



CHAPTER 6

Set Commands

Revised: October 26, 2010, OL-23878-01

This chapter contains the following **set** commands:

- [set account](#)
- [set accountlocking](#)
- [set cli pagination](#)
- [set commandcount](#)
- [set logging](#)
- [set network dhcp](#)
- [set network dns](#)
- [set network dns options](#)
- [set network domain](#)
- [set network failover](#)
- [set network gateway](#)
- [set network hostname](#)
- [set network ip](#)
- [set network mtu](#)
- [set network max_ip_conntrack](#)
- [set network mtu](#)
- [set network nic](#)
- [set network pmtud](#)
- [set network restore](#)
- [set network status](#)
- [set password maximum age](#)
- [set password minimum age](#)
- [set password complexity character](#)
- [set password complexity minimum-length](#)
- [set password expiry maximum-age](#)

- `set password expiry minimum-age`
- `set password history`
- `set password inactivity`
- `set password user admin`
- `set snmp trapdest add`
- `set snmp trapdest del`
- `set snmp user add`
- `set snmp user del`
- `set syslog facility`
- `set syslog heartbeat facility`
- `set syslog heartbeat interval`
- `set syslog heartbeat msg`
- `set syslog timezone`
- `set syslog version`
- `set web-security`
- `set workingdir`

set account

set account *name*

Syntax Description

<i>name</i>	Represents the username for the new account.
-------------	--

Command Modes

Admin
Command privilege level: 0
Allowed during upgrade: No

Command History

Release	Modifications
1.2	This command was first introduced.

Usage Guidelines

This command sets up a new account on the operating system. After you enter the username, the system prompts you to enter the privilege level and password for the new account.

Examples

admin:**set account**

set accountlocking

set accountlocking {enable | disable}

Options

- **enable** enables accountlocking.
- **disable** disables accountlocking.

Syntax Description

None.

Command Modes

Admin

Command privilege level: 0

Allowed during upgrade: No

Command History

Release	Modifications
1.7	This command was first introduced.

Usage Guidelines

This command enables or disables locking on admin accounts if three consecutive unsuccessful login attempts are made.

After login account is locked, user will need to wait for at least 5 mins before the account gets unlocked.

Examples

admin:**set accountlocking enable**

set cli pagination

set cli pagination {on | off}

Options

- **on** turns on cli pagination for the current CLI session.
- **off** turns off cli pagination for the current CLI session.

Syntax Description

None.

Command Modes

Admin

Command privilege level: 0

Allowed during upgrade: No

Command History

Release	Modifications
1.7	This command was first introduced.

Usage Guidelines

This command is used to turn automatic pagination ON or OFF, for the current CLI session.

Use the **show cli pagination** command to see the status of the automatic pagination.

Examples

admin:**set cli pagination on**

set commandcount

set commandcount {enable | disable}

Options

- **enable** enables commandcount.
- **disable** disables commandcount.

Command Modes

Admin

Command privilege level: 1

Allowed during upgrade: No

Command History

Release	Modifications
1.2	This command was first introduced.

Usage Guidelines

This command changes the CLI command prompt to display how many CLI commands have been executed.

Examples

```
admin:set commandcount enable
```

set logging

set logging {enable | disable}

Options

- **enable** enables logging.
- **disable** disables logging.

Syntax Description

None

Command Modes

Admin

Command privilege level: 0

Allowed during upgrade: No

Command History

Release	Modifications
1.2	This command was first documented.

Usage Guidelines

This command allows you to enable or disable logging.

Examples

admin:**set logging disable**

set network dhcp

set network dhcp eth0

enable

disable *node_ip net_mask gateway_ip*

Options

- **eth0** specifies Ethernet interface 0.
- **enable** enables DHCP.
- **disable** disables DHCP.

Syntax Description

<i>node_ip</i>	Represents the new 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

Admin

Command privilege level: 1

Allowed during upgrade: No

Command History

Release	Modification
1.2	This command was first documented.

Usage Guidelines

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

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



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.

Examples

```
admin:set network dhcp eth0 enable
```


set network dns

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

Options

- **primary** specifies the primary DNS server.
- **secondary** specifies the secondary DNS server.

