Cisco ISE CLI Commands in Configuration Mode

This chapter describes commands that are used in configuration (config) mode in the Cisco ISE command-line interface (CLI). Each of the command in this chapter is followed by a brief description of its use, command syntax, usage guidelines, and one or more examples.

Switch to Configuration Mode in EXEC Mode

In EXEC mode, you can enter into configuration mode by running the **configure** or **configure terminal (conf t)** command.

You cannot enter configuration commands directly in EXEC mode from the Cisco ISE CLI. Some of the configuration commands require you to enter the configuration submode to complete the command configuration.

To exit configuration mode, enter the **exit**, **end**, or **Ctrl-z** command.

Configuration commands include **interface**, **Policy List**, and **repository**.

You can perform configuration tasks in configuration mode. You must save your configuration changes so that you preserve them during a system reload or power outage.

When you save the configuration, these commands remain across Cisco ISE server reboots, but only if you run either of these commands:

- **copy running-config startup-config**
- **write memory**

Configuring Cisco ISE in the Configuration Mode

You can enter configuration and configuration submodes commands to change the actual configuration of the Cisco ISE server in configuration mode.

Step 1 Enter **configure terminal** to enter into the configuration mode.

```
ise/admin# configure terminal
Enter configuration commands, one per line. End with CNTL-Z.
ise/admin(config)# (configuration mode)
```

Step 2 Enter a question mark (?) to obtain a listing of commands in the configuration mode.

```
ise/admin(config)# ?
Configure commands:
cdp               CDP Configuration parameters
clock             Configure timezone
conn-limit        Configure a TCP connection limit from source IP
do                EXEC command
end               Exit from configure mode
exit              Exit from configure mode
hostname          Configure hostname
icmp              Configure icmp echo requests
interface         Configure interface
ip                Configure IP features
kron              Configure command scheduler
logging           Configure system logging
max-ssh-sessions  Configure number of concurrent SSH sessions
no                Negate a command or set its defaults
ntp               Specify NTP configuration
password-policy   Password Policy Configuration
rate-limit        Configure a TCP/UDP/ICMP packet rate limit from source IP
repository        Configure Repository
service           Specify service to manage
snmp-server       Configure snmp server
synflood-limit    Configure a TCP SYN packet rate limit
username          User creation
```

Step 3 Enter into the configuration submode. The configuration mode has several configuration submodes. Each of these submodes places you deeper in the prompt hierarchy. From this level, you can enter commands directly into the Cisco ISE configuration.

```
ise/admin(config)# interface GigabitEthernet 0
ise/admin(config-GigabitEthernet)#
```

Step 4 Enter **exit** in sequence at the command prompt to exit both Configuration and EXEC modes. When you enter **exit**, Cisco ISE backs you out one level and returns you to the previous level. When you enter **exit** again, Cisco ISE backs you out to the EXEC level.

```
ise/admin(config)# exit
ise/admin# exit
```

Configuring Cisco ISE in the Configuration Submode

You can enter commands for specific configurations in the configuration submodes. You can use the **exit** or **end** command to exit this prompt and return to the configuration prompt.

Step 1 Enter **configure terminal** to enter into the configuration mode.

```
ise/admin# configure terminal
Enter configuration commands, one per line. End with CNTL-Z.
ise/admin(config)# (configuration mode)
```

Step 2 Enter into the configuration submode.

```
ise/admin# configure terminal
ise/admin(config)# interface GigabitEthernet 0
ise/admin(config-GigabitEthernet)# ?
Configure ethernet interface:
  do        EXEC command
  end       Exit from configure mode
  exit      Exit from this submode
  ip        Configure IP features
  ipv6      Configure IPv6 features
  no        Negate a command or set its defaults
  shutdown  Shutdown the interface
ise/admin(config-GigabitEthernet)# ip ?
address  Configure IP address
```

Step 3 Enter **exit** at the command prompt to exit both configuration submode and configuration mode.

```
ise/admin(config-GigabitEthernet)# exit
ise/admin(config)# exit
ise/admin#
```

CLI Configuration Command Default Settings

CLI configuration commands can have a default form, which returns the command settings to the default values. Most commands disable by default, so in such cases using the default form has the same result as using the **no** form of the command.

However, some commands are enabled by default and have variables set to certain default values. In these cases, the default form of the command enables the command and sets the variables to their default values.

cdp holdtime

To specify the amount of time for which the receiving device should hold a Cisco Discovery Protocol packet from the Cisco ISE server before discarding it, use the **cdp holdtime** command in configuration mode.

cdp holdtime *seconds*

To revert to the default setting, use the **no** form of this command.

no cdp holdtime

Syntax Description

holdtime	Specifies the Cisco Discovery Protocol hold time advertised.
seconds	Advertised hold time value, in seconds. The value ranges from 10 to 255 seconds.

Command Default The default CDP holdtime, in seconds is 180.

Command Modes Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

Cisco Discovery Protocol packets transmit with a time to live, or hold time, value. The receiving device will discard the Cisco Discovery Protocol information in the Cisco Discovery Protocol packet after the hold time has elapsed.

The **cdp holdtime** command takes only one argument; otherwise, an error occurs.

Example

```
ise/admin(config)# cdp holdtime 60
ise/admin(config)#
```

cdp run

To enable the Cisco Discovery Protocol on all interfaces, use the **cdp run** command in configuration mode.

cdp run *GigabitEthernet*

To disable the Cisco Discovery Protocol, use the **no** form of this command.

no cdp run

Syntax Description

run	Enables the Cisco Discovery Protocol. Disables the Cisco Discovery Protocol when you use the **no** form of the **cdp run** command.
GigabitEthernet	(Optional). Specifies the GigabitEthernet interface on which to enable the Cisco Discovery Protocol.
0-3	Specifies the GigabitEthernet interface number on which to enable the Cisco Discovery Protocol.

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

The command has one optional argument, which is an interface name. Without an optional interface name, the command enables the Cisco Discovery Protocol on all interfaces.

Note The default for this command is on interfaces that are already up and running. When you are bringing up an interface, stop the Cisco Discovery Protocol first; then, start the Cisco Discovery Protocol again.

Example

```
ise/admin(config)# cdp run GigabitEthernet 0
ise/admin(config)#
```

cdp timer

To specify how often the Cisco ISE server sends Cisco Discovery Protocol updates, use the **cdp timer** command in configuration mode.

cdp timer *seconds*

To revert to the default setting, use the **no** form of this command.

no cdp timer

Syntax Description

timer	Refreshes at the time interval specified.
seconds	Specifies how often, in seconds, the Cisco ISE server sends Cisco Discovery Protocol updates. The value ranges from 5 to 254 seconds.

Command Default

The default refreshing time interval value, in seconds is 60.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

Cisco Discovery Protocol packets transmit with a time to live, or hold time, value. The receiving device will discard the Cisco Discovery Protocol information in the Cisco Discovery Protocol packet after the hold time has elapsed.

The **cdp timer** command takes only one argument; otherwise, an error occurs.

Example

```
ise/admin(config)# cdp timer 60
ise/admin(config)#
```

clear screen

To clear the contents of terminal screen, use the **clear screen** command in configuration mode.

clear screen

Syntax Description

This command has no keywords and arguments.

Command Default No default behavior or values.

Command Modes Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines **clear screen** is a hidden command. Although **clear screen** is available in Cisco ISE, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line.

Example

The following example shows how to clear the contents of the terminal:

```
ise/admin(config)# clear screen
ise/admin#
```

clock timezone

To set the time zone, use the **clock timezone** command in configuration mode.

clock timezone *timezone*

To disable the time zone, use the **no** form of this command.

no clock timezone

Note Changing the time zone on a Cisco ISE appliance after installation causes the Cisco ISE application on that node to be unusable, which requires you to restart ISE. We recommend that you use the preferred time zone (default UTC) during the installation when the initial setup wizard prompts you for the time zones.

Syntax Description

timezone	Configures system timezone.
timezone	Name of the time zone visible when in standard time. Supports up to 64 alphanumeric characters.

