complexity character difference *num-char*

Syntax Description

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

Command Modes Administrator (admin:)

Usage Guidelines Enter 0 to indicate no difference.

Note The maximum password length is 31 characters.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set password complexity character max-repeat

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

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

Syntax Description

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

Command Modes Administrator (admin:)

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.

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

Syntax Description

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

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Example

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

set password expiry minimum-age

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

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

Syntax Description

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

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Example

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

set password expiry user maximum-age

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

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

Syntax Description

Parameters	Description
enable	Turns on the maximum age password expiry settings for a particular Cisco Unified Operating System administrator account. The set password expiry user enable command sets the value of maximum password age to 3650 days (10 yrs) for the Cisco Unified Operating System Administrator account.

Parameters	Description
disable	Turns off the maximum age password expiry settings for a particular Cisco Unified Operating System administrator account. The set password expiry user disable command results in that Cisco Unified Operating System Administrator account never expiring.
userid	Specifies a particular Cisco Unified Operating System Administrator account.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Example

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

set password expiry user minimum-age

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

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

Syntax Description

Parameters	Description
enable	Turns on the minimum age password expiry settings for a particular Cisco Unified Operating System administrator account.
disable	Turns off the minimum age password expiry settings for a particular Cisco Unified Operating System administrator account.
userid	Specifies a particular Cisco Unified Operating System Administrator account.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Example

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

set password history

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

set password history *number*

Syntax Description

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

Command Modes

Administrator (admin:)

Usage Guidelines

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

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

set password inactivity

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

Syntax Description

Parameters	Description
enable	Enable the password inactivity globally and update individual OS users according to the setting.

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

Command Modes Administrator (admin:)

Usage Guidelines

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

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

set password user admin

This command allows you to change the administrator password.

set password user admin

Command Modes Administrator (admin:)

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

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

set password user security

This command allows you to change the security password.

set password user security

Command Modes Administrator (admin:)

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

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

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

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

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

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

Requirements

Command privilege level: 1

Allowed during upgrade: No

set session maxlimit

This command sets the upper limit for concurrent sessions.

set session maxlimit [*value*]

Syntax Description

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

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

set smtp

This command sets the SMTP server hostname.

set smtp *hostname*

Syntax Description

Parameters	Description
hostname	Represents the SMTP server name.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: No

set timezone

This command lets you change the system time zone.

set timezone *zone*

Syntax Description

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

Command Modes

Administrator (admin:)

Usage Guidelines

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

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

Requirements

Command privilege level: 0

Allowed during upgrade: No

Example Setting Time Zone to Pacific Time

```
admin:set timezone Pac
```

set trace*

set trace default

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

Command Syntax

set trace default

Note The system prompts you for the service name.

Usage Guidelines

For a list of services, see the *Cisco Hosted Collaboration Mediation Fulfillment Planning Guide, Release 10.1(1)*.

Requirements

Command privilege level: 0

Allowed during upgrade: No

set trace status

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

Command Syntax

set trace status

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

Parameters

- *status* = **enable** | **disable**
- For a list of services, see the *Cisco Hosted Collaboration Mediation Fulfillment Planning Guide, Release 10.1(1)*.

Requirements

Command privilege level: 0

Allowed during upgrade: No

set trace tracelevel

This commands sets the trace level for the specified service.

Command Syntax

set trace tracelevel

Note The system prompts you for the trace level and service name.

Parameters

- *tracelevel* = use "show tracelevels" CLI command to find allowed trace levels for a given service name.
- For a list of services, see the *Cisco Hosted Collaboration Mediation Fulfillment Planning Guide, Release 10.1(1)*.

Requirements

Command privilege level: 0

Allowed during upgrade: No

set trace maxfilesize

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

Command Syntax

set trace maxfilesize

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

Parameters

- *size* in MBs specifies an integer value between 1 and 10.
- For a list of services, see the *Cisco Hosted Collaboration Mediation Fulfillment Planning Guide, Release 10.1(1)*.

Requirements

Command privilege level: 0

Allowed during upgrade: No

set trace maxnumfiles

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

Command Syntax

set trace maxnumfiles

Note The system prompts you for the file count and the service name.

Parameters

- *filecount* represents an integer value from 1 to 10000.
- For a list of services, see the *Cisco Hosted Collaboration Mediation Fulfillment Planning Guide, Release 10.1(1)*.

Requirements

Command privilege level: 0

Allowed during upgrade: No

set trace usercategories

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

Command Syntax

set trace usercategories

Note The system prompts you for the flag number and the service name.

Parameters

- *flagnumber* specifies 0 to 7FFF. 7FFF means all the flags get enabled.

- For a list of services, see the *Cisco Hosted Collaboration Mediation Fulfillment Planning Guide, Release 10.1(1)*.

Requirements

Command privilege level: 0

Allowed during upgrade: No

set web-security

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

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

Syntax Description

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

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: No

Example

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

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

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

set webapp session timeout

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

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

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

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

set webapp session timeout *minutes*

Syntax Description

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

Command Modes

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.

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

Syntax Description

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

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0 for logs, 1 for TFTP

Allowed during upgrade: Yes