Syntax Description

<i>ip-address</i>	Represents the IP address of the primary or secondary DNS server.
-------------------	---

Command Modes

Admin
Command privilege level: 1
Allowed during upgrade: No

Command History

Release	Modifications
1.2	This command was first documented.

Usage Guidelines

This command sets the IP address for the primary or secondary DNS server.
The system asks whether you want to continue to execute this command.



Note

If you change the IP address for the primary DNS server, you must also restart the Cisco Web server service. For more information, refer to the [utils service](#) command.



Caution

Running this command causes a temporary loss of network connectivity. If you change the IP address of the DNS server, you must restart Cisco Web server. For more information, see [utils service, page 9-17](#).

Examples

admin:**set network dns primary**

set network dns options

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

Syntax Description

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

Command Modes

Admin
 Command privilege level: 0
 Allowed during upgrade: Yes

Command History

Release	Modifications
1.2	This command was first documented.

Usage Guidelines

This command sets DNS options.
 .

Examples

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

set network domain

set network domain *domain-name*

Syntax Description

<i>domain-name</i>	Represents the system domain that you want to assign.
--------------------	---

Command Modes

Admin
 Command privilege level: 1
 Allowed during upgrade: No

Command History

Release	Modifications
1.2	This command was first documented.

Usage Guidelines

This command sets the domain name for the system.



Caution

Running this command causes a temporary loss of network connectivity.

Examples

```
admin:set network domain cisco.com
***  W A R N I N G  ***
Adding, deleting, or changing domain information on this server
will break communication with other servers using DNS
(ex. Unified CM, CTMS, CTRS and CTS-MAN). After domain modification is
completed and matches on each of the servers,
please reboot each to ensure they continue to work together.

Continue (y/n)?y
Warning: Restart could take up to 5 minutes...
Shutting down Service Manager will take some time..
```

set network failover

failover {enable | disable}

Syntax Description

enable	Enables Network Fault Tolerance.
disable	Disables Network Fault Tolerance.

Command Modes

Admin
Command privilege level: 1
Allowed during upgrade: No

Command History

Release	Modifications
1.2	This command was first documented.

Usage Guidelines

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

Examples

```
admin:failover disable
```

set network gateway

set network gateway *ip-address*

Syntax Description	<i>ip-address</i>	Represents the IP address of the network gateway that you want to assign.				
Command Modes	Admin Command privilege level: 1 Allowed during upgrade: No					
Command History	<table><tr><th>Release</th><th>Modifications</th></tr><tr><td>1.2</td><td>This command was first documented.</td></tr></table>	Release	Modifications	1.2	This command was first documented.	
Release	Modifications					
1.2	This command was first documented.					
Usage Guidelines	This command enables you to configure the IP address of the network gateway.					
 Caution	Running this command causes the system to restart.					
Examples	admin: set network gateway 168.10.22.1					

set network hostname

set network hostname *my-name*

Syntax Description

<i>my-name</i>	Represents the new hostname that you want to set for CTS-Manager.
----------------	---

Command Modes

Admin
 Command privilege level: 1
 Allowed during upgrade: No

Command History

Release	Modifications
1.7	This command was first documented.

Usage Guidelines

This command allows you to set the network hostname for CTS-Manager.

The hostname must follow the rules for ARPANET host names. The hostname must start with an alphabetic character and end with an alphanumeric character, and may contain any alphanumeric characters or hyphens in between. The hostname must be 63 characters or less.



Caution

Running this command causes CTS-Manager to restart.

Examples

admin: **set network hostname ctsman1**

set network ip

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

Syntax Description

eth0	Specifies Ethernet interface 0.
<i>ip-address</i>	Represents the IP address that you want to assign
<i>ip-mask</i>	Represents the IP mask that you want to assign.

Command Modes

Admin
Command privilege level: 1
Allowed during upgrade: No

Command History

Release	Modifications
1.2	This command was first documented.

Usage Guidelines

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



Caution

Executing this command causes CTS-Manager to restart.