Command Default Coordinated Universal Time (UTC)

Command Modes Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

The system internally keeps time in UTC. If you do not know your specific time zone, you can enter the region, country, and city (see Tables 4-1, 4-2, and 4-3 for common time zones and time zones for Australia and Asia to enter on your system).

Note Several more time zones are available to you. Enter **show timezones** and a list of all time zones available appears in the Cisco ISE server. Choose the most appropriate one for your time zone.

Example

```
ise/admin(config)# clock timezone EST
ise/admin(config)# exit
ise/admin# show timezone
EST
ise/admin#
```

Changing the Time Zone on Cisco ISE Nodes

Changing the time zone on a Cisco ISE appliance after installation causes the Cisco ISE application on that node to be unusable. However, the preferred time zone (default UTC) can be configured during the installation when the initial setup wizard prompts you for the time zones.

Changing time zone impacts different Cisco ISE nodes types of your deployment.

To recover from the impact, use the following steps:

Standalone or Primary Cisco ISE Node

To change the timezone after installation you must re-image the node.

Ensure that you have a backup of latest configuration, and export the necessary certificates and keys.

If you wish to change the time zone, do the following:

- Re-image the Primary Cisco ISE node.
- During the installation, select the appropriate timezone.
- Restore backup and certificates.
- Rejoin Active Directory and apply any per-node configurations for ISE profiling probes, LDAP,etc.

Secondary ISE Node

If you want to change the time zone on the secondary node to keep it to be the same as the primary node, do the following:

- Export the necessary certificates.
- Deregister the secondary node.
- Re-image the node.
- Import the necessary certificates, if required.

- Re-register the node as a secondary node to the primary node.
- Rejoin Active Directory and apply any per-node configurations for ISE profiling probes, LDAP,etc.

Common Time Zones

Table 1: Table 4-1 Common Time Zones (Continued)

Acronym or name	Time Zone Name
Europe	
GMT, GMT0, GMT-0, GMT+0, UTC, Greenwich, Universal, Zulu	Greenwich Mean Time, as UTC
GB	British
GB-Eire, Eire	Irish
WET	Western Europe Time, as UTC
CET	Central Europe Time, as UTC + 1 hour
EET	Eastern Europe Time, as UTC + 2 hours
United States and Canada	
EST, EST5EDT	Eastern Standard Time, as UTC - 5 hours
CST, CST6CDT	Central Standard Time, as UTC - 6 hours
MST, MST7MDT	Mountain Standard Time, as UTC - 7 hours
PST, PST8PDT	Pacific Standard Time, as UTC - 8 hours
HST	Hawaiian Standard Time, as UTC - 10 hours

Australia Time Zones

Note Enter the country and city together with a forward slash (/) between them for the Australia time zone; for example, Australia/Currie.

Table 2: Table 4-2 Australia Time Zones (Continued)

Australia			
Australian Capital Territory (ACT)	Adelaide	Brisbane	Broken_Hill
Canberra	Currie	Darwin	Hobart

Australia			
Lord_Howe	Lindeman	Lord Howe Island (LHI)	Melbourne
North	New South Wales (NSW)	Perth	Queensland
South	Sydney	Tasmania	Victoria
West	Yancowinna		

Asia Time Zones

Note The Asia time zone includes cities from East Asia, Southern Southeast Asia, West Asia, and Central Asia. Enter the region and city or country together separated by a forward slash (/); for example, Asia/Aden.

Table 3: Table 4-3 Asia Time Zones (Continued)

Asia			
Aden	Almaty	Amman	Anadyr
Aqtau	Aqtobe	Ashgabat	Ashkhabad
Baghdad	Bahrain	Baku	Bangkok
Beirut	Bishkek	Brunei	Calcutta
Choibalsan	Chongqing	Columbo	Damascus
Dhakar	Dili	Dubai	Dushanbe
Gaza	Harbin	Hong_Kong	Hovd
Irkutsk	Istanbul	Jakarta	Jayapura
Jerusalem	Kabul	Kamchatka	Karachi
Kashgar	Katmandu	Kuala_Lumpur	Kuching
Kuwait	Krasnoyarsk		

cls

To clear the contents of terminal screen, use the **cls** command in configuration mode.

cls

Syntax Description This command has no keywords and arguments.

Command Default No default behavior or values.

Command Modes Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines **cls** is a hidden command. Although **cls** is available in Cisco ISE, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line.

Example

The following example shows how to clear the contents of the terminal:

```
ise/admin(config)# cls
ise/admin#
```

conn-limit

To configure the limit of incoming TCP connections from a source IP address, use the **conn-limit** command in configuration mode. To remove this function, use the **no** form of this command.

Syntax Description

<1-2147483647>	Number of TCP connections.
ip	(Optional). Source IP address to apply the TCP connection limit.
mask	(Optional). Source IP mask to apply the TCP connection limit.
port	(Optional). Destination port number to apply the TCP connection limit.

Command Default No default behavior or values.

Command Modes Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines Use this **conn-limit** command for more than 99 TCP connections. For less than 100 connections, the system displays the following warning:

```
% Warning: Setting a small conn-limit may adversely affect system performance
```

Example

```
ise/admin(config)# conn-limit 25000 ip 77.10.122.133 port 22
ise/admin(config)# end
ise/admin
```

do

To execute an EXEC-system level command from configuration mode or any configuration submode, use the **do** command in any configuration mode.

do *EXEC commands*

Syntax Description

EXEC commands	Specifies to execute an EXEC-system level command (see Table 4: Table 4-4 Command Options for Do Command (Continued)).

Table 4: Table 4-4 Command Options for Do Command (Continued)

Command	Description
application configure	Configures a specific application.
application install	Installs a specific application.
application remove	Removes a specific application.
application reset-config	Resets application configuration to factory defaults.
application reset-passwd	Resets application password for a specified user.
application start	Starts or enables a specific application
application stop	Stops or disables a specific application.
application upgrade	Upgrades a specific application.
backup	Performs a backup (Cisco ISE and Cisco ADE OS) and places the backup in a repository.
backup-logs	Performs a backup of all logs in the Cisco ISE server to a remote location.
clock	Sets the system clock in the Cisco ISE server.
configure	Enters configuration mode.
copy	Copies any file from a source to a destination.
debug	Displays any errors or events for various command situations; for example, backup and restore, configuration, copy, resource locking, file transfer, and user management.

Command	Description
delete	Deletes a file in the Cisco ISE server.
dir	Lists files in the Cisco ISE server.
forceout	Forces the logout of all sessions of a specific Cisco ISE node user.
halt	Disables or shuts down the Cisco ISE server.
mkdir	Creates a new directory.
nslookup	Queries the IPv4 or IPv6 address or hostname of a remote system.
password	Updates the CLI account password.
patch	Installs a Patch Bundle or uninstalls an Application patch.
ping	Determines the IPv4 address or hostname of a remote system.
ping6	Determines the IPv6 address of a remote system.
reload	Reboots the Cisco ISE server.
restore	Performs a restore and retrieves the backup out of a repository.
rmdir	Removes an existing directory.
show	Provides information about the Cisco ISE server.
ssh	Starts an encrypted session with a remote system.
tech	Provides Technical Assistance Center (TAC) commands.
telnet	Establishes a Telnet connection to a remote system.
terminal length	Sets terminal line parameters.
terminal session-timeout	Sets the inactivity timeout for all terminal sessions.
terminal session-welcome	Sets the welcome message on the system for all terminal sessions.
terminal terminal-type	Specifies the type of terminal connected to the current line of the current session.
traceroute	Traces the route of a remote IP address.

Command	Description
undebug	Disables the output (display of errors or events) of the debug command for various command situations; for example, backup and restore, configuration, copy, resource locking, file transfer, and user management.
write	Erases the startup configuration that forces to run the setup utility and prompt the network configuration, copies the running configuration to the startup configuration, displays the running configuration on the console.

Command Default

No default behavior or values.

Command Modes

Configuration (config)# or any configuration submode (config-GigabitEthernet)# and (config-Repository)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

Use this **do** command to execute EXEC commands (such as **show**, **clear**, and **debug** commands) while configuring the Cisco ISE server. After the EXEC command is executed, the system will return to configuration mode you were using.

