



## Set Commands

---

- [set account enable](#), on page 3
- [set account name](#), on page 3
- [set accountlocking](#), on page 4
- [set accountlocking count](#), on page 5
- [set accountlocking unlocktime](#), on page 6
- [set cert bulk consolidate](#), on page 6
- [set cert bulk export](#), on page 7
- [set cert bulk import](#), on page 8
- [set cert bulk sftp](#), on page 8
- [set cert delete](#), on page 9
- [set cert import](#), on page 9
- [set cert regen](#), on page 10
- [set cert regen ITLRecovery](#), on page 10
- [set cli pagination](#), on page 11
- [set cli session timeout](#), on page 12
- [set commandcount](#), on page 13
- [set csr gen](#), on page 13
- [set cuc jetty stderrlog](#), on page 14
- [set cuc jetty stdoutlog](#), on page 15
- [set cuc jetty requestlog](#), on page 16
- [set cuc speechview registration certificate size](#), on page 16
- [set cuc srsv timeout](#), on page 17
- [set cuc trace](#), on page 17
- [set date](#), on page 18
- [set dscp defaults](#), on page 19
- [set dscp](#), on page 19
- [set dscp marking](#), on page 20
- [set ipsec policy\\_group](#), on page 21
- [set ipsec policy\\_name](#), on page 21
- [set logging](#), on page 22
- [set Login Grace Timeout](#), on page 22
- [set network cluster publisher](#), on page 23
- [set network cluster subscriber details](#), on page 23

- [set network cluster subscriber dynamic-cluster-configuration](#), on page 24
- [set network dhcp eth0](#), on page 24
- [set network dns](#), on page 25
- [set network dns options](#), on page 26
- [set network domain](#), on page 26
- [set network failover](#), on page 27
- [set network gateway](#), on page 27
- [set network hostname](#), on page 28
- [set network ip eth0](#), on page 30
- [set network ipv6 dhcp](#), on page 31
- [set network ipv6 gateway](#), on page 31
- [set network ipv6 service](#), on page 32
- [set network ipv6 static\\_address](#), on page 32
- [set network max\\_ip\\_contrack](#), on page 33
- [set network mtu](#), on page 34
- [set network name-service hosts cache-enable](#), on page 34
- [set network name-service hosts max-db-size](#), on page 35
- [set network name-service hosts negative-time-to-live](#), on page 35
- [set network name-service hosts persistent](#), on page 36
- [set network name-service hosts positive-time-to-live](#), on page 36
- [set network name-service hosts suggested-size](#), on page 37
- [set network name-service services cache-enable](#), on page 37
- [set network name-service services max-db-size](#), on page 37
- [set network name-service services negative-time-to-live](#), on page 38
- [set network name-service services persistent](#), on page 38
- [set network name-service services positive-time-to-live](#), on page 39
- [set network name-service services suggested-size](#), on page 39
- [set network nic eth0](#), on page 40
- [set network ntp option](#), on page 41
- [set network pmtud state](#), on page 41
- [set network restore](#), on page 42
- [set network status eth0](#), on page 43
- [set network name-service](#), on page 43
- [set password complexity minimum-length](#), on page 44
- [set password age](#), on page 44
- [set password change-at-login](#), on page 45
- [set password complexity character](#), on page 46
- [set password complexity character difference](#), on page 47
- [set password complexity character max-repeat](#), on page 47
- [set password expiry maximum-age](#), on page 48
- [set password expiry user maximum-age configure](#), on page 49
- [set password expiry minimum-age](#), on page 49
- [set password expiry user maximum-age](#), on page 50
- [set password expiry user minimum-age](#), on page 51
- [set password history](#), on page 52
- [set password inactivity](#), on page 52

- [set password system bootloader encryptHash](#) , on page 53
- [set password user admin](#), on page 54
- [set password user security](#), on page 54
- [Set replication-sync monitor](#), on page 55
- [set samltrace level](#), on page 55
- [set session maxlimit](#), on page 56
- [set smtp](#), on page 57
- [set strace enable](#), on page 57
- [set strace disable](#), on page 57
- [set timezone](#), on page 58
- [set trace disable](#), on page 59
- [set trace enable](#), on page 59
- [set tlsresumptiontimeout](#), on page 60
- [set tlstrace\\*](#), on page 60
- [set web-security](#), on page 61
- [set webapp session timeout](#), on page 63
- [set workingdir](#), on page 64

## set account enable

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

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

Syntax	Description
<b>Parameters</b>	<b>Description</b>
<i>user-id</i>	Specifies the user ID of the account that was disabled.

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 4

Allowed during upgrade: No

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

## set account name

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

**set account name** *name*

Syntax Description	Parameters	Description
	<i>name</i>	Represents the username for the new account.  Enter a name comprised of only alphabets or characters comprised of alphanumeric characters (a-z, A-D, 0-9).

**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 during installation has a privilege level of 4. The administrator can run all commands in the CLI.

- **'Allow this User to login to SAML SSO-enabled system through the Recovery URL ? (Yes / No)'** — Level 4 administrators can enable or disable the access to the recovery URL sign-in option for new platform administrators by typing **'Yes'** or **'No'** on the CLI. The value can be configured to **'Yes'** if a user chooses to sign-in using the Recovery URL.
- **'To authenticate a platform login for SSO, a Unique Identifier (UID) must be provided that identifies this user to LDAP (such as sAMAccountName or UPN). Please enter the appropriate LDAP Unique Identifier (UID) for this user:[UID]'** — Level 4 administrator can type the unique identifier value for each platform administrator for this prompt.



