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. Configuration changes are saved by default to preserve them during a system reload or power outage.

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.

```
ise32/iseadmin#configure terminal
Entering configuration mode terminal
ise/iseadmin(config)#?
Possible completions:
cdp                CDP Configuration parameters
clock              Configure timezone
conn-limit         Configure a TCP connection limit from source IP
hostname           Configure hostname
icmp               Configure icmp echo requests
identity-store     Configure identity store for CLI users
interface          Configure interface
ip                 Configure IP features
ipv6               Configure IPv6 features
kron               Configure command scheduler
logging            Configure system logging
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            Modify use of network based services
snmp-server        Configure snmp server
synflood-limit     Average number of TCP SYN packets per second allowed
username           User creation
---
do                 Run an operational-mode command
end                Terminate configuration session
exit               Exit from current mode
no                 Negate a command or set its defaults
<cr>
```

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:
  backup    Configure NIC bonding feature
  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)#
```

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.

backup interface

To configure two Ethernet interfaces in to a single virtual interface for high availability (also called as the NIC bonding or NIC teaming feature), use the **backup interface** command in configuration submode. To remove the NIC bonding configuration, use the **no** form of this command. When two interfaces are bonded, the two NICs appear to be a single device with a single MAC address.

The NIC bonding feature in Cisco ISE does not support load balancing or link aggregation features. Cisco ISE supports only the high availability feature of NIC bonding.

The bonding of interfaces ensures that Cisco ISE services are not affected when there is:

- Physical interface failure
- Loss of switch port connectivity (shut or failure)
- Switch line card failure

When two interfaces are bonded, one of the interfaces becomes the primary interface and the other becomes the backup interface. When two interfaces are bonded, all traffic normally flows through the primary interface. If the primary interface fails for some reason, the backup interface takes over and handles all the traffic. The bond takes the IP address and MAC address of the primary interface.

When you configure the NIC bonding feature, Cisco ISE pairs fixed physical NICs to form bonded NICs. The following table outlines which NICs can be bonded together to form a bonded interface.

Cisco ISE Physical NIC Name	Linux Physical NIC Name	Role in Bonded NIC	Bonded NIC Name
Gigabit Ethernet 0	Eth0	Primary	Bond 0
Gigabit Ethernet 1	Eth1	Backup	
Gigabit Ethernet 2	Eth2	Primary	Bond 1
Gigabit Ethernet 3	Eth3	Backup	
Gigabit Ethernet 4	Eth4	Primary	Bond 2
Gigabit Ethernet 5	Eth5	Backup	

The NIC bonding feature is supported on all supported platforms and node personas. The supported platforms include:

- SNS-3400 series appliances - Bond 0 and 1 (Cisco ISE 3400 series appliances support up to 4 NICs)
- SNS-3500 series appliances - Bond 0, 1, and 2
- VMware virtual machines - Bond 0, 1, and 2 (if six NICs are available to the virtual machine)
- Linux KVM nodes - Bond 0, 1, and 2 (if six NICs are available to the virtual machine)

Syntax Description

backup interface	Configures the NIC bonding feature.
GigabitEthernet	Configures the Gigabit Ethernet interface specified as the backup interface.

0 - 3	Number of the Gigabit Ethernet port to configure as the backup interfac

Command Default

No default behavior or values.

Command Modes

Interface configuration submode (config-GigabitEthernet)#

Command History

Release	Modification
2.1.0.474	This command was introduced.

Usage Guidelines

- As Cisco ISE supports up to six Ethernet interfaces, it can have only three bonds, bond 0, bond 1, and bond 2.
- You cannot change the interfaces that are part of a bond or change the role of the interface in a bond. Refer to the above table for information on which NICs can be bonded together and their role in the bond.
- The Eth0 interface acts as both the management interface as well as the runtime interface. The other interfaces act as runtime interfaces.
- Before you create a bond, the primary interface (primary NIC) must be assigned an IP address. The Eth0 interface must be assigned an IPv4 address before you create bond 0. Similarly, before you create bond 1 and 2, Eth2 and Eth4 interfaces must be assigned an IPv4 or IPv6 address, respectively.
- Before you create a bond, if the backup interface (Eth1, Eth3, and Eth5) has an IP address assigned, remove the IP address from the backup interface. The backup interface should not be assigned an IP address.
- You can choose to create only one bond (bond 0) and allow the rest of the interfaces to remain as is. In this case, bond 0 acts as the management interface and runtime interface, and the rest of the interfaces act as runtime interfaces.
- You can change the IP address of the primary interface in a bond. The new IP address is assigned to the bonded interface because it assumes the IP address of the primary interface.
- When you remove the bond between two interfaces, the IP address assigned to the bonded interface is assigned back to the primary interface.
- If you want to configure the NIC bonding feature on a Cisco ISE node that is part of a deployment, you must deregister the node from the deployment, configure NIC bonding, and then register the node back to the deployment.
- If a physical interface that acts as a primary interface in a bond (Eth0, Eth2, or Eth4 interface) has static route configured, the static routes are automatically updated to operate on the bonded interface instead of the physical interface.

Example 1 - Configure NIC Bonding

The following procedure explains how you can configure bond 0 between Eth0 and Eth1 interfaces.

Note If a physical interface that acts as a backup interface (for example, Eth1, Eth3, Eth5 interfaces), is configured with an IP address, you must remove the IP address from the backup interface. The backup interface should not be assigned an IP address.