Examples

```
admin:set network ip eth0 192.168.10.12 255.255.255.0
```

set network max_ip_conntrack

set network max_ip_conntrack *ip_conntrack_max*

Syntax Description	<i>ip_conntrack_max</i>	Specifies the value for ip_conntrack_max.
---------------------------	-------------------------	---

Command Modes	Admin Command privilege level: 1 Allowed during upgrade: No
----------------------	---

Command History	<table><tr><th>Release</th><th>Modifications</th></tr><tr><td>1.2</td><td>This command was first documented.</td></tr></table>	Release	Modifications	1.2	This command was first documented.
Release	Modifications				
1.2	This command was first documented.				

Usage Guidelines	This command sets the ip_conntrack_max value. The value must be an integer and cannot be less than 65536.
-------------------------	--

Examples	admin: set network max_ip_conntrack 256000
-----------------	---

set network mtu

set network mtu *mtu_max*

Syntax Description

<i>mtu_max</i>	Specifies the maximum MTU value.
----------------	----------------------------------

Command Modes

Admin
Command privilege level: 1
Allowed during upgrade: No

Command History

Release	Modifications
1.2	This command was first documented.

Usage Guidelines

This command sets the maximum MTU value.



Note

The system default MTU value equals 1500.



Caution

Executing this command will cause CTS-Manager to temporarily lose network connectivity.

Examples

```
admin:set network mtu 576
*** WARNING ***
This will cause the system to temporarily lose network connectivity

Do you want to continue ?

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

yes
executing...
```

set network nic

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

Syntax Description

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

Command Modes

Admin
 Command privilege level: 1
 Allowed during upgrade: No

Command History

Command	Modifications
1.2	This command was first documented.

Usage Guidelines

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



Note

You can enable only one active NIC at a time.



Caution

Executing this command will cause CTS-Manager to temporarily lose network connectivity while the NIC is reset.

Examples

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

set network pmtud

set network pmtud [enable | disable]

Syntax Description

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

Command Modes

Admin
Command privilege level: 1
Allowed during upgrade: No

Command History

Release	Modifications
1.2	This command was first documented.

Usage Guidelines

This command enables and disables Path MTU Discovery.



Caution

Executing this command will cause CTS-Manager to temporarily lose network connectivity.

Examples

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

Do you want to continue ?

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

set network restore

set network restore eth0 ip address

Syntax Description

<i>ip address</i>	Defines value for static IP address.
-------------------	--------------------------------------

Command Modes

Admin
 Command privilege level: 1
 Allowed during upgrade: No

Command History

Release	Modifications
1.2	This command was first documented.

Usage Guidelines

This command configures the specified Ethernet port with a static IP address. A temporary loss of network connectivity will occur while the network is being restarted with the new configuration.

It's important to configure the original Ethernet port settings AFTER executing this command by using the other CLI **set network** commands.



Caution

Executing this command will cause CTS-Manager to restart.

Examples

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

```
*** WARNING ***
```

Only use this command in the event that all other CLI 'set network ...' commands have failed to restore network connectivity to an Ethernet port. This command wipes out all previous Ethernet and Network Fault Tolerance settings. The specified Ethernet port is configured with a minimal static IP address configuration.

set network status

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

Syntax Description

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

Command Modes

Admin
Command privilege level: 1
Allowed during upgrade: No

Command History

Release	Modifications
1.2	This command was first introduced.

Usage Guidelines

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



Caution

Executing this command will cause CTS-Manager to temporarily lose network connectivity.

Examples

```
admin: set network status eth0 down
```

set password maximum age

set password maximum *days*

Syntax Description

<i>days</i>	Specifies the number of days
-------------	------------------------------

Command Modes

Admin
Command privilege level: 1
Allowed during upgrade: No

Command History

Release	Modifications
1.7	This command was first introduced.

Usage Guidelines

This command modifies the value of the maximum password age for Cisco Unified CM OS admin accounts in days.

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

Examples

```
admin:set password maximum 667
```

set password minimum age

set password minimum *days*

Syntax Description

<i>days</i>	Specifies the number of days
-------------	------------------------------

Command Modes

Admin
Command privilege level: 1
Allowed during upgrade: No

Command History

Release	Modifications
1.7	This command was first introduced.

Usage Guidelines

This command modifies the value of the minimum password age for OS admin accounts in days. Acceptable values should be equal to or greater than 0 days but less than or equal to 10 days.