**Note**

#### Requirements

Command privilege level: 4

Allowed during upgrade: No

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

## set accountlocking

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

**set accountlocking enable | disable**

Syntax Description	Parameters	Description
	<b>enable</b>	Enable account locking.
	<b>disable</b>	Disable account locking.

**Command Modes** Administrator (admin:)

### Usage Guidelines



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

When the Administration account locking feature is enabled, and the user enters the wrong password more than the accountlocking count, the account gets locked for a set period. The message that the account is locked is only seen on the VM console and secure logs.

### Requirements

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

## set accountlocking count

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

**set accountlocking count** *attempts*

Syntax Description	Parameters	Description
	<i>attempts</i>	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

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

## 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
	<i>seconds</i>	Specifies the unlock time in seconds. Value Range: 30-3600 Default value: 300

**Note**

- The account gets automatically unlocked only after the configured unlock time.
- This command is only valid when account locking is enabled. If account locking is disabled, the system does not remember the account locking unlock time and uses the default value, 300, after you enable account locking.

**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

## set cert bulk consolidate

This command consolidates all the certificates that are available on the unit.

**set cert bulk consolidate** *unit*

Syntax Description	Parameters	Description
	<i>unit</i>	Represents the unit name.

**Command Modes** Administrator (admin:)

**Usage Guidelines** You must specify the SFTP server information to use for cert bulk operations.

#### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

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

#### Related Topics

[set cert bulk sftp](#), on page 8

## set cert bulk export

This command exports all the certificates that are available on the unit.

**set cert bulk export** *unit*

Syntax Description	Parameters	Description
	<b>export</b>	Exports all the available certificates for this unit in this cluster to the preconfigured SFTP location.
	<i>unit</i>	Represents the unit name.

**Command Modes** Administrator (admin:)

**Usage Guidelines** You must specify the SFTP server information to use for cert bulk operations.

#### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

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

#### Example

```
admin:set cert bulk export all
Successfully exported tomcat certificate(s) to sftp server.
Successfully exported tftp certificate(s) to sftp server.
```

**Related Topics**

[set cert bulk sftp](#), on page 8

## set cert bulk import

This command imports the certificates that are in the SFTP location into the specified unit trust-store.

**set cert bulk import** *unit*

**Syntax Description**

Parameters	Description
<i>unit</i>	Represents the unit name.

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

You must specify the SFTP server information to use for cert bulk operations.

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

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

**Example**

```
admin:set cert bulk import all
Successfully imported tomcat certificates.
Successfully imported tftp certificates.
```

**Related Topics**

[set cert bulk sftp](#), on page 8

## set cert bulk sftp

This command prompts for the SFTP server information to use for bulk operations.

**set cert bulk sftp**

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

You must specify the SFTP server information to use for cert bulk operations.

**Requirements**

Command privilege level: 1



Allowed during upgrade: Yes

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

## set cert delete

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

**set cert delete** *unit name*

Syntax Description	Parameters	Description
	<i>unit</i>	Specifies the name of the trust category, as “own” or “trust”.
	<i>name</i>	Certificate file name.

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

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

### 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
	<i>type</i>	Specifies the certificate type as “own” or “trust”.
	<i>name</i>	Represents the unit name.
	[ <i>caCert</i> ]	Represents the name of the CA certificate file name.

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

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

**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
	<i>name</i>	Represents the unit name.

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

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

**Example**

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

## set cert regen ITLRecovery

This command regenerates the ITLRecovery certificate for the specified unit.

After you type this command, a warning message appears displaying that if you are using a tokenless CTL and if the you are regenerating the CallManager certificate, ensure that the CTL file has the updated CallManager certificate and that certificate is updated to endpoints. To regenerate the certificate, type **yes** or else type **no**.

**set cert regen** *ITLRecovery*

Syntax Description	Parameters	Description
	<i>ITLRecovery</i>	Represents the ITLRecovery certificate.

**Command Modes** Administrator (admin:)

### Requirements



**Caution** You must restart the services related to ITLRecovery for the regenerated certificates to become active.

Command privilege level: 1

Allowed during upgrade: No

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

### Example

```
admin:set cert regen ITLRecovery
```

```
WARNING: If you are using a tokenless CTL and if the CallManager certificate is recently
generated, please ensure that the CTL File already has the new CallManager certificate and
is
updated to the endpoints, before generating the ITL Recovery certificate. Are you sure want
to proceed?
```

```
Proceed with regeneration (yes|no)? yes
```

```
Successfully Regenerated Certificate for ITLRecovery.
```

```
You must restart the services related to ITLRecovery for the regenerated certificates to
become active.
```

## 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
	<b>on</b>	Turns pagination on.
	<b>off</b>	Turns pagination off.

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

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

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

## set cli session timeout

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

**set cli session timeout** *minutes*

**Syntax Description**

Parameters	Description
<i>minutes</i>	Specifies the time, in minutes, that can elapse before an active CLI session times out and disconnects.
	<ul style="list-style-type: none"> <li>Value range: 5-99999 minutes</li> <li>Default value: 30 minutes</li> </ul>






**Command Modes**

Administrator (admin:)

**Usage Guidelines**

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



**Note**

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

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

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

## set commandcount

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

**set commandcount enable | disable**

Syntax Description	Parameters	Description
	<b>enable</b>	Turns on command count.
	<b>disable</b>	Turns off command count.