Example

```
ise/admin(config)# do show run
Generating configuration...
!
hostname ise
!
ip domain-name cisco.com
!
interface GigabitEthernet 0
  ip address 172.23.90.113 255.255.255.0
  ipv6 address autoconfig
!
ip name-server 171.70.168.183
!
ip default-gateway 172.23.90.1
!
clock timezone EST
!
ntp server time.nist.gov
!
username admin password hash $1$JbbHvKVG$xMZ/XL4tH15Knf.FfcZZr. role admin
!
service sshd
!
backup-staging-url nfs://loc-filer02a:/vol/local1/private1/jdoe
!
password-policy
  lower-case-required
  upper-case-required
  digit-required
```

```
  no-username
  disable-cisco-passwords
  min-password-length 6
!
logging localhost
logging loglevel 6
!
--More--
ise/admin(config)#
```

end

To end the current configuration session and return to EXEC mode, use the **end** command in configuration mode.

This command has no keywords and arguments.

end

Command Default No default behavior or values.

Command Modes Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines This command brings you back to EXEC mode regardless of what configuration mode or submode you are in.

Use this command when you finish configuring the system and you want to return to EXEC mode to perform verification steps.

Example

```
ise/admin(config)# end
ise/admin#
```

exit

To exit any configuration mode to the next-highest mode in the CLI mode hierarchy, use the **exit** command in configuration mode.

exit

This command has no keywords and arguments.

Command Default No default behavior or values.

Command Modes Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

The **exit** command is used in the Cisco ISE server to exit the current command mode to the next highest command mode in the CLI mode hierarchy.

For example, use the **exit** command in configuration mode to return to EXEC mode. Use the **exit** command in the configuration submodes to return to configuration mode. At the highest level, EXEC mode, the **exit** command exits EXEC mode and disconnects from the Cisco ISE server.

Example

```
ise/admin(config)# exit
ise/admin#
```

hostname

To set the hostname of the system, use the **hostname** command in configuration mode.

hostname *hostname*

Syntax Description

hostname	Name of the host. Supports up to 19 alphanumeric characters and an underscore (_). The hostname must begin with a character that is not a space.

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

Note If 'Ctrl-C' is issued during the CLI configuration change of 'hostname' command, the system might end up in a state where some application components might have the old hostname while some components might use the new hostname. This will bring the Cisco ISE node to a non-working state.

The workaround for this issue is to run the 'hostname' configuration command again to set the hostname to the desired value.

You can use the **hostname** command to change the current hostname. A single instance type of command, **hostname** only occurs once in the configuration of the system. The hostname must contain one argument; otherwise, an error occurs.

When you update the hostname of the Cisco ISE server with this command, the following warning message is displayed:

```
 % Warning:  Updating the hostname will cause any certificate using the old
%           hostname to become invalid. Therefore, a new self-signed
%           certificate using the new hostname will be generated now for
%           use with HTTPs/EAP.  If CA-signed certs were used on this node,
%           please import them with the correct hostname. In addition,
%           if this ISE node will be joining a new
%           Active Directory domain, please leave your current Active
%           Directory domain before proceeding. If this ISE node is already
%           joined to an Active Directory domain, then it is strongly advised
%           to rejoin all currently joined join-points in order to
%           avoid possible mismatch between current and previous
%           hostname and joined machine account name.
```

Example

```
ise/admin(config)# hostname new-hostname
% Changing the hostname will cause ISE services to restart
Continue with hostname change?  Y/N [N]: y
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Log Processor...
ISE Identity Mapping Service is disabled
ISE pxGrid processes are disabled
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE Profiler Database...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE AD Connector...
Stopping ISE Database processes...
ISE Database processes already running, PID: 9651
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler Database...
Starting ISE Application Server...
Starting ISE Certificate Authority Service...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE AD Connector...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise-1/admin#
```

icmp echo

To configure the Internet Control Message Protocol (ICMP) echo responses, use the **icmp echo** command in configuration mode.

icmp echo {*off* | *on*}

Syntax Description

echo	Configures ICMP echo response.
off	Disables ICMP echo response
on	Enables ICMP echo response.

Command Default

The system behaves as if the ICMP echo response is on (enabled).

Command Modes Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines Use this **icmp echo** to turn on or turn off ICMP echo response.

Example

```
ise/admin(config)# icmp echo off
ise/admin(config)#
```

interface

To configure an interface type and enter the interface configuration mode, use the **interface** command in configuration mode. This command does not have a **no** form.

Note VMware virtual machine may have a number of interfaces available that depends on how many network interfaces (NIC) are added to the virtual machine.

interface GigabitEthernet {*0* | *1* | *2* | *3*}

Syntax Description

GigabitEthernet	Configures the Gigabit Ethernet interface.
0 - 3	Number of the Gigabit Ethernet port to configure.

Note After you enter the Gigabit Ethernet port number in the **interface** command, you enter the config-GigabitEthernet configuration submode (see the following Syntax Description).

Syntax Description

do	EXEC command. Allows you to perform any EXEC commands in this mode.
end	Exits the config-GigabitEthernet submode and returns you to EXEC mode.
exit	Exits the config-GigabitEthernet configuration submode.
ip	Sets the IP address and netmask for the Gigabit Ethernet interface.
ipv6	Configures IPv6 autoconfiguration address and IPv6 address from DHCPv6 server.

no	Negates the command in this mode. Two keywords are available: • ip—Sets the IP address and netmask for the interface. • ipv6—Sets the IPv6 address for the interface. • shutdown—Shuts down the interface.
shutdown	Shuts down the interface.

Command Default No default behavior or values.

Command Modes Interface configuration (config-GigabitEthernet)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines You can use the **interface** command to configure the interfaces to support various requirements.

Example

```
ise/admin(config)# interface GigabitEthernet 0
ise/admin(config-GigabitEthernet)#
```

ip address

To set the IP address and netmask for the GigabitEthernet interface, use the **ip address** command in interface configuration mode.

ip address *ip-address network mask*

To remove an IP address or disable IP processing, use the **no** form of this command.

no ip address

Note You can configure the same IP address on multiple interfaces. You might want to do this to limit the configuration steps that are needed to switch from using one interface to another.

Syntax Description

ip-address	IPv4 address.
network mask	Mask of the associated IP subnet.

Command Default Enabled.

Command Modes Interface configuration (config-GigabitEthernet)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

Note If 'Ctrl-C' is issued during the CLI configuration change of 'ip address' command, in case of IP address change the system may end up in a state where some application components have the old IP address, and some components use the new IP address.

This will bring the Cisco ISE node into a non-working state. The workaround for this is to issue another 'ip address' configuration CLI to set the IP address to the desired value.

Requires exactly one address and one netmask; otherwise, an error occurs.

Example

```
ise/admin(config)# interface GigabitEthernet 1
ise/admin(config-GigabitEthernet)# ip address 209.165.200.227 255.255.255.224
Changing the hostname or IP may result in undesired side effects,
such as installed application(s) being restarted.
........
To verify that ISE processes are running, use the
'show application status ise' command.
ise/admin(config-GigabitEthernet)#
```

ip default-gateway

To define or set a default gateway with an IP address, use the **ip default-gateway** command in configuration mode.

ip default-gateway *ip-address*

To disable this function, use the **no** form of this command.

no ip default-gateway

Syntax Description

default-gateway	Defines a default gateway with an IP address.
ip-address	IP address of the default gateway.

Command Default Disabled.

Command Modes Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines If you enter more than one argument or no arguments at all, an error occurs.

Example

```
ise/admin(config)# ip default-gateway 209.165.202.129
ise/admin(config)#
```

ip domain-name

To define a default domain name that the Cisco ISE server uses to complete hostnames, use the **ip domain-name** command in configuration mode.

ip domain-name *domain-name*

To disable this function, use the **no** form of this command.

no ip domain-name

Syntax Description

domain-name	Defines a default domain name.
domain-name	Default domain name used to complete the hostnames. Contains at least 2 to 64 alphanumeric characters.

Command Default Enabled.

Command Modes Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

Note If 'Ctrl-C' is issued during the CLI configuration change of 'ip domain-name' command, in case of ip domain-name change the system may end up in a state where some application components have the old domain-name and some components use the new domain-name.