Examples

```
admin:set password maximum 8
```

set password complexity character

set password complexity character {enable | disable}

Syntax Description

enable	Enables this feature
disable	Disables this feature

Command Modes

Admin
 Command privilege level: 1
 Allowed during upgrade: No

Command History

Release	Modifications
1.7	This command was first introduced.

Usage Guidelines

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



Note

You must change the passwords for the existing Cisco Unified CM OS accounts for the password complexity rules to be effective.

When enabled, the passwords will need to following guidelines:

1. It must have at least one lower-case character.
2. It must have at least one uppercase, one digit and one special character.
3. All of the adjacent characters on the keyboard will not be accepted.
4. Any of the previous ten passwords cannot be reused.
5. The admin user password can only be changed only once in 24 hours.

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

Examples

```
admin:set password complexity character enable
```


set password complexity minimum-length

set password complexity minimum-length *value*

Syntax Description

<i>value</i>	Specifies the minimum character length of the password.
--------------	---

Command Modes

Admin
Command privilege level: 1
Allowed during upgrade: No

Command History

Release	Modifications
1.7	This command was first introduced.

Usage Guidelines

This command modifies the value of the minimum password length for Cisco Unified CM OS accounts. Acceptable values should be equal to or greater than 8.



Note

Use this command only after enabling the character complexity of passwords.

Examples

```
admin:set password complexity minimum-length 8
```

set password expiry maximum-age

set password expiry maximum-age {enable | disable}

Syntax Description

enable	Turns on the password expiry maximum-age feature.
disable	Turns off the password expiry maximum-age feature.

Command Modes

Admin
 Command privilege level: 1
 Allowed during upgrade: No

Command History

Release	Modifications
1.7	This command was first introduced.

Usage Guidelines

This command enables or disables the password expiry maximum-age feature for OS accounts.
 This command sets the value of maximum password age to 3650 days (10 yrs) for Unified CM OS admin accounts.

Examples

admin: **set password expiry maximum-age enable**

set password expiry minimum-age

set password expiry minimum-age {enable | disable}

Syntax Description

enable	Turns on the password expiry minimum-age feature.
disable	Turns off the password expiry minimum-age feature.

Command Modes

Admin
Command privilege level: 1
Allowed during upgrade: No

Command History

Release	Modifications
1.7	This command was first introduced.

Usage Guidelines

This command enables or disables the password expiry maximum-age feature for OS accounts.
This command sets the value of minimum password age to 1 day (24 hrs) for OS admin accounts.

Examples

```
admin:set password expiry minimum-age enable
```

set password history

set password history *value*

Syntax Description

<i>value</i>	Specifies the number of passwords that will be maintained.
--------------	--

Command Modes

Admin
 Command privilege level: 1
 Allowed during upgrade: No

Command History

Release	Modifications
1.7	This command was first introduced.

Usage Guidelines

This command modifies the number of passwords that will be maintained in the history for OS admin accounts.



Note

New passwords matching remembered passwords are not allowed.

Examples

```
admin:set password history 12
```

set password inactivity

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

Syntax Description

period	Sets the password inactivity feature for OS accounts.
<i>days</i>	Specifies the password inactivity value in days.
enable	Turns on the password inactivity feature with the default value set to 10 days.
disable	Turns off the password inactivity feature with the default value set to 10 days.

Command Modes

Admin
Command privilege level: 1
Allowed during upgrade: No

Command History

Release	Modifications
1.7	This command was first introduced.

Usage Guidelines

This command enables, disables or sets the password inactivity for the OS accounts.

Examples

```
admin:set password inactivity enable
```

set password user admin

set password user admin

Syntax Description None

Command Modes Admin
 Command privilege level: 1
 Allowed during upgrade: No

Command History	Release	Modifications
	1.7	This command was first introduced.

Usage Guidelines This command sets a new SysAdmin password.



Note

The password must be at least 6 characters long and is checked for strength. The password should not be something you'd find in a dictionary, a name or any variation of your personal or account name.

