C H A P T E R 4

CTRS Set Commands

October 2011

This chapter contains Cisco TelePresence Recording Server (CTRS) **set** commands:

> **Note** For information about using the CTRS administration software, refer to the *Cisco TelePresence Recording Server Release 1.8 Administration Guide* at the following URL:
>
> http://www.cisco.com/en/US/products/ps10341/prod_maintenance_guides_list.html

set account enable

set account enable *user-id*

Syntax Description	*user-id*	Name of the user account.

Command Modes   Admin

Command History	Release	Modifications
	1.8	This command was first documented.

Usage Guidelines   Use this command to enable a user account that has been disabled due to inactivity.

Examples   admin:**set account enable test2**

set account name

set account name *name*

Syntax Description

name	Name of the administrative account.

Command Modes   Admin

Command History

Release	Modifications
1.6	This command was first documented.
1.8	This command was changed from **set account** to **set account name**.

Usage Guidelines   Use this command to create a new administrative account. You will be prompted for the appropriate privilege level and password during account creation.

Examples
```
admin:set account test2
Please enter the privilege level :1
        Please enter the password :******
                re-enter to confirm :******
```

set accountlocking

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

Syntax Description		
	disable	Disable account locking
	enable	Enable account locking
	unlocktime *seconds*	The number of seconds an account is disabled. Valid values comprise greater than 300 seconds, but less than 3600 seconds (60 minutes).

Command Modes   Admin

Command History	Release	Modifications
	1.8	This command was first documented.

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 the number of seconds configured with the **unlocktime** option before the account gets unlocked. The default is 300 seconds (5 minutes).

Examples   `set accountlocking enable`

set cli pagination

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

Syntax Description

on	Turns on automatic pagination.
off	Turns off automatic pagination.

Command Modes   Admin

Command History

Release	Modifications
1.6	This command was first documented.

Usage Guidelines   Use this command to turn automatic pagination on or off for the current CLI session. Before running this command, please use the **show cli pagination** command to see the status of automatic pagination.

Examples

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

set commandcount

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

Syntax Description

enable	Enables command count feature. Using **enable** changes the CLI command prompt so that it displays a numeric value showing how many CLI commands have been executed
disable	Disables command count feature. Using **disable** changes the CLI command prompt so that it stops displaying a numeric value showing how many CLI commands have been executed.

Command Modes   Admin

Command History

Release	Modifications
1.6	This command was first documented.

Usage Guidelines   Use this command to either enable or disable the command count feature. This command changes the CLI command prompt so that it displays a numeric value showing how many CLI commands have been executed. This setting is valid for current session only.

Examples
```
admin:set commandcount enable
admin 0005:
```

set date

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

Syntax Description	*HH:mm:ss:MM/DD/YY*	The time in format hours:minutes:seconds and the date in the format month/day/year. The date format *MM/DD/YYY* is also accepted.

Command Modes   Admin

Command History

Release	Modifications
1.8	This command was first documented.

Usage Guidelines   Use this command to set the date and time on the CTRS.

Examples   admin:**set date 12:30:00:08/01/11**

set diskalertthreshold

set diskalertthreshold *threshold email*

Syntax Description	*threshold*	A value between 1 and 100 defining the percentage of the capacity of the hard disk that must be filled before an alert is sent.
	email	A valid email address to which alerts will be sent.

Command Modes   Admin

Command History	Release	Modifications
	1.8	This command was first documented.

Usage Guidelines   Use this command to cause the CTRS to send email alerts when the internal hard disk is filled to the capacity defined by the *threshold* parameter.

Examples   admin:**set diskalertthreshold 90 test22@cisco.com**

set hdcapable

set hdcabable {enable | disable}

Syntax Description

enable	Set the default to record HD video
disable	Set the default not to record HD video

Command Modes   Admin

Command History

Release	Modifications
1.8	This command was first documented.

Usage Guidelines   This command sets the default value for High Definition (HD) video recording.

Examples   admin:**set hdcapable enable**

set ldcapable

set ldcabable {enable | disable}

Syntax Description		
	enable	Set the default to record LD video
	disable	Set the default not to record LD video

Command Modes   Admin

Command History	Release	Modifications
	1.8	This command was first documented.

Usage Guidelines   This command sets the default value for Low Definition (LD)video recording.