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: No

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

## set csr gen

This command generates the csr for the unit name.

**set csr gen name**

Syntax Description	Parameters	Description
	<i>name</i>	Specifies the unit on which the certificate is generated.

**Command Modes** Administrator (admin:)

### Requirements

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

### Example

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

### Requirements

Command privilege level: 1

Allowed during upgrade: No

## set cuc jetty stderrlog

This command enables or disables the error log getting generated while any standard error occurs during communicating with the Jetty server. This error log gets generated and is available at the path `/var/log/active/jetty/`.

**set cuc jetty stderrlog enable | disable**

Syntax Description	Parameters	Description
	<b>enable</b>	Enables the error log on the Jetty server. Be aware that enable is case sensitive.
	<b>disable</b>	Disables the error log on the Jetty server. Be aware that disable is case sensitive.

**Command Modes** Administrator (admin:)

### Usage Guidelines



**Caution**

You must restart the Jetty services after enabling or disabling the error log on the Jetty server.

### Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Cisco Unity Connection only.

### Enable Error Log on Jetty Server Example

```
admin:set cuc jetty stderrlog enable
```

Command is executed successfully

To effect changes restart jetty server

Restart Jetty Server through Unity Connection Servicability .

Go to Tools -> Service Management -> Restart Connection Jetty Service.

Check the logs that should not be generated after running above command.

Check the requestlog by sending one voice message through webinbox.

Notifications should not come in logs

# set cuc jetty stdoutlog

This command enables or disables the standard input and output log getting generated while communicating with Jetty server. This standard input and output log gets generated and is available at the path `/var/log/active/jetty/`.

**set cuc jetty stdoutlog enable | disable**

Syntax Description	Parameters	Description
	<b>enable</b>	Enables the standard input and output log on the Jetty server. Be aware that enable is case sensitive.
	<b>disable</b>	Disables the standard input and output log on the Jetty server. Be aware that disable is case sensitive.

**Command Modes** Administrator (admin:)

## Usage Guidelines



**Caution** You must restart the Jetty services after enabling or disabling the standard input and output log on the Jetty server.

## Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Cisco Unity Connection only.

## Enable Standard Input and Output Log on Jetty Server Example

```
admin:set cuc jetty stdoutlog enable
```

```
Command is executed successfully
To effect changes restart jetty server
Restart Jetty Server through Unity Connection Servicability .
Go to Tools -> Service Management -> Restart Connection Jetty Service.
Check the logs that should not be generated after running above command.
Check the requestlog by sending one voice message through webinbox.
Notifications should not come in logs
```

## set cuc jetty requestlog

This command enables or disables the request log getting generated from the Jetty server while any request is raised for notifications. This request log gets generated and is available at the path `/usr/local/jetty/logs/`.

**set cuc jetty requestlog enable | disable**

Syntax Description	Parameters	Description
	<b>enable</b>	Enables the request log on the Jetty server. Be aware that “enable” is case sensitive.
	<b>disable</b>	Disables the request log on the Jetty server. Be aware that “disable” is case sensitive.

**Command Modes** Administrator (admin:)

### Usage Guidelines



**Caution**

You must restart the Jetty services after enabling or disabling the request log on the Jetty server.

### Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Cisco Unity Connection only.

### Enable Request Log on Jetty Server Example

```
admin:set cuc jetty requestlog enable
```

Command is executed successfully

To effect changes restart jetty server

Restart Jetty Server through Unity Connection Serviciability .

Go to Tools -> Service Management -> Restart Connection Jetty Service.

Check the logs that should not be generated after running above command.

Check the requestlog by sending one voice message through webinbox.

Notifications should not come in logs

## set cuc speechview registration certificate size

This command sets up new certificate bit size for Speech to Text service registration and Voicemail transcription with Nuance server.



**set cuc speechview registration certificate size bit\_size**

Syntax Description	Parameters	Description
	<b>bit_size</b>	Specifies the bit_size of certificate. Its allowed values are 1k, 2k or 4k.

**Command Modes** Administrator (admin:)

**Usage Guidelines** To set the desired certificate bit size, use the **set cuc speechview registration certificate size** (Cisco Unity Connection Only) command. The CLI must be executed on the publisher. It will restart the Connection SpeechView Processor service.

**Requirements**

Command privilege level: 4

## set cuc srsv timeout

This command sets the value for SRSV session timeout.

**set cuc srsv timeout** *timeout\_value*

Syntax Description	Parameters	Description
	<i>timeout_value</i>	Sets the time for session logout.

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Cisco Unity Connection

## set cuc trace

This command enables or disables the specified traces and trace levels.

**set cuc trace** **enable** | **disable** *trace\_name level*

Syntax Description	Parameters	Description
	<b>enable</b>	Enables Connection traces.
	<b>disable</b>	Disables Connection traces.
	<i>trace_name</i>	Specifies the name of the trace to enable or disable. Be aware that trace names are case sensitive.

---

**Parameters Description**


---

*level* Specifies the level or levels of trace\_name that you want to enable or disable. Each trace comprises up to 31 levels, numbered 0 to 30; each level provides a different type of information for the specified trace. When you enable or disable multiple levels, use a comma to separate levels and a hyphen to indicate a range of levels. Do not include spaces.

---

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

To display a list of the traces and trace levels that are currently enabled, use the **show cuc trace levels** (Cisco Unity Connection Only) command.