Examples admin:set password user admin

set snmp trapdest add

set snmp trapdest add *version username destination [passphrase][engineID][level]*

Syntax Description		
<i>version</i>		Defines Simple Network Management Protocol (SNMP) version, either 3 or 2c.
<i>username</i>		Defines SNMP username (version 3) or community string (version 2c).
<i>destination</i>		Defines destination host, using the following format: n.n.n.n[:port].
<i>passphrase</i>		Defines SNMP version 3 only: defines the user passphrase. The passphrase must contain at least 8 characters.
<i>engineID</i>		Defines SNMP version 3 only: defines engine ID to use for trap.
<i>level</i>		Defines SNMP version 3 only: defines level. Available values for this field are: - authNoPriv (default) - authPriv - noauthNoPriv

Command Modes	Admin
	Command privilege level: 1

Command History	Release	Modifications
	1.2	This command was first introduced.

Usage Guidelines	This command sets a Simple Network Management Protocol (SNMP) trap destination.
------------------	---

Examples	<pre>admin:set snmp trapdest add 3 trapusr 64.101.180.49:162 authnopriv trappass 0x8000DEECAF8111BEEFADE</pre> Successfully added trap destination
----------	---

set snmp trapdest del

set snmp trapdest del

Syntax Description None

Command Modes Admin
Command privilege level: 1

Command History	Release	Modifications
	1.2	This command was first introduced.

Usage Guidelines This command deletes a Simple Network Management Protocol (SNMP) trap destination.

Examples

```
admin:set snmp trapdest del
  1) Host = 64.101.180.49:162 (Version 3)

      Version 3 Options:
        User = TimTrap                PW = authpriv
        Level = authnopriv            Hash = md5
        EngineID = 0x80001f8803001a6406bc16

  2) Host = 64.101.180.49 (Version 3)

      Version 3 Options:
        User = TimTrap2                PW = authpriv
        Level = authnopriv            Hash = md5
        EngineID = 0x80001f8803001a6406bc16

  3) Host = 64.101.180.49:162 (Version 3)

      Version 3 Options:
        User = trapusr                PW = trappass
        Level = authnopriv            Hash = md5
        EngineID = 0x8000DEECAFE8111BEEFADE

Enter which trap number to delete: 2
Successfully deleted trap destination
```


set snmp user add

set snmp trapdest add *version username access [phrase] [level]*

Syntax Description		
<i>version</i>		Defines Simple Network Management Protocol (SNMP) version, either 3 or 2c.
<i>username</i>		Defines SNMP username (version 3) or community string (version 2c). User names can be from 1 to 32 characters.
<i>access</i>		defines which SNMP tasks can be accessed; values are: • r (read) • w (write) • rw (read and write)
<i>phrase</i>		SNMP version 3 only: defines the user passphrase. The passphrase must contain at least 8 characters.
<i>level</i>		SNMP version 3 only: defines level. Available values for this field are: • authNoPriv (default) • authPriv • noauthNoPriv

Command Modes

Admin

Command privilege level: 1

Command History	Release	Modifications
	1.7	This command was first introduced.

Usage Guidelines

This command adds a new user or community to snmp.

Examples

```
admin:set snmp user add 3 testusr rw authpriv testpass
Successfully added user

admin:set snmp user add 2c test_RO r
Successfully added user
```

set snmp user del

set snmp user del *version username*

Syntax Description	<i>version</i>	Defines Simple Network Management Protocol (SNMP) version, either 3 or 2c.
	<i>username</i>	Defines SNMP username (version 3) or community string (version 2c). User names can be from 1 to 32 characters.

Command Modes	Admin
	Command privilege level: 1

Command History	Release	Modifications
	1.7	This command was first introduced.

Usage Guidelines	This command deletes a user or community from snmp.
-------------------------	---

Examples	admin: set snmp user del 3 tim Successfully deleted user
	admin: set snmp user del 2c test_RO Successfully deleted user

set syslog facility

set syslog facility *facility*

Syntax Description	<i>facility</i>	Defines default syslog message facility. Values are from local0 to local7.				
Command Modes	Admin Command privilege level: 1					
Command History	<table><tr><th>Release</th><th>Modifications</th></tr><tr><td>1.7</td><td>This command was first introduced.</td></tr></table>	Release	Modifications	1.7	This command was first introduced.	
Release	Modifications					
1.7	This command was first introduced.					
Usage Guidelines	This command sets the default facility used for syslog messages.					
Examples	admin: set syslog facility local1 Setting to local1 facility					

set syslog heartbeat facility

set syslog heartbeat facility *facility*

Syntax Description	<i>facility</i>	Defines default syslog heartbeat facility. Values are from local0 to local7.
Command Modes	Admin Command privilege level: 1	
Command History	Release	Modifications
	1.7	This command was first introduced.
Usage Guidelines	This command sets the facility for heartbeat messages.	
Examples	admin: set syslog heartbeat facility local1 Setting to local1 facility	

set syslog heartbeat interval

set syslog heartbeat interval *interval*

Syntax Description	<i>interval</i> Defines interval in minutes from 0 to 2880. If set to 0, heartbeat messages will be disabled.
---------------------------	---