Examples   admin:**set ldcapable enable**

set logging

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

Syntax Description	**enable**	Enables logging.
	disable	Disables logging.

Command Modes   Admin

Command History

Release	Modifications
1.6	This command was first documented.

Usage Guidelines   Use this command to either enable or disable logging for the current admin accounts.

Examples   admin:**set logging enable**

set network dhcp eth0

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

Syntax Description

enable	Sets the Ethernet interface to use Dynamic Host Configuration Protocol (DHCP).
disable	Sets the Ethernet interface NOT to use DHCP.
node_ip	Node IP address
net_mask	Subnet mask
gateway_ip	Gateway IP address

Command Modes   Admin

Command History

Release	Modification
1.6	This command was first documented.

Usage Guidelines   Use this command (with the **enable** keyword) to set the Ethernet interface to use Dynamic Host Configuration Protocol (DHCP) if not already enabled, then to restart the system.

Use this command (with the **disable** keyword) to set the Ethernet interface to not use DHCP provided DHCP is enabled, then to restart the system.

Examples
```
admin:set network dhcp eth0 enable
        ***   W A R N I N G   ***
This will cause the system to restart - Do you want to continue ?
Enter "yes" to continue and restart or any other key to abort
yes
executing...
Broadcast message from root (Thu Jun 24 13:00:21 2004):

The system is going down for restart NOW!

admin:set network dhcp eth0 disable 1.2.3.4  255.255.255.0  5.4.3.2
        ***   W A R N I N G   ***
This will cause the system to restart - Do you want to continue ?
Enter "yes" to continue and restart or any other key to abort
yes
executing...
Broadcast message from root (Thu Jun 24 13:00:21 2004):

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

set network dns

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

Syntax Description		
primary *address*	Defines a new address for the primary Domain Name System (DNS) server. Values for *address* are valid dotted decimal IP addresses.	
secondary *address*	Defines a new address for the secondary DNS server. Values for *address* are valid dotted decimal IP addresses.	

Command Modes   Admin

Command History	Release	Modifications
	1.6	This command was first documented.

Usage Guidelines   Use this command to define new IP addresses for primary or secondary DNS servers.

This command causes a temporary loss of network connectivity. If you want to continue with defining a new address for the DNS server, type **Yes**. Otherwise, click any other key to abort.

Examples
```
admin:set network dns primary 1.2.3.4
*** 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
```

set network dns options

set network dns options [timeout *value*] [attempts *value*] [rotate]

Syntax Description		
timeout *value*		Defines how long CTRS waits before considering a Domain Name System (DNS) query to have failed. *Value* indicates number of seconds.
attempts *value*		Defines the number of times CTRS repeats a DNS query before considering the query to have failed. *Value* indicates number of attempts.
rotate		Defines the way in which DNS servers are contacted (round-robin fashion). This options distributes the load across DNS servers.

Command Modes   Admin

Command History	Release	Modifications
	1.6	This command was first documented.

Usage Guidelines   Use this command to set optional features in contacting DNS servers, such as the way in which DNS servers are contacted, the amount of time and the number of retries before a DNS query is considered a failed attempt.

This command causes a temporary loss of network connectivity.

Examples
```
admin:set network dns options timeout 10
         ***  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 domain

set network domain *name*

Syntax Description

name	Defines domain name in which the CTRS resides.

Command Modes Admin

Command History

Release	Modifications
1.6	This command was first documented.

Usage Guidelines Use this command to set the domain of the CTRS.

This command causes a temporary loss of network connectivity.

Examples
```
admin:set network domain cisco.com
        ***   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 failover

set network failover {enable | disable}

Syntax Description	enable	Enables network failover
	disable	Disables network failover

Command Modes   Admin

Command History	Release	Modifications
	1.6	This command was first documented.

Usage Guidelines   Use this command to enable or disable network failover.

Enabling network failover creates a virtual interface (bond0) that uses Ethernet interface eth0, but fails over to Ethernet interface eth1 if eth0 fails. All three interfaces (bond0, eth0, and eth1) share the same IP and MAC address.

Disabling network failover restores Ethernet interface eth0 with equivalent configuration parameters and removes the virtual interface bond0.

Setting failover will cause a restart of the system.

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

        ***   W A R N I N G   ***
This will cause the system to restart - Do you want to continue?
Enter "yes" to continue and restart or any other key to abort
yes
executing...
```

set network gateway

set network gateway *address*

Syntax Description	*address*	Defines new gateway IP address.