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Cisco Unity Connection only.

**Enable VUI Traces 1, 13, and 17 Through 20 Example**

```
admin:set cuc trace enable VUI 1,13,17-20
VUI trace levels are now set to: 1,13,17-20
```

**Disable VUI Traces 17 Through 20 While VUI Trace Levels 1 and 13 Remain Set Example**

```
admin:set cuc trace disable VUI 17-20
VUI trace levels are now set to: 1,13
```

**Related Topics**

[show cuc trace levels](#)

# 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**

Applies to: Unified Communications Manager and Cisco Unity Connection.

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

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

**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.

**set dscp defaults****Command Modes**

Administrator (admin:)

**Usage Guidelines**

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

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

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

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

## set dscp

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

```
set dscp enable | disableallport_tag
```

**Syntax Description****Parameters Description**

Parameters	Description
<b>all</b>	Disables all DSCP port tags.

Parameters	Description
<i>port_tag</i>	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 <b>show dscp defaults</b> . The set of port tags is predefined.

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

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

## set dscp marking

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

**set dscp marking** *port\_tag value***Syntax Description**

Parameters	Description
<i>port_tag</i>	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 <b>show dscp defaults</b> . The set of port tags is predefined.
<i>value</i>	A DSCP value. You can enter the name of a well-known DSCP class or a numeric value in decimal or hexadecimal format. Precede hexadecimal values with 0x or 0X.

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

The valid class names as defined by DSCP are:

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

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

- Expedited Forwarding: value EF

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

- Best Effort: value BE

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

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

There are four types of Assured Forwarding classes, each of which has three drop precedence values.

These precedence values define the order in which a packet is dropped (if needed) due to network congestion. For example, packets in AF13 class are dropped before packets in the AF12 class.

### Requirements

Command privilege level: 1

Allowed during upgrade: No

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

## set ipsec policy\_group

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

**set ipsec policy\_group** *ALLgroup*

Syntax Description	Parameters	Description
	<b>ALL</b>	Enables all ipsec policy groups.
	<i>group</i>	Specifies the name of a particular ipsec policy group to enable.

### Command Modes

Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager and Cisco Unity Connection.

## set ipsec policy\_name

This command enables the specified ipsec policy.

**set ipsec policy\_name** *ALLpolicy\_name*

Syntax Description	Parameters	Description
	<b>ALL</b>	Enables all ipsec policies.
	<i>policy_name</i>	Specifies the name of a particular ipsec policy to enable.

### Command Modes

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager and Cisco Unity Connection.

## set logging

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

**set logging enable | disable**

Syntax Description	Parameters	Description
	<b>enable</b>	Turns on logging.
	<b>disable</b>	Turns off logging.

**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, and Cisco Unity Connection.

## set Login Grace Timeout

This command allows you to configure the LoginGraceTimeout value to the mentioned value.

**set Login Grace Timeout** *LoginGraceTimeout value*

Syntax Description	Parameters	Description
	<i>LoginGraceTimeout value</i>	Sets the LoginGraceTimeout value for login grace timeout.

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

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

## set network cluster publisher

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

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

Syntax Description	Parameters	Description
	<b>hostname</b>	Specifies the hostname of the network cluster.
	<b>ip</b>	Specifies the ip address of the network cluster.
	<i>name</i>	Hostname or IP address to assign to the network cluster publisher.

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

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

## set network cluster subscriber details

Use this command to add subscriber to the processnode or appserver table when Tomcat Webserver is server down and GUI is inaccessible.

**set network cluster subscriber details** *servertype hostname ip domainname*

Syntax Description	Parameter	Description
	<i>servertype</i>	Choose one of these products for this parameter— Unified Communications Manager, IM and Presence Service, and Cisco Unity Connection. This field is mandatory.
	<i>hostname</i>	The hostname of the node that you add to the cluster. The hostname is supported on the same domain. This field is mandatory.
	<i>ip</i>	The IPv4 address of the node that you add to the cluster. This field is mandatory for IM and Presence publisher and Cisco Unity Connection.

Parameter	Description
<i>domainname</i>	The domain name of the IM and Presence Service publisher. This field is mandatory for IM and Presence publisher.

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

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

## set network cluster subscriber dynamic-cluster-configuration

Use this command to enable the Dynamic Cluster Configuration on the publisher. Use this command to specify the duration in which you can add subscriber nodes to the publisher server table. The addition of subscriber nodes is authenticated immediately and those nodes need not wait for the publisher details during the installation of the subscriber nodes.

**set network cluster subscriber dynamic-cluster-configuration default | no. of hours**

**Syntax Description**

Parameter	Description
<b>default</b>	Enables the Dynamic Cluster Configuration for 24 hours.
<b>no. of hours</b>	Specifies a value from 1 to 24 hours.

**Command Modes**

Administrator (admin)

**Requirements**

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

## set network dhcp eth0

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

**set network dhcp eth0 enable | disable node\_ipnet\_maskgateway\_ip**

**Syntax Description**

Parameters	Description
<b>eth0</b>	Specifies Ethernet interface 0.
<b>enable</b>	This enables DHCP.



Parameters	Description
<b>disable</b>	This disables DHCP.
<i>node_ip</i>	Represents the static IP address for the server.
<i>net_mask</i>	Represents the subnet mask for the server.
<i>gateway_ip</i>	Represents the IP address of the default gateway.