```
ise/admin# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ise/admin(config)# interface gigabitEthernet 0
ise/admin(config-GigabitEthernet)# backup interface gigabitEthernet 1
Changing backup interface configuration may cause ISE services to restart.
Are you sure you want to proceed? Y/N [N]: Y
Stopping ISE Monitoring & Troubleshooting Log Processor...
ISE PassiveID Service is disabled
ISE pxGrid processes are disabled
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE EST Service...
ISE Sxp Engine Service is disabled
Stopping ISE Profiler Database...
Stopping ISE Indexing Engine...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE AD Connector...
Stopping ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler Database...
Starting ISE Application Server...
Starting ISE Indexing Engine...
Starting ISE Certificate Authority Service...
Starting ISE EST Service...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE AD Connector...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin(config-GigabitEthernet)#
```

Example 2 - Verify NIC Bonding Configuration

To verify if NIC bonding feature is configured, run the **show running-config** command from the Cisco ISE CLI. You will see an output similar to the following:

```
!
interface GigabitEthernet 0
  ipv6 address autoconfig
  ipv6 enable
  backup interface GigabitEthernet 1
  ip address 192.168.118.214 255.255.255.0
!
```

In the output above, "backup interface GigabitEthernet 1" indicates that NIC bonding is configured on Gigabit Ethernet 0, with Gigabit Ethernet 0 being the primary interface and Gigabit Ethernet 1 being the backup interface. Also, the ADE-OS configuration does not display an IP address on the backup interface in the running config, even though the primary and backup interfaces effectively have the same IP address.

You can also run the **show interfaces** command to see the bonded interfaces.

```
ise/admin# show interface
bond0: flags=5187<UP,BROADCAST,RUNNING,PRIMARY,MULTICAST>  mtu 1500
        inet 10.126.107.60  netmask 255.255.255.0  broadcast 10.126.107.255
        inet6 fe80::8a5a:92ff:fe88:4aea  prefixlen 64  scopeid 0x20<link>
        ether 88:5a:92:88:4a:ea  txqueuelen 0  (Ethernet)
        RX packets 1726027  bytes 307336369 (293.0 MiB)
        RX errors 0  dropped 844  overruns 0  frame 0
        TX packets 1295620  bytes 1073397536 (1023.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

GigabitEthernet 0
        flags=6211<UP,BROADCAST,RUNNING,SUBORDINATE,MULTICAST>  mtu 1500
        ether 88:5a:92:88:4a:ea  txqueuelen 1000  (Ethernet)
        RX packets 1726027  bytes 307336369 (293.0 MiB)
        RX errors 0  dropped 844  overruns 0  frame 0
        TX packets 1295620  bytes 1073397536 (1023.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0xfab00000-fabfffff

GigabitEthernet 1
        flags=6147<UP,BROADCAST,SUBORDINATE,MULTICAST>  mtu 1500
        ether 88:5a:92:88:4a:ea  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0xfaa00000-faafffff
```

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 sec

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 Pr when you use the **no** form of the **cdp run** command.
GigabitEthernet	(Optional). Specifies the GigabitEthernet interface on which to enable t Discovery Protocol.
0-3	Specifies the GigabitEthernet interface number on which to enable the 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 Discover 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)#
```

clock timezone

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

clock timezone *timezone*

Syntax Description

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

If you have the primary Administration node (PAN) auto-failover configuration enabled, disable it before you set the time zone. You can enable it after the time zone is set.

Command Default

Coordinated Universal Time (UTC)

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.
3.2	The no form of this command is no longer supported.