Command Modes   Admin

Command History

Release	Modifications
1.6	This command was first documented.

Usage Guidelines   Use this command to set a new gateway IP address; this command causes a temporary loss of network connectivity.

✎
Note   Entering the wrong gateway address effectively disables network access to this node.

Examples
```
admin:set network gateway 192.168.1.1
        ***   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
```

set network hostname

set network hostname *name*

Syntax Description	*name*	Defines hostname.

Command Modes   Admin

Command History	Release	Modifications
	1.6	This command was first documented.

Usage Guidelines   Use this command to set the network hostname; this command causes a restart of the system.

> **Note**   The hostname must start with a letter, end with an alphanumeric, and may contain any alphanumeric characters or hyphen in between. The hostname must be 63 characters or less.

Examples

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

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

set network ip eth0

set network ip eth0 *address*

Syntax Description

address	Defines a new IP address and subnet mask for Ethernet 0. Values for *address* are valid dotted decimal IP addresses followed by subnet mask value.

Command Modes   Admin

Command History

Release	Modifications
1.6	This command was first documented.

Usage Guidelines   Use this command to define a new IP address and subnet mask for Ethernet 0. The system automatically restarts after you execute this command.

Examples
```
admin:set network ip eth0 192.168.1.5 255.255.255.0
*** WARNING ***
This will cause the system to restart - Do you want to continue?
Enter "yes" to continue and restart or any other key to abort
yes
```

set network max_ip_conntrack

set network max_ip_contrack *value*

Syntax Description	*value*	Defines ip_conntrack_max value.

Command Modes   Admin

Command History	**Release**	**Modifications**
	1.6	This command was first documented.

Usage Guidelines   Use this command to set the ip_conntrack_max value.

Examples   admin:**set network max_ip_conntrack 256000**

set network mtu

set network mtu *value*

Syntax Description

value	Defines MTU maximum size. Standard size is 1500.

Command Modes   Admin

Command History

Release	Modifications
1.6	This command was first documented.

Usage Guidelines   Use this command to set the MTU maximum size. This command causes a temporary loss of network connectivity.

Examples

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

        Do you want to continue ?

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

yes
executing...
```

set network nic eth0 auto

set network nic eth0 auto {en | dis}

Syntax Description

en	Enables auto negotiation
dis	Disabled auto negotiation

Command Modes   Admin

Command History

Release	Modifications
1.6	This command was first documented.

Usage Guidelines   Use this command to configure auto negotiation for speed and duplex settings for a Network Interface card (NIC), meaning that CRMS will attempt to negotiate the highest speed possible with the switch. Per the IEEE standard, 1000BASE-T (1 GB Ethernet) can only be enabled via auto-negotiation.

> **Note**   For the changes to take effect, the NIC will be reset, which will cause a temporary loss of network connectivity.

Examples   admin:**set network nic eth0 auto en**

set network nic eth0 speed

set network nic eth0 speed {10 | 100}

Syntax Description	10	10 megabits per second
	100	100 megabits per second

Command Modes   Admin

Command History	Release	Modifications
	1.6	This command was first documented.

Usage Guidelines   Use this command to configure speed settings for a Network Interface card (NIC). This command controls the speed of the Ethernet connection in megabits per second. When used, this command disables auto negotiation.

> **Note**   Per the IEEE standard, 1000BASE-T (1 GB Ethernet) can only be enabled via auto-negotiation.

> **Note**   For the changes to take effect, the NIC will be reset, which will cause a temporary loss of network connectivity.

Examples   admin:**set network nic eth0 speed 100**

set network nic eth0 duplex

set network nic eth0 duplex {half | full}

Syntax Description

half	Enables half duplex
full	Enables full duplex

Command Modes   Admin

Command History

Release	Modifications
1.6	This command was first documented.

Usage Guidelines   Use this command to configure duplex settings of the Ethernet connection. When used, it will disable auto negotiation.

✎

Note   For the changes to take effect, the NIC will be reset, which will cause a temporary loss of network connectivity.

Examples   admin:**set network nic eth0 duplex half**

set network pmtud

set network pmtud {enable | disable}

Syntax Description

enable	Enables Path MTU Discovery
disable	Disables Path MTU Discovery

Command Modes   Admin

Command History

Release	Modifications
1.6	This command was first documented.

Usage Guidelines   Use this command to enable or disable Path MTU Discovery.

Note   For the changes to take effect, this command causes a temporary loss of 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 network_mask gateway*

Syntax Description

ip address	Defines value for static IP address.
network_mask	Defines value for network mask
gateway	Defines IP address of primary gateway

Command Modes   Admin

Command History

Release	Modifications
1.6	This command was first documented.

Usage Guidelines   Use this command to configure 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.

> **Note**   It is imperative that the original Ethernet port settings be reconfigured after this command using other CLI 'set network ...'commands.

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.

It's imperative that the original Ethernet port settings be
reconfigured AFTER this command using other CLI 'set network ...'
commands.

This command will restart the networking on this host.

Continue (y/n)?y

Shutting down interface eth0:  [  OK  ]
Shutting down loopback interface:  [  OK  ]
Setting network parameters:  [  OK  ]
Bringing up loopback interface:  [  OK  ]
Bringing up interface eth0:  [  OK  ]
```