This will bring the Cisco ISE node into a non-working state. The workaround for this is to issue another 'ip domain-name' configuration CLI to set the domain name to the desired value.

If you enter more or fewer arguments, an error occurs.

If you update the domain name for the Cisco ISE server with this command, it displays the following warning message:

```
%  Warning: Updating the domain name will cause any certificate
%  using the old domain name to become invalid. Therefore, a new
%  self-signed certificate using the new domain name will be
%  generated now for use with HTTPs/EAP. If CA-signed certificates
%  were used on this node, please import them with the correct domain name.
```

```
%  In addition, if this ISE node will be joining
%  a new Active Directory domain, please leave your current
%  Active Directory domain before proceeding.
```

Example

```
ise/admin(config)# ip domain-name cisco.com
ise/admin(config)#
```

ip host

To associate a host alias and fully qualified domain name (FQDN) string to an ethernet interface such as eth1, eth2, and eth3 other than eth0, use the **ip host** command in global configuration mode.

When Cisco ISE processes an authorization profile redirect URL, it replaces the IP address with the FQDN of the Cisco ISE node.

ip host [*ipv4-address* | *ipv6-address*] [*host-alias* | *FQDN-string*]

To remove the association of host alias and FQDN, use the **no** form of this command.

no ip host [*ipv4-address* | *ipv6-address*] [*host-alias* | *FQDN-string*]

Syntax Description

ipv4-address	IPv4 address of the network interface.
ipv6-address	IPv6 address of the network interface.
host-alias	Host alias is the name that you assign to the network interface.
FQDN-string	Fully qualified domain name (FQDN) of the network interface.

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

Supported IPv6 address formats include:

- Full notation: Eight groups of four hexadecimal digits separated by colons. For example, 2001:0db8:85a3:0000:0000:8a2e:0370:7334
- Shortened notation: Exclude leading zeros in a group; replace groups of zeros with two consecutive colons. For example: 2001:db8:85a3::8a2e:370:7334
- Dotted-quad notation (IPv4-mapped and IPv4 compatible-IPv6 addresses): For example, ::ffff:192.0.2.128

Use the **ip host** command to add host alias and fully qualified domain name (FQDN) string for an IP address mapping. It is used to find out the matching FQDN for ethernet interfaces such as eth1, eth2, and eth3. Use the **show running-config** command to view the host alias definitions.

You can provide either the host alias or the FQDN string, or both. If you provide both the values, the host alias must match the first component of the FQDN string. If you provide only the FQDN string, Cisco ISE replaces the IP address in the URL with the FQDN. If you provide only the host alias, Cisco ISE combines the host alias with the configured IP domain name to form a complete FQDN, and replaces the IP address of the network interface in the URL with the FQDN.

Example 1

```
ise/admin(config)# ip host 172.21.79.96 ise1 ise1.cisco.com
Host alias was modified. You must restart ISE for change to take effect.
Do you want to restart ISE now? (yes/no) yes
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Application Server...
Stopping ISE Profiler DB...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE Database processes...
Starting ISE Database processes...
Stopping ISE Database processes...
Starting ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler DB...
Starting ISE Application Server...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE Monitoring & Troubleshooting Log Processor...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin(config)#
```

Example 2

```
ise/admin(config)# ipv6 host 2001:db8:cc00:1::1 ise1 ise1.cisco.com
Host alias was modified. You must restart ISE for change to take effect.
Do you want to restart ISE now? (yes/no) yes
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Application Server...
Stopping ISE Profiler DB...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE Database processes...
Starting ISE Database processes...
Stopping ISE Database processes...
Starting ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler DB...
Starting ISE Application Server...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE Monitoring & Troubleshooting Log Processor...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin(config)#
```

ip name-server

To set the Domain Name Server (DNS) for use during a DNS query, use the **ip name-server** command in configuration mode. You can configure one to three DNS servers.

ip name-server *ip-address* {*ip-address**}

To disable this function, use the **no** form of this command.

no ip name-server *ip-address* {*ip-address**}

Note Using the **no** form of this command removes all the name servers from the configuration. The **no** form of this command and one of the IP names removes only that name server.

Syntax Description

name-server	Configures the IP addresses of the name server(s).
ip-address	Address of a name server.
*ip-address**	(Optional). IP addresses of additional name servers. **Note** You can configure three IPv4 addresses and one IPv6 address in the name server.

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

The first name server that is added with the **ip name-server** command occupies the first position and the system uses that server first to resolve the IP addresses.

You can add name servers to the system using IPv4 or IPv6 addresses. You can configure one to three IPv4 or IPv6 addresses through a single command. If you have already configured the system with four name servers, you must remove at least one server to add additional name servers.

To place a name server in the first position so that the subsystem uses it first, you must remove all name servers with the **no** form of this command before you proceed.

Note If you modified this setting for AD connectivity, you must restart Cisco ISE for the changes to take effect. Also, ensure that all DNS servers configured in Cisco ISE are able to resolve all relevant AD DNS records. If the configured AD join points are not correctly resolved after the DNS settings are changed, you must manually perform the Leave operation and re-join the AD join point.

Example 1

```
ise/admin(config)# ip name-server ?
<A.B.C.D>|<valid IPv6 format>  Primary DNS server IP address
<A.B.C.D>|<valid IPv6 format>  DNS server 2 IP address
<A.B.C.D>|<valid IPv6 format>  DNS server 3 IP address

ise/admin(config)# ip name-server
```

Example 2

You can see the following output after you configure the IP name server.

```
ise/admin# show run | in name-server
ip name-server 171.70.168.183 171.68.226.120
3201:db8:0:20:f41d:eee:7e66:4eba
ise/admin#
```

Example 3

```
ise/admin(config)# ip name-server ?
ip name-server 10.126.107.120 10.126.107.107 10.106.230.244
DNS Server was modified. If you modified this setting for AD connectivity, you must restart
 ISE for the change to take effect.
Do you want to restart ISE now? (yes/no)
```

ip route

To configure the static routes, use the **ip route** command in configuration mode. To remove static routes, use the **no** form of this command.

ip route *prefix mask* **gateway** *ip-address*

no ip route *prefix mask*

Syntax Description

prefix	IP route prefix for the destination.
mask	Prefix mask for the destination.
ip-address	IP address of the next hop that can be used to reach that network.

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

Static routes are manually configured, which makes them inflexible (they cannot dynamically adapt to network topology changes), but extremely stable. Static routes optimize bandwidth utilization, because no routing updates need to be sent to maintain them. They also make it easy to enforce routing policy.

While the **ip route** command can be used to define static routes on individual Cisco ISE node, this command is enhanced to define a default route for each interface and reduce the effects of asymmetrical IP forwarding, which is inherent in multi-interface IP nodes.

When a single default route is configured on a multi-interface node, all IP traffic received from any of the node's IP interfaces is routed to the next hop of the default gateway that produces asymmetrical IP forwarding. Configuring multiple default routes on the Cisco ISE node eliminates the effects of asymmetric forwarding.

The following example describes how to configure multiple default routes:

Consider the following interface configuration on Cisco ISE node eth0, eth1, eth2, and eth3 interfaces respectively:

```
ISE InterfaceIPNetworkGateway
192.168.114.10 192.168.114.0 192.168.114.1
192.168.115.10 192.168.115.0 192.168.115.1
192.168.116.10 192.168.116.0 192.168.116.1
192.168.117.10 192.168.117.0 192.168.117.1
```

The **ip route** command is used here to define default routes for each interface.

```
ise/admin(config)# ip route 0.0.0.0 0.0.0.0 192.168.114.1
ise/admin(config)# ip route 0.0.0.0 0.0.0.0 192.168.115.1
ise/admin(config)# ip route 0.0.0.0 0.0.0.0 192.168.116.1
ise/admin(config)# ip route 0.0.0.0 0.0.0.0 192.168.117.1
ise/admin(config)# ip default-gateway 192.168.118.1
```

Note The "ip default-gateway" shown above is the route of last resort for all interfaces.