Command Modes	Admin Command privilege level: 1
----------------------	-------------------------------------

Command History	<table><tr><th>Release</th><th>Modifications</th></tr><tr><td>1.7</td><td>This command was first introduced.</td></tr></table>	Release	Modifications	1.7	This command was first introduced.
Release	Modifications				
1.7	This command was first introduced.				

Usage Guidelines	This command sets the heartbeat interval in minutes.
-------------------------	--

Examples	admin: set syslog heartbeat interval 10
-----------------	--

set syslog heartbeat msg

set syslog heartbeat msg *text*

Syntax Description

<i>text</i>	Defines text string within double quotes ("text") for heartbeat messages.
-------------	---

Command Modes

Admin

Command privilege level: 1

Command History

Release	Modifications
1.7	This command was first introduced.

Usage Guidelines

This command sets the heartbeat message text.

Examples

```
admin:set syslog heartbeat msg "example message"
Setting message to "example message"
```

set syslog timezone

set syslog timezone *zone*

Syntax Description

zone Defines the timezone for syslog message timestamps. Choices are:

- local: local timezone
- gmt: Greenwich mean time

Command Modes

Admin
Command privilege level: 1

Command History

Release	Modifications
1.7	This command was first introduced.

Usage Guidelines

This command sets the timezone used for syslog message timestamps.

Examples

admin:**set syslog timezone gmt**

set syslog version

set syslog version *version*

Syntax Description

version Defines the syslog message output format version. Choices are:

- 0: CiscoLog versions 1.1 format
- 1: IETF/RFC Syslog Protocol Version 1 format

Command Modes

Admin
Command privilege level: 1

Command History

Release	Modifications
1.7	This command was first introduced.

Usage Guidelines

This command sets the output format version of the syslog messages to either CiscoLog v1.1 or RFC Syslog v1.

Examples

```
admin:set syslog version 0
Setting to 0, the CiscoLog v1.1 format
```


set web-security

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

Syntax Description

<i>orgunit</i>	Represents the organizational unit
<i>orgname</i>	Represents the organizational name.
<i>locality</i>	Represents the organization location.
<i>state</i>	Represents the organization state.
<i>country</i>	Represents the organization country.
<i>alternate-host-name</i> (optional)	Specifies an alternate name for the host when you generate a web-server (Tomcat) certificate.7ays8Nun

Command Modes

Admin
Command privilege level: 0
Allowed during upgrade: No

Command History

Release	Modifications
1.3	This command was first introduced.

Usage Guidelines

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



Note

When you set an alternate-host-name parameter with the **set web-security** command, self-signed certificates for tomcat will contain the Subject Alternate Name extension with the alternate-host-name specified. CSR for Cisco Unified Communications Manager will contain Subject Alternate Name Extension with the alternate host name included in the CSR. You need to restart the “Cisco Tomcat” service for the new certificate to take effect.

Examples

```
admin:set web-security mydept mycorp SanJose CA US
Successfully generated self signed certificate for tomcat
```

set workingdir

set workingdir [**activelog** | **inactivelog**] *directory*

Syntax Description

activelog	sets the working directory for active logs.
inactivelog	set the working directory for inactive logs.
<i>directory</i>	Represents the current working directory.

Command Modes

Admin
 Command privilege level: 00 for logs, 1 for TFTP
 Allowed during upgrade: Yes

Command History

Release	Modifications
1.2	This command was first documented.

Usage Guidelines

This command sets the working directory for active, inactive, and installation logs.
 Only a valid subdirectory can be used. Please do not use “/” or “..” in front of the directory name. Use the **show workingdir** command to validate that this command worked.

Examples

```
admin:set workingdir activelog syslog
```