set network status eth0

set network status eth0 {up | down}

Syntax Description

up	Sets state of eth0 to up.
down	Sets state of eth0 to down.

Command Modes   Admin

Command History

Release	Modifications
1.6	This command was first documented.

Usage Guidelines   Use this command to set the state of the Ethernet interface eth0 to up or down.

Examples
```
admin:set network restore eth0 down
***   W A R N I N G   ***
This will cause the system to temporarily lose network connectivity
Continue (y/n) ?y
Executed command unsuccessfully
status is down
```

set password admin

set password admin

Syntax Description   None

Command Modes   Admin

Command History

Command	Modifications
1.1	This command was first documented.
1.8	This command was removed and is no longer supported in version 1.8.

Usage Guidelines   Use this command to set a new administrator password.

> **Note**   Passwords must be at least 6 characters, but not more than 64 characters in length, and can contain upper and lower case alphanumeric characters and the underscore and dash characters. The following usernames are not allowed: apache, daemon, nobody, operator, and shutdown.

Examples
```
admin:set password admin
Please enter the old password: ******
Please enter the new password: ********
Re-enter new password to confirm: ********
```

set password age maximum

set password age maximum *days*

Syntax Description

days	The number of days before a password must be changed.

Command Modes   Admin

Command History

Command	Modifications
1.8	This command was first documented.

Usage Guidelines   This command modifies the value of the maximum password age for OS admin accounts in days.

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

Examples   admin:**set password age maximum 60**

set password age minimum

set password age minimum *days*

Syntax Description

days	The number of days before a password can be changed.

Command Modes   Admin

Command History

Command	Modifications
1.8	This command was first documented.

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

Acceptable values for minimum password age should be equal to or greater than 0 days but less than or equal to 10 days.

Examples   admin:**set password age minimum 7**

set password complexity character

set password complexity character {enable | disable}

Syntax Description

enable	Enable password complexity
disable	Disable password complexity

Command Modes   Admin

Command History

Command	Modifications
1.8	This command was first documented.

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 *length*

Syntax Description

length	The minimum number of characters required for all passwords.

Command Modes   Admin

Command History

Command	Modifications
1.8	This command was first documented.

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	Enable password expiration upon reaching maximum age.
disable	Disable password expiration.

Command Modes   Admin

Command History

Command	Modifications
1.8	This command was first documented.

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	Enable password minimum age.
	disable	Disable password minimum age.

Command Modes   Admin

Command History	Command	Modifications
	1.8	This command was first documented.

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 expiry user maximum-age

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

Syntax Description

enable	Enable password expiration upon reaching maximum age.
disable	Disable password expiration.

Command Modes   Admin

Command History

Command	Modifications
1.8	This command was first documented.

Usage Guidelines   This command enables or disables the password expiry maximum-age feature for a specific OS account.

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

set password expiry user minimum-age

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

Syntax Description

enable	Enable password minimum age.
disable	Disable password minimum age.

Command Modes   Admin

Command History

Command	Modifications
1.8	This command was first documented.