The **show ip route** command displays the output of the static routes created using the **ip route** command (default routes and non-default routes) and system created routes including the one configured using "ip default gateway" command. It displays the outgoing interface for each of the routes.

Note When you change the IP address of an interface and if any static route becomes unreachable due to an unreachable gateway, the static route gets deleted from the running configuration. The console displays the route that has become unreachable.

Example 2

```
ise/admin(config)# ip route 192.168.0.0 255.255.0.0 gateway 172.23.90.2
ise/admin(config)#
```

ipv6 address autoconfig

Command Default No default behavior or values.

Command Modes Interface configuration (config-GigabitEthernet)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines IPv6 stateless autoconfiguration has the security downfall of having predictable IP addresses. This downfall is resolved with privacy extensions. You can verify that the privacy extensions feature is enabled by using the **show interface** command.

Example

```
ise/admin(config-GigabitEthernet)# ipv6 address autoconfig
ise/admin(config)#
```

Configuring IPv6 Auto Configuration

To enable IPv6 stateless autoconfiguration, use the **interface GigabitEthernet 0** command in Interface configuration mode:

```
ise/admin# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ise/admin(config)# interface GigabitEthernet 0
ise/admin(config)# (config-GigabitEthernet)# ipv6 address autoconfig
ise/admin(config)# (config-GigabitEthernet)# end
ise/admin#
```

When IPv6 autoconfiguration is enabled, the running configuration shows the interface settings similar to the following:

```
!
interface GigabitEthernet 0
  ip address 172.23.90.116 255.255.255.0
  ipv6 address autoconfig
!
```

You can use the **show interface GigabitEthernet 0** command to display the interface settings. In the example below, you can see that the interface has three IPv6 addresses. The first address (starting with 3ffe) is obtained using the stateless autoconfiguration.

For the stateless autoconfiguration to work, you must have IPv6 route advertisement enabled on that subnet. The next address (starting with fe80) is a link-local address that does not have any scope outside the host.

You will always see a link local address regardless of the IPv6 autoconfiguration or DHCPv6 configuration. The last address (starting with 2001) is obtained from a IPv6 DHCP server.

```
ise/admin# show interface GigabitEthernet 0
eth0      Link encap:Ethernet  HWaddr 00:0C:29:AF:DA:05
          inet addr:172.23.90.116  Bcast:172.23.90.255  Mask:255.255.255.0
```

```
          inet6 addr: 3ffe:302:11:2:20c:29ff:feaf:da05/64 Scope:Global
          inet6 addr: fe80::20c:29ff:feaf:da05/64 Scope:Link
          inet6 addr: 2001:558:ff10:870:8000:29ff:fe36:200/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:77848 errors:0 dropped:0 overruns:0 frame:0
          TX packets:23131 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10699801 (10.2 MiB)  TX bytes:3448374 (3.2 MiB)
          Interrupt:59 Base address:0x2000
ise/admin#
```

Verifying the Privacy Extensions Feature

To verify that the privacy extensions feature is enabled, you can use the **show interface GigabitEthernet 0** command. You can see two autoconfiguration addresses: one address is without the privacy extensions, and the other is with the privacy extensions.

In the example below, the MAC is 3ffe:302:11:2:20c:29ff:feaf:da05/64 and the non-RFC3041 address contains the MAC, and the privacy-extension address is 302:11:2:9d65:e608:59a9:d4b9/64.

The output appears similar to the following:

```
ise/admin# show interface GigabitEthernet 0
eth0      Link encap:Ethernet  HWaddr 00:0C:29:AF:DA:05
          inet addr:172.23.90.116  Bcast:172.23.90.255  Mask:255.255.255.0
          inet6 addr: 3ffe:302:11:2:9d65:e608:59a9:d4b9/64 Scope:Global
          inet6 addr: 3ffe:302:11:2:20c:29ff:feaf:da05/64 Scope:Global
          inet6 addr: fe80::20c:29ff:feaf:da05/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:60606 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2771 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9430102 (8.9 MiB)  TX bytes:466204 (455.2 KiB)
          Interrupt:59 Base address:0x2000
ise/admin#
```

ipv6 address dhcp

To acquire an IPv6 address on an interface from the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server, use the **ipv6 address dhcp** command in the interface configuration mode. To remove the address from the interface, use the **no** form of this command.

ipv6 address dhcp

Command Default No default behavior or values.

Command Modes Interface configuration (config-GigabitEthernet)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

Example

```
ise/admin# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ise/admin(config)# interface GigabitEthernet 1
ise/admin(config-GigabitEthernet)# ipv6 address dhcp
ise/admin(config-GigabitEthernet)# end
ise/admin#
```

When IPv6 DHCP is enabled, the running configuration shows the interface settings similar to the following:

```
!
interface GigabitEthernet 1
  ipv6 address dhcp
  ipv6 enable
!
```

Note The IPv6 stateless autoconfiguration and IPv6 address DHCP are not mutually exclusive. It is possible to have both IPv6 stateless autoconfiguration and IPv6 address DHCP on the same interface.

You can use the **show interface** command to display what IPv6 addresses are in use for a particular interface.

When both the IPv6 stateless autoconfiguration and IPv6 address DHCP are enabled, the running configuration shows the interface settings similar to the following:

```
!
interface GigabitEthernet 1
    ipv6 address dhcp
    ipv6 address autoconfig
    ipv6 enable
!
```

kron occurrence

To schedule one or more Command Scheduler commands to run at a specific date and time or a recurring level, use the **kron occurrence** command in configuration mode. To delete this schedule, use the **no** form of this command.

kron occurrence *occurrence-name*

Syntax Description

occurrence	Schedules Command Scheduler commands.
occurrence-name	Name of the occurrence. Supports up to 80 alphanumeric characters. (See the following note and Syntax Description.)

Note After you enter the *occurrence-name* in the **kron occurrence** command, you enter the config-Occurrence configuration submode (see the following Syntax Description).

Syntax Description

at	Identifies that the occurrence is to run at a specified calendar date and time. Usage: at [*hh:mm*] [*day-of-week* | *day-of-month* | *month day-of-month*].
do	EXEC command. Allows you to perform any EXEC commands in this mode.
end	Exits the kron-occurrence configuration submode and returns you to EXEC mode.
exit	Exits the kron-occurrence configuration mode.
no	Negates the command in this mode. Three keywords are available: • at—Usage: at [hh:mm] [day-of-week | day-of-month | month day-of-month]. • policy-list—Specifies a policy list to be run by the occurrence. Supports up to 80 alphanumeric characters. • recurring—Execution of the policy lists should be repeated.
policy-list	Specifies a Command Scheduler policy list to be run by the occurrence.
recurring	Identifies that the occurrences run on a recurring basis. **Note** If kron occurrence is not recurring, then the kron occurrence configuration for the scheduled backup is removed after it has run.

Command Default

No default behavior or values.

Command Modes

Configuration (config-Occurance)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

Use the **kron occurrence** and **policy-list** commands to schedule one or more policy lists to run at the same time or interval.

Use the **kron policy-list** command in conjunction with the **cli** command to create a Command Scheduler policy that contains the EXEC CLI commands to be scheduled to run in the Cisco ISE server at a specified time.

Note When you run the **kron** command, backup bundles are created with a unique name (by adding a time stamp) to ensure that the files do not overwrite each other.

Note It is recommended that you schedule configuration or monitoring backups through the GUI by using the **Administration > System > Backup and Restore** page.

Example 1: Weekly Backup

```
ise/admin(config)# kron occurrence WeeklyBackup
ise/admin(config-Occurrence)# at 14:35 Monday
ise/admin(config-Occurrence)# policy-list SchedBackupPolicy
ise/admin(config-Occurrence)# recurring
ise/admin(config-Occurrence)# exit
ise/admin(config)#
```

Example 2: Daily Backup

```
ise/admin(config)# kron occurrence DailyBackup
ise/admin(config-Occurrence)# at 02:00
ise/admin(config-Occurrence)# exit
ise/admin(config)#
```

Example 3: Weekly Backup

```
ise/admin(config)# kron occurrence WeeklyBackup
ise/admin(config-Occurrence)# at 14:35 Monday
ise/admin(config-Occurrence)# policy-list SchedBackupPolicy
ise/admin(config-Occurrence)# no recurring
ise/admin(config-Occurrence)# exit
ise/admin(config)#
```

kron policy-list

To specify a name for a Command Scheduler policy and enter the kron-Policy List configuration submode, use the **kron policy-list** command in configuration mode. To delete a Command Scheduler policy, use the **no** form of this command.

kron policy-list *list-name*

Syntax Description

policy-list	Specifies a name for Command Scheduler policies.
list-name	Name of the policy list. Supports up to 80 alphanumeric characters.