**Command Modes** Administrator (admin:)

### Usage Guidelines



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

### Requirements

Command privilege level: 1

Allowed during upgrade: No

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

## set network dns

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

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

Syntax Description	Parameters	Description
	<b>primary</b>	
	<b>secondary</b>	
	<i>addr</i>	Represents the IP address of the primary or secondary DNS server.

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: No

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

## set network dns options

This command sets DNS options.

```
set network dns options [timeoutseconds] [attemptsnumber] [rotate]
```

### Syntax Description

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

### Command Modes

Administrator (admin:)

#### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

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

## set network domain

This command sets the domain name for the system.



**Note** Changing the domain name triggers an automatic regeneration of all 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
	<i>domain_name</i>	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

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

## set network failover

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

**set network failover** *ena* | *dis*

Syntax Description	Parameters	Description
	<b>ena</b>	Enables Network Fault Tolerance.
	<b>dis</b>	Disables Network Fault Tolerance.

**Command Modes** Administrator (admin:)

#### Requirements

Command privilege level: 1

Allowed during upgrade: No

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

## set network gateway

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

**set network gateway** *addr*

Syntax Description	Parameters	Description
	<i>addr</i>	Represents the IP address of the network gateway that you want to assign.

**Command Modes** Administrator (admin:)

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



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

### Requirements

Command privilege level: 1

Allowed during upgrade: No

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

## 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
	<i>hostname</i>	Represents the new network hostname of the system.
	<b>Note</b>	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

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

### 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
	<b>eth0</b>	Specifies Ethernet interface 0.
	<i>addr</i>	Represents the IP address that you want to assign.
	<i>mask</i>	Represents the IP mask that you want to assign.
	<i>gw</i>	Represents the IP default gw that you want to assign.

**Command Modes** Administrator (admin:)

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



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

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

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

## set network ipv6 dhcp

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

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

Syntax Description	Parameters	Description
	<b>dhcp</b>	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.
	<b>enable</b>	Enables IPv6 support.
	<b>disable</b>	Disables IPv6 support.
	<b>reboot</b>	(Optional) Causes the server to automatically restart after you enter the command.

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified 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
	<b>gateway</b>	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.
	<b>addr</b>	The IPv6 gateway address.

Parameters	Description
<b>reboot</b>	(Optional) Causes the server to automatically restart after you enter the command.

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified 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
<b>service</b>	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.
<i>enable</i>	Enables IPv6 service on the server.
<i>disable</i>	Disables IPv6 service on the server.
<b>reboot</b>	(Optional) Causes the server to automatically restart after you enter the command.

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified 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
	<b>static_address</b>	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.
	<i>addr</i>	Specifies the static IPv6 address you assign to the server.
	<i>mask</i>	Specifies the IPv6 network mask (0-128).
	<b>reboot</b>	(Optional) Causes the server to automatically restart after you enter the command.

**Command Modes** Administrator (admin:)

#### Requirements

Command privilege level: 1

Allowed during upgrade: No

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

## set network max\_ip\_contrack

This command sets the ip\_contrack\_max value.

**set network max\_ip\_contrack** *ip\_contrack\_max value*

Syntax Description	Parameters	Description
	<i>ip_contrack_max value</i>	Specifies the value for ip_contrack_max.
	<b>Note</b>	The value of ip_contrack_max cannot be less than 65536.

**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, and Cisco Unity Connection.

#### Example

```
admin:set network max_ip_contrack 65536
```

## set network mtu

This command sets the maximum MTU value.

**set network mtu** *mtu\_max*

Syntax Description	Parameters	Description
	<i>mtu_max</i>	Specifies the maximum MTU value. The system default MTU value equals 1500.
	<b>Caution</b>	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

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

### Example

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

## set network name-service hosts cache-enable

This command enables the nsd related cache.

**set network name-service hosts cache-enable** *value*

Syntax Description	Parameters	Description
	<i>value</i>	The boolean value must be either <i>yes</i> or <i>no</i> .

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

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

## set network name-service hosts max-db-size

This command sets the maximum allowed size for a service.

**set network name-service hosts max-db-size** *value***Syntax Description**

Parameters	Description
<i>value</i>	Enter the number of bytes for the database size.

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

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

## set network name-service hosts negative-time-to-live

This command sets the time-to-live (TTL) for negative entries or unsuccessful queries in the specified cache for service. So, using this command improves the performance if there are various files owned by user IDs (UIDs) and are unavailable in system databases. For example, files that are available in the Linux kernel sources as root. To reduce the cache coherency problems, the number of such files should be kept to the minimum.

**set network name-service hosts negative-time-to-live** *value***Syntax Description**

Parameters	Description
<i>value</i>	Enter the number of seconds.

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

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

## set network name-service hosts persistent

This command retains the content of the cache for service over server restarts. This command is useful when *paranoia* mode is configured.

**set network name-service hosts persistent** *value*

Syntax Description	Parameters	Description
	<i>value</i>	Enter a value for a service.

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

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

## set network name-service hosts positive-time-to-live

This command sets the time-to-live (TTL) for positive entries or successful queries in the specified cache for service. Configure the value in seconds. Larger values increase cache hit rates and reduce mean response times. However, such values increase problems with cache coherence.

**set network name-service hosts positive-time-to-live** *value*

Syntax Description	Parameters	Description
	<i>value</i>	Enter the number of seconds.

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

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

## set network name-service hosts suggested-size

This command changes the internal hash table size.