Usage Guidelines   This command enables or disables the password expiry minimum-age feature for a specific OS account.

admin:**set password expiry user minimum-age enable**

set password history

set password history *number*

Syntax Description

number	The number of historical passwords that will be retained for each account. Set this number to 0 to disable password history tracking.

Command Modes   Admin

Command History

Command	Modifications
1.8	This command was first documented.

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

Examples   admin:**set password history 8**

set password inactivity

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

Syntax Description	**enable**	Enable password inactivity.
	disable	Disable password inactivity
	days	The number of days a password must be inactive before it is disabled.

Command Modes   Admin

Command History	**Command**	**Modifications**
	1.8	This command was first documented.

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

Examples   admin:**set password enable**

set password user admin

set password user admin

Syntax Description   None

Command Modes   Admin

Command History

Command	Modifications
1.8	This command was first documented.

Usage Guidelines   Use this command to set a new administrator password.

> **Note**   Passwords must be at least 6 characters, but not more than 64 characters in length, and can contain upper and lower case alphanumeric characters and the underscore and dash characters. The following usernames are not allowed: apache, daemon, nobody, operator, and shutdown.

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

set password user security

set password user security

Syntax Description   None

Command Modes   Admin

Command History

Command	Modifications
1.8	This command was first documented.

Usage Guidelines   Use this command to set a new security password. The security password is used to authenticate other servers.

Note   Passwords must be at least 6 characters, but not more than 64 characters in length, and can contain upper and lower case alphanumeric characters and the underscore and dash characters. The following usernames are not allowed: apache, daemon, nobody, operator, and shutdown.

Examples
```
admin:set password security
Please enter the old password: ******
Please enter the new password: ********
Re-enter new password to confirm: ********
```

set refreshrate

set refreshrate *rate*

Syntax Description

rate	The number of seconds to space apart IDR frames.

Command Modes   Admin

Command History

Command	Modifications
1.8	This command was first documented.

Usage Guidelines   Use this command to set the default spacing between Instantaneous Decoding Refresh (IDR) frames in the video streams. Larger spaces between IDR frames will cause better file compression, resulting in a smaller file, but possibly lower-quality recording.

```
admin:set refreshrate 15
```

set snmp trapdest add

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

Syntax Description

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

Command Modes   Admin

Command History

Release	Modifications
1.6	This command was first documented.

Usage Guidelines   Use this command to set a Simple Network Management Protocol (SNMP) trap destination.

In SNMP v3, if you use the same username in the **set snmp trapdest add** and **set snmp user add** commands, you must also use the same password. You cannot use the same username with different passwords.

Examples   admin:**set snmp trapdest add 3 trapusr 64.101.180.49:162 authnopriv trappass 0x8000DEECAFE8111BEEFADE**

Successfully added trap destination

set snmp trapdest del

set snmp trapdest del

Syntax Description   None

Command Modes   Admin

Command History

Release	Modifications
1.6	This command was first documented.

Usage Guidelines   Use this command to delete 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 user add *version username access* [*level*] [*passphrase*]

Syntax Description

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

Command Modes   Admin

Command History

Release	Modifications
1.6	This command was first documented.

Usage Guidelines   Use this command to add a new user or community to SNMP. You can add up to eight SNMP users.

✎
Note   For SNMP version 3, hash will always be MD5 and encryption will be DES.

In SNMP v3, if you use the same username in the **set snmp trapdest add** and **set snmp user add** commands, you must also use the same password. You cannot use the same username with different passwords.

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

version	Defines Simple Network Management Protocol (SNMP) version, either 3 or 2c
username	Defines SNMP username (version 3) or community string (version 2c)

Command Modes   Admin

Command History

Release	Modifications
1.6	This command was first documented.

Usage Guidelines   Use this command to delete a user or community from SNMP.

> **Note**   For SNMP version 3, hash will always be MD5 and encryption will be DES.

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	*facility*	Defines default syslog message facility. Values are from local0 to local7.

Command Modes   Admin

Command History

Release	Modifications
1.6	This command was first documented.

Usage Guidelines   Use this command to set 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

facility	Defines default syslog heartbeat facility. Values are from local0 to local7.

Command Modes   Admin

Command History

Release	Modifications
1.6	This command was first documented.

Usage Guidelines   Use this command to set the default facility used 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	*interval*	Defines interval in minutes from 0 to 2880. If set to 0, heartbeat messages will be disabled.