Note After you enter the list-name in the **kron policy-list** command, you enter the config-Policy List configuration submode (see the following Syntax Description).

Syntax Description

cli	Command to be executed by the scheduler. Supports up to 80 alphanumeric characters.
do	EXEC command. Allows you to perform any EXEC commands in this mode.
end	Exits from the config-Policy List configuration submode and returns you to EXEC mode.
exit	Exits this submode.
no	Negates the command in this mode. One keyword is available: • cli—Command to be executed by the scheduler.

Command Default No default behavior or values.

Command Modes Configuration (config-Policy List)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines Use the **kron policy-list** command in conjunction with the **cli** command to create a Command Scheduler policy that contains the EXEC CLI commands to be scheduled to run on the ISE server at a specified time. Use the **kron occurrence** and **policy list** commands to schedule one or more policy lists to run at the same time or interval.

Note You cannot use the **kron policy-list** command to schedule configuration and operational data backups from the CLI. You can schedule these backups from the Cisco ISE Admin portal.

Example

```
ise/admin(config)# kron policy-list BackupLogs
ise/admin(config-Policy List)# cli backup-logs ScheduledBackupLogs repository SchedBackupRepo
 encryption-key plain xyzabc
ise/admin(config-Policy List)# exit
ise/admin(config)#
```

logging

To configure the log level, use the **logging** command in configuration mode.

logging loglevel {*0* | *1* | *2* | *3* | *4* | *5* | *6* | *7*}

To disable this function, use the **no** form of this command.

no logging

Syntax Description

loglevel	The command to configure the log level for the logging command.
0-7	The desired priority level to set the log messages. Priority levels are (enter the number for the keyword): • 0-emerg—Emergencies: System unusable. • 1-alert—Alerts: Immediate action needed. • 2-crit—Critical: Critical conditions. • 3-err—Error: Error conditions. • 4-warn—Warning: Warning conditions. • 5-notif—Notifications: Normal but significant conditions. • 6-inform—(Default) Informational messages. • 7-debug—Debugging messages.

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

This command requires the **loglevel** keyword.

Example

```
ise/admin(config)# logging loglevel 0
ise/admin(config)#
```

max-ssh-sessions

To configure the maximum number of concurrent command-line interface (CLI) sessions for each of the node in the distributed deployment, use the **max-ssh-sessions** command in configuration mode.

max-ssh-sessions {*0* | *1* | *2* | *3* | *4* | *5* | *6* | *7* | *8* | *9* | *10*}

Syntax Description

1-10	Number of concurrent SSH sessions. The default is 5.

Command Default

The default number of maximum concurrent CLI sessions allowed is set to five from the Cisco ISE Admin portal.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

The max-ssh-sessions parameter is not configurable from the command-line interface. The maximum number of active CLI sessions is replicated from the primary administration ISE Admin portal.

When you exceed the maximum number of CLI sessions, the “Maximum active ssh sessions reached” message is displayed in the command-line interface closing that session, and you can see the “Not connected - press Enter or Space to connect” message at the bottom.

You can log in to the CLI through the console and use the **forceout username** command to log out users to reduce the active SSH sessions.

The navigation path to configure the maximum number of command-line interface (CLI) sessions is in the Session tab of the Cisco ISE Admin portal in the following location: **Administration** > **System** > **Admin Access** > **Settings** > **Access** .

ntp

To specify an NTP configuration, use the **ntp** command in configuration mode with **authenticate**, **authentication-key**, **server**, and **trusted-key** commands.

ntp authenticate

ntp authentication-key <*key id*> **md5hash** | **plain**<*key value*>

ntp server {*ip-address* | *hostname*} *key* <*peer key number*>

ntp trusted-key <*key*>

no ntp server

Syntax Description

authenticate	Enables authentication of all time sources.
authentication-key	Specifies authentication keys for trusted time sources.

server	Specifies NTP server to use.
trusted-key	Specifies key numbers for trusted time sources.

Command Default

None

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

Use the **ntp** command to specify an NTP configuration.

To terminate NTP service on a device, you must enter the **no ntp** command with keywords or arguments such as **authenticate**, **authentication-key**, **server,** and **trusted-key**. For example, if you previously issued the **ntp server** command, use the **no ntp** command with **server**.

Example

```
ise/admin(config)# ntp ?
  authenticate        Authenticate time sources
  authentication-key  Authentication key for trusted time sources
  server              Specify NTP server to use
  trusted-key         Key numbers for trusted time sources
ise/admin(config)#
ise/admin(config)# no ntp server
ise/admin(config)# do show ntp
% no NTP servers configured
ise/admin(config)#
```

ntp authenticate

To enable authentication of all time sources, use the **ntp authenticate** command. Time sources without the NTP authentication keys will not be synchronized.

To disable this capability, use the **no** form of this command.

ntp authenticate

Syntax Description

authenticate	Enables authentication of all time sources.

Command Default

None

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

Use the **ntp authenticate** command to enable authentication of all time sources. This command is optional and authentication will work even without this command.

If you want to authenticate in a mixed mode where only some servers require authentication, that is, only some servers need to have keys configured for authentication, then this command should not be executed.

Example

```
ise/admin(config)# ntp authenticate
ise/admin(config)#
```

ntp authentication-key

To specify an authentication key for a time source, use the **ntp authentication-key** command in configuration command with a unique identifier and a key value.

ntp authentication-key *key id* **md5 hash | plain** *key value*

To disable this capability, use the **no** form of this command.

no ntp authentication-key

Syntax Description

authentication-key	Configures authentication keys for trusted time sources.
key id	The identifier that you want to assign to this key. Supports numeric values from 1–65535.
md5	The encryption type for the authentication key.
hash	Hashed key for authentication. Specifies an encrypted (hashed) key that follows the encryption type. Supports up to 40 characters.
plain	Plaintext key for authentication. Specifies an unencrypted plaintext key that follows the encryption type. Supports up to 15 characters.
key value	The key value in the format matching either **md5 plain** | **hash**, above.

Command Default

None

Command Modes

Configuration (config)#.

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

Use the **ntp authentication-key** command to set up a time source with an authentication key for NTP authentication and specify its pertinent key identifier, key encryption type, and key value settings. Add this key to the trusted list before you add this key to the **ntp server** command.

Time sources without the NTP authentication keys that are added to the trusted list will not be synchronized.

Note The **show running-config** command will always show keys that are entered in Message Digest 5 (MD5) plain format converted into hash format for security. For example, **ntp authentication-key** 1 **md5 hash***ee18afc7608ac7ecdbeefc5351ad118bc9ce1ef3*.

Example 1

```
ise/admin# configure
ise/admin(config)#
ise/admin(config)# ntp authentication-key 1 md5 plain SharedWithServe
ise/admin(config)# ntp authentication-key 2 md5 plain SharedWithServ
ise/admin(config)# ntp authentication-key 3 md5 plain SharedWithSer
```

Example 2

```
ise/admin(config)# no ntp authentication-key 3
(Removes authentication key 3.)
```

Example 3

```
ise/admin(config)# no ntp authentication-key
(Removes all authentication keys.)
```

ntp server

To allow for software clock synchronization by the NTP server for the system, use the **ntp server** command in configuration mode. Allows up to three servers each with a key in a separate line. The key is an optional parameter but the key is required for NTP authentication.

The Cisco ISE always requires a valid and reachable NTP server.

Although key is an optional parameter, it must be configured if you need to authenticate an NTP server.