**set network name-service hosts suggested-size** *value*

Syntax Description	Parameters	Description
	<i>value</i>	Enter a prime number for optimum efficiency.

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

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

## set network name-service services cache-enable

This command enables the nscd related cache.

**set network name-service services cache-enable** *value*

Syntax Description	Parameters	Description
	<i>value</i>	The boolean value must be either <i>yes</i> or <i>no</i> .

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

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

## set network name-service services max-db-size

This command sets the maximum allowed size for the service.

**set network name-service services max-db-size** *value*

Syntax Description	Parameters	Description
	<i>value</i>	Enter the value in number of bytes.

**Command Modes** Administrator (admin:)

#### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

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

## set network name-service services negative-time-to-live

This command sets the time-to-live (TTL) for negative entries or unsuccessful queries in the specified cache for service. So, using this command improves the performance if there are various files owned by user IDs (UIDs) and are unavailable in system databases. For example, files that are available in the Linux kernel sources as root. To reduce the cache coherency problems, the number of such files should be kept to the minimum.

**set network name-service services negative-time-to-live** *value*

Syntax Description	Parameters	Description
	<i>value</i>	Enter a prime number for optimum efficiency.

**Command Modes** Administrator (admin:)

#### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

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

## set network name-service services persistent

This command retains the content of the cache for service over server restarts. This command is useful when *paranoia* mode is configured.

**set network name-service services persistent** *value*

Syntax Description	Parameters	Description
	<i>value</i>	Enter a value for a service.

**Command Modes** Administrator (admin:)

#### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

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

## set network name-service services positive-time-to-live

This command sets the time-to-live (TTL) for positive entries or successful queries in the specified cache for service. If you enter a large value for this command, it increases cache hit rates and reduces mean response times. However, a large value increases issues with cache coherence.

**set network name-service services positive-time-to-live** *value*

Syntax Description	Parameters	Description
	<i>value</i>	Enter the number of seconds.

**Command Modes** Administrator (admin:)

#### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

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

## set network name-service services suggested-size

This command sets the internal hash table size.

**set network name-service services suggested-size** *value*

Syntax Description	Parameters	Description
	<i>value</i>	Enter a prime number for optimum efficiency.

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

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

## 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
	<b>eth0</b>	Specifies Ethernet interface 0.
	<b>auto</b>	Specifies whether auto negotiation gets enabled or disabled.
	<b>speed</b>	Specifies whether the speed of the Ethernet connection: 10 or 100 Mb/s.
	<b>duplex</b>	Specifies half-duplex or full-duplex.

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

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

**Note**

You can enable only one active NIC at a time.

**Caution**

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

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

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



## set network ntp option

This command adds the *noquery* option to the `/etc/config` file.

**set network ntp option**

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

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

## set network pmtud state

This command enables and disables Path MTU Discovery.

**set network pmtud state enable | disable**

Syntax Description	Parameters	Description
	<b>enable</b>	Enables Path MTU Discovery.
	<b>disable</b>	Disables Path MTU Discovery.

**Command Modes** Administrator (admin:)

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



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

### Requirements

Command privilege level: 1

Allowed during upgrade: No

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

### 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
	<b>eth0</b>	Specifies Ethernet interface 0.
	<i>ip-address</i>	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 <b>utils service</b> command. We also recommend that you restart all nodes whenever any IP address gets changed.
	<i>network-mask</i>	Represents the subnet mask for the server.
	<i>gateway</i>	Specifies the IP address of the default gateway.
	<i>ip-address</i>	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 <b>utils service</b> command. We also recommend that you restart all nodes whenever any IP address gets changed.

**Command Modes** Administrator (admin:)

### Usage Guidelines



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



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

### Requirements

Command privilege level: 0

Allowed during upgrade: Yes

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

### Example

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

## set network status eth0

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

**set network status eth0 up | down**

Syntax Description	Parameters	Description
	<b>eth0</b>	Specifies Ethernet interface 0.
	<b>up</b>	Sets the status of Ethernet interface 0 to up.
	<b>down</b>	Sets the status of Ethernet interface 0 to down.

**Command Modes** Administrator (admin:)

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



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

### Requirements

Command privilege level: 1

Allowed during upgrade: No

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

## set network name-service

This command displays name service cache attributes.

**set network name-service [attribute] [value]**

Syntax Description	Attribute	Value
	<b>Paranoia</b>	Bool must be either Yes or No. Enabling paranoia mode causes Name Service to restart itself periodically.

Attribute	Value
<b>debug-level</b>	If level is higher than 0, Name Service will create some debug output. Higher the level, more verbose the output.
<b>reload-count</b>	Sets the number of times a cached record is reloaded before it is pruned from the cache. Each cache record has a timeout. When that timeout expires Name Service will either reload it (query the NSS service again if the data hasn't changed) or drop it.
<b>restart-interval</b>	Sets the restart interval to time seconds if periodic restart is enabled by enabling paranoia mode. The default value is 3600.

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

## set password complexity minimum-length

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

**Note**

Use this command after you enable the character complexity of passwords.

**set password complexity minimum-length** *max-repeat*

**Syntax Description**

Parameters	Description
<i>value</i>	Enter a value of or greater than 6.

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

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

## 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
	<b>maximum</b>	Specifies the maximum age.
	<b>minimum</b>	Specifies the minimum age.
	<i>days</i>	Specifies the maximum password age and must be greater-than or equal-to 90 days.