Command Modes   Admin

Command History	Release	Modifications
	1.6	This command was first documented.

Usage Guidelines   Use this command to set the syslog heartbeat interval in minutes. Setting this command to 0 disables syslog heartbeat messages.

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

set syslog heartbeat msg

set syslog heartbeat msg *text*

Syntax Description	*text*	Text string within double quotes ("text") for heartbeat messages.

Command Modes   Admin

Command History

Release	Modifications
1.6	This command was first documented.

Usage Guidelines   Use this command to define the syslog heartbeat message text.

Examples

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

set syslog heartbeat severity

set syslog heartbeat severity *level*

Syntax Description	*level*	Defines the level of severity for syslog heartbeat messages. Available choices are from 0 (emergency) to 7(debug).

Command Modes   Admin

Command History

Release	Modifications
1.6	This command was first documented.

Usage Guidelines   Use this command to set the level of severity for syslog heartbeat messages.

Examples   admin:**set syslog heartbeat severity 7**
Setting severity to 7

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 History

Release	Modifications
1.6	This command was first documented.

Usage Guidelines   Use this command to set 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: RFC Syslog Protocol Version 1 format

Command Modes   Admin

Command History

Release	Modifications
1.6	This command was first documented.

Usage Guidelines   Use this command to set the system message output format version.

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

set timezone

set timezone *timezone*

Syntax Description

timezone	Enter the appropriate text string or timezone code for the zone you want to configure. Use the **show timezone list** command to display a complete list of available timezone codes.

Command Modes   Admin

Command History

Release	Modifications
1.6	This command was first documented.

Usage Guidelines   Use this command to set a new timezone value. This sets system time on CTRS server.

Examples

```
admin:set timezone America/Los_Angeles
Using timezone: America/Los_Angeles

A system restart is required

Change timezone and reboot (yes|no)? yes
Executed command successfully
```

set videoquality

set videoqualty {high | higher | highest | low | lower | lowest | medium}

Syntax Description

high	Highest Details, Good Motion: 1080p
higher	Highest Details, Better Motion: 1080p
highest	Highest Details, Best Motion: 1080p
low	High Detail, Limited Motion: 720P (Lite)
lower	High Detail, Good Motion: 720p
lowest	High Detail, Better Motion: 720p
medium	High Detail, Best Motion: 720p

Command Modes   Admin

Command History

Release	Modifications
1.8	This command was first documented.

Usage Guidelines   Use this command to set video recording quality.

Examples   admin:**set videoquality highest**

set web-security

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

Syntax Description

orgunit	Specifies the organizational business unit or division.
orgname	Specifies the organization name.
city	Specifies the city in which the organization is located.
state	Specifies the state in which the organization is located.
country	Specifies the country in which the organization is located.
alternatehostname	Specifies an alternate name for the host when you generate the self-signed certificate.

Command Modes   Admin

Command History

Release	Modifications
1.8	This command was reintroduced.

Usage Guidelines   Use this command if you are denied access to the CTRS Administrative UI because of a revoked SSL certificate. This command generates a self-signed certificate for the web server (Tomcat) that enables you to regain access to the CTRS Administrative UI.

For each argument, you can enter upper- and lower-case alphabetical characters. Spaces between characters are not allowed.

> **Note**   You must restart the "Cisco Tomcat" service for the new certificate to take effect.

Examples

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

set workingdir activelog

set workingdir activelog *directory*

Syntax Description	*directory*	Valid subdirectory of activelog

Command Modes   Admin

Command History

Release	Modifications
1.6	This command was first documented.

Usage Guidelines   Use this command to set the CLI working directory for activelog. Only a valid subdirectory can be used. Do not use a forward slash (/) or a period (.) in front of the directory name. Use the **show workingdir** command to confirm this command worked.

Examples   admin:**set workingdir activelog syslog**

set workingdir inactivelog

set workingdir inactivelog *directory*

Syntax Description

directory	Valid subdirectory of inactivelog

Admin

Command History

Release	Modifications
1.6	This command was first documented.

Usage Guidelines Use this command to set the CLI working directory for inactivelog. Only a valid subdirectory can be used. Do not use a forward slash (/) or a period (.) in front of the directory name. Use the **show workingdir** command to validate.

Examples admin:**set workingdir inactivelog syslog**