To disable this capability, use the **no** form of this command only when you want to remove an NTP server and add another one.

ntp server {*ip-address* | *hostname*} *key <peer key number>*

Syntax Description

server	Allows the system to synchronize with a specified server.
ip-address | *hostname*	IPv4 or address or hostname of the server providing the clock synchronization. Arguments are limited to 255 alphanumeric characters.

autokey	Specifies that public-key authentication should be used for NTP server. If you choose this option, ensure that you import the NTP server's public key in to the Cisco ISE node using the **crypto** command.
key	(Optional). Peer key number. Supports up to 65535 numeric characters. This key needs to be defined with a key value, by using the **ntp authentication-key** command, and also needs to be added as a trusted-key by using the **ntp trusted-key** command. For authentication to work, the key and the key value should be the same as that which is defined on the actual NTP server.

Command Default

No servers are configured by default.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

Use this **ntp server** command with a trusted key if you want to allow the system to synchronize with a specified server.

The key is optional, but it is required for NTP authentication. Define this key in the **ntp authentication-key** command first and add this key to the **ntp trusted-key** command before you can add it to the **ntp server** command.

The **show ntp** command displays the status of synchronization. If none of the configured NTP servers are reachable or not authenticated (if NTP authentication is configured), then this command displays synchronization to local with the least stratum.

If an NTP server is not reachable or is not properly authenticated, then its reach as per this command statistics will be 0.

To define an NTP server configuration and authentication keys from the Cisco ISE Admin portal, see the System Time and NTP Server Settings section in the *Cisco Identity Services Engine Administration Guide*.

Note This command gives conflicting information during the synchronization process. The synchronization process can take up to 20 minutes to complete.

Configuring Trusted Keys for NTP Server Authentication

Verifying the Status of Synchronization

To check the status of synchronization, use the **show ntp** command.

Example 1

```
ise/admin# show ntp
Primary NTP   : ntp.esl.cisco.com
Secondary NTP : 171.68.10.80
Tertiary NTP : 171.68.10.150
synchronised to local net at stratum 11
   time correct to within 448 ms
   polling server every 64 s
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*127.127.1.0     .LOCL.          10 l   46   64   37    0.000    0.000   0.001
 171.68.10.80    .RMOT.          16 u   46   64    0    0.000    0.000   0.000
 171.68.10.150   .INIT.          16 u   47   64    0    0.000    0.000   0.000
Warning: Output results may conflict during periods of changing synchronization.
ise/admin#
```

Example 2

```
ise/admin# show ntp
Primary NTP   : ntp.esl.cisco.com
Secondary NTP : 171.68.10.150
Tertiary NTP : 171.68.10.80
synchronised to NTP server (171.68.10.150) at stratum 3
   time correct to within 16 ms
   polling server every 64 s
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 127.127.1.0     .LOCL.          10 l   35   64  377    0.000    0.000   0.001
+171.68.10.80    144.254.15.122   2 u   36   64  377    1.474    7.381   2.095
*171.68.10.150   144.254.15.122   2 u   33   64  377    0.922   10.485   2.198
Warning: Output results may conflict during periods of changing synchronization.
ise/admin#
```

ntp trusted-key

To add a time source to the trusted list, use the **ntp trusted-key** command with a unique identifier.

ntp trusted-key *key*

To disable this capability, use the **no** form of this command.

no ntp trusted-key

Syntax Description

trusted-key	The identifier that you want to assign to this key.

key	Specifies key numbers for trusted time sources that needs to be defined as NTP authentication keys. Supports up to 65535 numeric characters.

Command Default

None

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

Define this key as an NTP authentication key and then add this key to the trusted list before you add this key to an NTP server. Keys that are added to the trusted list can only be used that allows synchronization by the NTP server with the system.

Example 1

```
ise/admin# configure
ise/admin(config)#
ise/admin(config)# ntp trusted-key 1
ise/admin(config)# ntp trusted-key 2
ise/admin(config)# ntp trusted-key 3
ise/admin(config)# no ntp trusted-key 2
(Removes key 2 from the trusted list).
```

Example 2

```
ise/admin(config)# no ntp trusted-key
(Removes all keys from the trusted list).
```

rate-limit

To configure the limit of TCP/UDP/ICMP packets from a source IP address, use the **rate-limit** command in configuration mode. To remove this function, use the **no** form of this command.

rate-limit 250 ip-address net-mask port

Syntax Description

<1-10000>	An average number of TCP/UDP/ICMP packets per second.
ip-address	Source IP address to apply the packet rate limit.
net-mask	Source IP mask to apply the packet rate limit.
port	Destination port number to apply the packet rate limit.

Command Default

No default behavior or values.

Command Modes Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines None.

Example

```
ise49/admin(config)# rate-limit 4000 ip 20.20.20.20 port 443
% Notice : Actual rate limit rounded up by iptables to 5000 per second
ise49/admin(config)# do show running-config | incl rate
rate-limit 5000 ip 20.20.20.20 port 443
ise49/admin(config)#
ise49/admin(config)# rate-limit 6000 ip 10.10.10.10 port 443
% Notice : Actual rate limit rounded up by iptables to 10000 per second
ise49/admin(config)# do show running-config | incl rate
rate-limit 10000 ip 10.10.10.10 port 443
rate-limit 5000 ip 20.20.20.20 port 443
ise49/admin(config)#
```

password-policy

To enable or configure the passwords on the system, use the **password-policy** command in configuration mode. To disable this function, use the **no** form of this command.

password-policy *options*

Note The **password-policy** command requires a policy option (see Syntax Description). You must enter the **password-expiration-enabled** command before the other password-expiration commands.

Note After you enter the **password-policy** command, you can enter the config-password-policy configuration submode.

Syntax Description

digit-required	Requires a digit in user passwords.
disable-cisco-password	Disables the ability to use the word Cisco or any combination as the password.
disable-repeat-chars	Disables the ability of the password to contain more than four identical characters.
do	Exec command.
end	Exit from configure mode.

exit	Exit from this submode.
lower-case-required	Requires a lowercase letter in user passwords.
min-password-length	Minimum number of characters for a valid password. Supports up to 40 characters.
no	Negate a command or set its defaults.
no-previous-password	Prevents users from reusing a part of their previous password.
no-username	Prohibits users from reusing their username as a part of a password.
password-delta	Number of characters to be different from the old password.
password-expiration-days	Number of days until a password expires. Supports an integer up to 3650.
password-expiration-enabled	Enables password expiration. **Note** You must enter the **password-expiration-enabled** command before the other password-expiration commands.
password-expiration-warning	Number of days before expiration that warnings of impending expiration begin. Supports an integer up to 3650.
password-lock-enabled	Locks a password after several failures.
password-lock-retry-count	Number of failed attempts before user password locks. Supports an integer up to 20.
password-time-lockout	Sets the time in minutes after which the account lockout is cleared. Supports time values from 5 minutes to 1440 minutes.
special-required	Requires a special character in user passwords.
upper-case-required	Requires an uppercase letter in user passwords.

Command Default

No default behavior or values.

Command Modes

Configuration (config-password-policy)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines None.

Example

```
ise/admin(config)# password-policy
ise/admin(config-password-policy)# password-expiration-days 30
ise/admin(config-password-policy)# exit
ise/admin(config)#
```

repository

To enter the repository submode for configuration of backups, use the **repository** command in configuration mode.

repository *repository-name*

Syntax Description

repository-name	Name of repository. Supports up to 80 alphanumeric characters.

Note After you enter the name of the repository in the **repository** command, you enter the config-Repository configuration submode (see the Syntax Description).

Syntax Description

do	EXEC command. Allows you to perform any of the EXEC commands in this mode.
end	Exits the config-Repository submode and returns you to EXEC mode.
exit	Exits this mode.
no	Negates the command in this mode. Two keywords are available: • url—Repository URL. • user—Repository username and password for access.
url	URL of the repository. Supports up to 300 alphanumeric characters (see Table 4-5).
user	Configure the username and password for access. Supports up to 30 alphanumeric characters for username and supports 15 alphanumeric characters for password. Passwords can consist of the following characters: 0 through 9, a through z, A through Z, -, ., |, @, #, $, %, ^, &, *, (,), +, and =.

Note Server is the server name and path refers to /subdir/subsubdir. Remember that a colon(:) is required after the server for an NFS network server.