**Command Modes** Administrator (admin:)

#### Requirements

Command privilege level: 1

Allowed during upgrade: No

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

## set password change-at-login

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

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

Syntax Description	Parameters	Description
	<b>disable</b>	This does not force users to change their password.
	<b>enable</b>	This forces users to change their password when they sign in to the system the next time.
	<i>userid</i>	Specifies the affected user account.

**Command Modes** Administrator (admin:)

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

#### Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: IM and Presence service on Unified Communications Manager only.

# set password complexity character

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



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

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

## Syntax Description

Parameters	Description
<b>disable</b>	This turns off password complexity for character types.
<b>enable</b>	This turns on password complexity for character types.
<b>Note</b>	When you disable password complexity, you also turn off <b>password character difference</b> , <b>password character max-repeat</b> , and <b>password history</b> .
<i>num-char</i>	This specifies the number of characters required from each of the four character sets: lowercase, uppercase, numbers, and special characters. <ul style="list-style-type: none"> <li>• Value range: 0-8</li> <li>• Default value: 1</li> </ul>

## Command Modes

Administrator (admin:)

## Usage Guidelines

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

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

## Requirements

Command privilege level: 1

Allowed during upgrade: No

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

## 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

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

## set password complexity character max-repeat

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

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

### Syntax Description

#### Parameters Description

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

- Value range: 0 – 10

Default value: 0

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

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

## set password expiry maximum-age

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

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

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

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

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



**Example**

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

## set password expiry user maximum-age configure

This command modifies the value of the maximum password age for a particular Cisco Collaboration Communication OS Administration account in days.

**set password expiry user maximum-age configure** *userid* *maximum password age*

Syntax Description	Parameters	Description
	<i>userid</i>	Enter Cisco Collaboration Communication OS (C3OS) Administrator account.
	<i>maximum password age</i>	Enter the maximum password age in days. This value must be equal to or greater than 10 days but less than 3650 days (10 years).

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

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

## 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
	<b>enable</b>	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.
	<b>disable</b>	Turns off password expiry minimum age settings for Cisco Unified Operating System administrator accounts. This means that passwords for administrator accounts can be changed at any interval.

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

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

**Example**

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

## set password expiry user maximum-age

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

```
set password expiry user maximum-age enable | disable userid
```

Syntax Description	Parameters	Description
	<b>enable</b>	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
<b>disable</b>	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.
<i>userid</i>	Specifies a particular Cisco Unified Operating System Administrator account.

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

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

**Example**

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

## set password expiry user minimum-age

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

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

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

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

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

**Example**

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

## set password history

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

**set password history** *number*

**Syntax Description****Parameters Description**

*number* Specifies the mandatory number of passwords to maintain in history.

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

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

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

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

## set password inactivity

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

**Syntax Description****Parameters Description**

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

Parameters	Description
<b>disable</b>	Disable the password inactivity globally and update individual OS users according to the setting.
<b>period</b>	Configure the password inactivity period globally and update individual OS users according to the setting.
<i>days</i>	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: 0

Allowed during upgrade: No

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

## set password system bootloader encryptHash

Use this command to configure the encrypted password in the `grub.conf` file for the system boot loader.

### set password system bootloader encryptHash

### Command Modes

Administrator (admin:)

### Requirements

Command privilege level: 4

Allowed during upgrade: No

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

## set password user admin

This command allows you to change the administrator password.

**set password user admin**

---

### Command Modes

Administrator (admin:)

---

### Usage Guidelines

The systems prompts you for the old and new passwords.



#### Note

- You can change the password only for the administrator account that you logged in to.
- The password must contain at least six characters, and the system checks it for strength.

---

### Requirements

Command privilege level: 1

Allowed during upgrade: No

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

## set password user security

This command allows you to change the security password.

**set password user security**

---

### Command Modes

Administrator (admin:)

---

### Usage Guidelines

The systems prompts you for the old and new passwords.



#### Note

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



#### Note

Before running the `set user password security` command on the IM and Presence Service servers (nodes), you must first go to the **Cisco Unified CM IM and Presence Administration > System > CUCM Publisher** window for each IM and Presence Service server (node), and enter the new security password.

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

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

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




---

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

---




---

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

---

### Requirements

Command privilege level: 1

Allowed during upgrade: No

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

## Set replication-sync monitor

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

**set replication-sync monitor {enable | disable}**

Syntax Description	Parameters	Description
	<b>enable</b>	Turns on the replication monitoring service.
	<b>disable</b>	Turns off the replication monitoring service

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: IM and Presence service on Unified Communications Manager only

## set samltrace level

This command sets the SAML trace level.

**set samltrace level** *trace level*

---

**Syntax Description**


---

**Parameters Description**

*trace level* Specifies the trace level. The available options are:

- DEBUG
- INFO
- WARNING
- ERROR
- FATAL

**Note** The default trace level is INFO.

---



---

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

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

## set session maxlimit

This command sets the upper limit for concurrent sessions.

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

---

**Syntax Description**


---

**Parameters Description**

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

*value* Acceptable values are 1 - 100.

---



---

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

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



## set smtp

This command sets the SMTP server hostname.

```
set smtp hostname
```

---

### Syntax Description

Parameters	Description
<i>hostname</i>	Represents the SMTP server name.

---

### 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, and Cisco Unity Connection.

## set strace enable

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

```
set strace enable [all]tracevalue servicename
```

---

### Syntax Description

Parameters	Description
<i>all</i>	Optional parameter to propagate the service trace settings change to all nodes.
<i>tracevalue</i>	Represents allowed trace values. Allowed trace values are [Info Debug Warn Error Fatal]
<i>servicename</i>	Represents the service for which the trace is enabled.