Table 5: Table 4-5 URL Keywords (Continued)

Keyword	Source of Destination
URL	Enter the repository URL, including server and path information. Supports up to 80 alphanumeric characters.
cdrom:	Local CD-ROM drive (read only).
disk:	Local storage. You can run the **show repository** repository_name to view all files in the local repository. **Note** All local repositories are created on the /localdisk partition. When you specify disk:// in the repository URL, the system creates directories in a path that is relative to /localdisk. For example, if you entered **disk://backup,** the directory is created at /localdisk/backup.
ftp:	Source or destination URL for an FTP network server. Use url ftp://server/path
http:	Source or destination URL for an HTTP network server (read only).
https:	Source or destination URL for an HTTPS network server (read only).
nfs:	Source or destination URL for an NFS network server. Use url nfs://server:/path
sftp:	Source or destination URL for an SFTP network server. Use url sftp://server/path
tftp:	Source or destination URL for a TFTP network server. Use url tftp://server/path **Note** You cannot use a TFTP repository for performing a Cisco ISE upgrade.

Command Default No default behavior or values.

Command Modes Configuration (config-Repository)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

service

To specify a service to manage, use the **service** command in configuration mode.

service sshd

To disable this function, use the **no** form of this command.

no service

Syntax Description

sshd	Secure Shell Daemon. The daemon program for SSH.
enable	Enables sshd service.
key-exchange-algorithm	Specifies allowable key exchange algorithms for sshd service.
diffie-hellman-group14-sha1	Restricts key exchange algorithm to diffie-hellman-group14-sha1
Loglevel	Specifies the log level of messages from sshd to secure system log. • 1—QUIET • 2—FATAL • 3— ERROR • 4—INFO (default) • 5—VERBOSE • 6—DEBUG • 7—DEBUG1 • 8 —DEBUG2 • 9—DEBUG3

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines None.

Example

```
ise/admin(config)# service sshd
ise/admin(config)# service sshd enable
ise/admin(config)# service sshd key-exchange-algorithm diffie-hellman-group14-sha1
ise/admin(config)# service sshd loglevel 4
ise/admin(config)#
```

shutdown

To shut down an interface, use the **shutdown** command in the interface configuration mode. To disable this function, use the **no** form of this command.

This command has no keywords and arguments.

Command Default No default behavior or values.

Command Modes Configuration (config-GigabitEthernet)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines When you shut down an interface using this command, you lose connectivity to the Cisco ISE appliance through that interface (even though the appliance is still powered on).

However, if you have configured the second interface on the appliance with a different IP and have not shut down that interface, you can access the appliance through that second interface.

To shut down an interface, you can also modify the ifcfg-eth[0,1] file, which is located at /etc/sysconfig/network-scripts, using the ONBOOT parameter:

- Disable an interface: set ONBOOT="no”
- Enable an interface: set ONBOOT="yes"

  You can also use the **no shutdown** command to enable an interface.

Example

```
ise/admin(config)# interface GigabitEthernet 0
ise/admin(config-GigabitEthernet)# shutdown
```

snmp-server community

To set up the community access string to permit access to the Simple Network Management Protocol (SNMP), use the **snmp-server community** command in configuration mode.

snmp-server community *community-string* **ro**

To disable this function, use the **no** form of this command.

no snmp-server

Syntax Description

community	Sets SNMP community string.
community-string	Accessing string that functions much like a password and allows access to SNMP. No blank spaces allowed. Supports up to 255 alphanumeric characters.
ro	Specifies read-only access.

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

The **snmp-server community** command requires a community string and the **ro** argument; otherwise, an error occurs. The SNMP agent on the Cisco ISE provides read-only SNMP-v1 and SNMP-V2c access to the following MIBs:

- SNMPv2-MIB
- RFC1213-MIB
- IF-MIB
- IP-MIB
- IP-FORWARD-MIB
- TCP-MIB
- UDP-MIB
- HOST-RESOURCES-MIB
- ENTITY-MIB-Only 3 MIB variables are supported on the ENTITY-MIB:
  - Product ID: entPhysicalModelName
  - Version ID: entPhysicalHardwareRev
  - Serial Number: entPhysicalSerialNumber
- DISMAN-EVENT-MIB
- NOTIFICATION-LOG-MIB
- CISCO-CDP-MIB

Example

```
ise/admin(config)# snmp-server community new ro
ise/admin(config)#
```

snmp-server contact

To configure the SNMP contact Management Information Base (MIB) value on the system, use the **snmp-server contact** command in configuration mode. To remove the system contact information, use the **no** form of this command.

snmp-server contact *contact-name*

Syntax Description

contact	Identifies the contact person for this managed node. Supports up to 255 alphanumeric characters.
contact-name	String that describes the system contact information of the node. Supports up to 255 alphanumeric characters.

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

None.

Example

```
ise/admin(config)# snmp-server contact Luke
ise/admin(config)#
```

snmp-server location

To configure the SNMP location MIB value on the system, use the **snmp-server location** command in configuration mode. To remove the system location information, use the **no** form of this command.

snmp-server location *location*

Syntax Description

location	Configures the physical location of this managed node. Supports up to 255 alphanumeric characters.
location	String that describes the physical location information of the system. Supports up to 255 alphanumeric characters.

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

Cisco recommends that you use underscores (_) or hyphens (-) between the terms within the *word* string. If you use spaces between terms within the *word* string, you must enclose the string in quotation marks (“).

Example 1

```
ise/admin(config)# snmp-server location Building_3/Room_214
ise/admin(config)#
```

Example 2

```
ise/admin(config)# snmp-server location “Building 3/Room 214”
ise/admin(config)#
```

synflood-limit

To configure a TCP SYN packet rate limit.

synflood-limit ?

Syntax Description

synflood-limit	Average number of TCP SYN packets per second allowed
?	1-2147483647 (Range for TCP SYN packets).

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

Use this **synflood-limit** to configure a TCP SYN packet rate limit.

Example 1

```
ise-pap-sec/admin(config)# synflood-limit ?
```

username

To add a user who can access the Cisco ISE appliance using SSH, use the **username** command in configuration mode. If the user already exists, the password, the privilege level, or both change with this command. To delete the user from the system, use the **no** form of this command.

username *username* **password hash** | **plain** {*password*} **role admin** | **user email** {*email-address*}

For an existing user, use the following command option:

username *username* **password role admin** | **user** {*password*}

Syntax Description

username	Only one word for the username argument. Blank spaces and quotation marks (“) are not allowed. Supports up to 31 alphanumeric characters.
password	Specifies password.
password	Password character length up to 40 alphanumeric characters. You must specify the password for all new users.
hash | **plain**	Type of password. Supports up to 34 alphanumeric characters.
role admin | **user**	Sets the user role and the privilege level for the user.
disabled	Disables the user according to the user’s email address.
email	Sets user’s email address.
email-address	Specifies the user’s email address. For example, user1@mydomain.com.

Command Default

The initial user during setup.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

The **username** command requires that the username and password keywords precede the hash | plain and the admin | user options.

Example 1

```
ise/admin(config)# username admin password hash ###### role admin
ise/admin(config)#
```

Example 2

```
ise/admin(config)# username admin password plain Secr3tp@swd role admin
ise/admin(config)#
```

Example 3

```
ise/admin(config)# username admin password plain Secr3tp@swd role admin email
admin123@mydomain.com
ise/admin(config)#
```

which

To display the contents of commands available in admin CLI, use the **which** command in configuration mode.

which

Syntax Description

This command has no keywords and arguments.

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

which is a hidden command. Although **which** is available in Cisco ISE, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line.

Example

The following example shows the output of **which** :

```
ise/admin(config)# which
[     1].  application  configure<STRING>
[     2].  application  install<STRING><STRING>
[     3].  application  remove<STRING>
[     4].  application  reset-config<STRING>
[     5].  application  reset-passwd<STRING><STRING>
[     6].  application  start<STRING>
[     7].  application  start<STRING>  safe
[     8].  application  stop<STRING>
[     9].  application  upgrade  cleanup
[    10].  application  upgrade  prepare<STRING><STRING>
```

which