---

### Command Modes

Administrator (admin:)

#### Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: IM and Presence service on Unified Communications Manager

## set strace disable

This command disables the service trace.

```
set strace disable [all] servicename
```

**Syntax Description****Parameters Description**

Parameters	Description
<i>all</i>	Optional parameter to propagate the service trace settings change to all nodes.
<i>servicename</i>	Represents the service for which the trace is enabled.

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 0

Allowed during upgrade: No

Applies to: IM and Presence service on Unified Communications Manager

## set timezone

This command lets you change the system timezone.

```
set timezone zone
```

**Syntax Description****Parameters Description**

Parameters	Description
<i>zone</i>	Specifies the new timezone. Enter the appropriate string or zone index id to uniquely identify the timezone. To view a list of valid timezones, use the CLI command: <b>show timezone list</b> .

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

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

**Caution**

You must restart the system after you change the timezone.

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

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

**Example Setting Timezone to Pacific Time**

```
admin:set timezone Pac
```

## set trace disable

This command unsets trace activity for the specified task.

**set trace disable** *tname*

Syntax Description	Parameters	Description
	<b>disable</b>	Unsets the task trace settings.
	<i>tname</i>	Represents the task for which you want to disable traces.

**Command Modes** Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: No

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

## set trace enable

This command sets trace activity for the specified task.

**set trace enable** **Arbitrary** | **Detailed** | **Entry\_exit** | **Error** | **Significant** | **Special** | **State\_Transition** *tname*

Syntax Description	Parameters	Description
	<b>Arbitrary</b>	Sets task trace settings to the arbitrary level.
	<b>Detailed</b>	Sets task trace settings to the detailed level.
	<b>Entry_exit</b>	Sets task trace settings to the entry_exit level.
	<b>Error</b>	Sets task trace settings to the error level.
	<b>Significant</b>	Sets task trace settings to the significant level.
	<b>Special</b>	Sets task trace settings to the special level.
	<b>State_transition</b>	Sets task trace settings to the state transition level.
	<i>tname</i>	Represents the task for which you want to disable traces.

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

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

## set tlsresumptiontimeout

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

**set tlsresumptiontimeout** *seconds*

Syntax Description	Parameters	Description
	<i>seconds</i>	Enter a value up to 3600 seconds. The TLS sessions are invalid after the configured value.

**Command Modes** Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

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

## set tlstrace\*

Unified Communications Manager Release 11.0 onwards, you can enable or disable TLS tracing for services. Currently, Tomcat is the only supported service. Use the CLI commands to view the reasons of connection failure of TLS connections to Unified Communications Manager.

Following TLS-based CLI commands are added for TLS tracing:

## set tlstrace disable

This CLI command disables the TLS tracing for a service.

**set tlstrace disable** *service*

Syntax Description	Parameters	Description
	<i>service</i>	Specifies the service that you use to disable TLS tracing.

**Command Modes** Administrator (admin:)

**Example**

```
admin:set tlstrace disable tomcat
TLS tracing is disabled for: tomcat
```

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

## set tlstrace enable

This CLI command enables the TLS tracing for a service.

```
set tlstrace enable service
```

**Syntax Description****Parameters Description**

Parameters	Description
<i>service</i>	Specifies the service that you use to enable TLS tracing.

**Command Modes**

Administrator (admin:)

**Example**

```
admin:set tlstrace enable tomcat
TLS tracing is enabled for: tomcat
```

**Requirements**

Command privilege level: 1

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
	<i>orgunit</i>	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.  <b>Note</b> For OU's that already contains a backslash, do not enter one more backslash as SLM registration and CSR generation fails during the time of installation.
	<i>orgname</i>	Represents the organizational name.
	<i>locality</i>	Represents the organization location.
	<i>state</i>	Represents the organization state.
	<i>country</i>	(Optional) Represents the organization country.
	<i>alternatehostname</i>	(Optional) Specifies an alternate name for the host when you generate a web-server (Tomcat) certificate.  You can use <i>alternatehostname</i> to set subject alternate hostname for self signed certificates. Subject alternate hostname for CSR is defined in the Certificate Management page. If you have set the alternate hostname for CSR using this command, the CSR generation process replaces the set alternate hostname.



**Note** The set web-security command when adding in the alternate hostname will apply and will be added to all future generated CSR's including, Tomcat, CallManager, CAPF, TVS, and IPsec.

#### Command Modes

Administrator (admin:)

#### Usage Guidelines

In case you are planning to rebuild the Unified CM server, ensure that you should use the same OU subject parameters. Else, this will create discrepancies when you execute the command **show web-security**. This is because the platformConfig.xml file will not have the saved parameters information provided before the rebuild as this file is not backed up during DRS backup.

#### Requirements

Command privilege level: 0

Allowed during upgrade: No

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

#### Example

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

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

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

## set webapp session timeout

This command sets the time, in minutes, that can elapse before a web application, such as 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
<i>minutes</i>	Specifies the time, in minutes, that can elapse before a web application times out and logs off the user. <ul style="list-style-type: none"> <li>• Value range: 5-99999 minutes</li> <li>• Default value: 30 minutes</li> </ul>

### Command Modes

Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: No

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

# set workingdir

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

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

## Syntax Description

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

## Command Modes

Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: Yes

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