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.

If you have the PAN auto-failover configuration enabled in your deployment, the following message appears:

```
PAN Auto Failover is enabled, this operation is not
allowed! Please disable PAN Auto-failover first.
```

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 the PSN or MnT nodes of a Cisco ISE appliance after installation, causes some known issues with the sorting order of the live logs and live sessions pages. The old logs and sessions are not diplayed in the right sorting order based on timestamps. New sessions created after the time zone change are

sorted and displayed in the right order. ISE reports may also have data inconsistencies in the timestamp fields and incorrect sorting order.

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

name	Enter a name for the conn-limit you are configuring.
<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.
3.2	This command is updated to include assigning a name for the conn-limit configure.

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 lablimit 25000 ip 10.0.0.1 port 22
ise/admin(config)# end
ise/admin
```

service cache

To cache the DNS requests for hosts, use the **service cache enable** command in configuration mode. Enabling this feature will reduce the load on DNS server.

service cache enable hosts ttl *ttl*

To disable this feature, use the no form of this command.

Syntax Description

ttl	You can configure the Time to Live (TTL) value, in seconds, for a host in the cache while enabling the cache. There is no default setting for *ttl*. The valid range for *ttl* is from 1 to 2147483647.

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Usage Guidelines

TTL value is honored for negative responses. The TTL value set in the DNS server is honored for positive responses. If there is no TTL defined on the DNS server, then the TTL configured from the command is honored. Cache can be invalidated by disabling the feature.

Example

```
ise/admin(config)# service cache enable hosts ttl 10000
Enabling dns cache
ise/admin(config)# exit
```

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: Tab 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 back repository.
backup-logs	Performs a backup of all logs in the Cisco ISE server to a remote locati
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 exam backup and restore, configuration, copy, resource locking, file transfer, management.
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.

Command	Description
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.
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 ses
traceroute	Traces the route of a remote IP address.
undebug	Disables the output (display of errors or events) of the debug command for va 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 pron the network configuration, copies the running configuration to the startup configuration, displays the running configuration on the console. **Note** Cisco ISE Release 3.2 onwards, this command is modified to n longer support running-config and startup-config functions.

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 10.0.0.1
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 unders (_). 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. If Internal-CA
%           signed certs are being used, please regenerate ISE Root CA certificate.
%           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 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 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)#
```

identity-store

To join a CLI Administrator to an Active Directory domain, use the **identity-store** command in config mode. If the Cisco ISE node has joined multiple domains, you can only join one domain with this command. Each CLI Administrator joins individually. Please allow five minutes for Cisco ISE to complete the operation.

If the domain you join with this command is the same as the one that was joined to the ISE node, then you must rejoin the domain in the Administrators console. The Admin CLI user must be a Super Admin.

Command History

Release	Modification
2.6.0.156	This command was introduced.

Example

```
identity-store active-directory domain-name <aDomainFQDN> user <adUserNameWithJoinPrivs>
```

Note Active Directory CLI does not support authentication using child domain users. Child domain is considered as a separate domain which needs to be explicitly joined for its corresponding users to be used for authentication.

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

backup	Configures the NIC bonding feature to provide high availability for the phy interfaces.
do	EXEC command. Allows you to perform any EXEC commands in this mo
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 DHCPv 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.

Note The "no ip address" command is not applicable to the GigabitEthernet 0 interface. However, you can modify the IP address using the "ip address" command.

We do not recommend configuring two interfaces with the same subnet on Cisco ISE because of the difficulty in ascertaining the interface that will be used for data transmission.

Syntax Description

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

If you have the primary Administration node (PAN) auto-failover configuration enabled, disable it before you set the IP address. You can enable the PAN auto-failover configuration after the IP address is configured.

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.

If you have the PAN auto-failover configuration enabled in your deployment, the following message appears:

```
PAN Auto Failover is enabled, this operation is not
allowed! Please disable PAN Auto-failover first.
```

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*

Note Deleting the default gateway is not recommended since it is mandatory for packet traffic to go out of the system. You can enable the default gateway function on another interface instead. If you want to have a quad zero static route, it is recommended that you add that on an interface that is not configured as the 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
Adding/Changing gateway may cause ise services to restart.
Are you sure you want to proceed? Y/N [N]:
```

Note When you add or change the gateway, you must restart the services for the changes to take effect.

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 leas 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 certs were used on this node,
%           please import them with the correct domain name. If Internal-CA
%           signed certs are being used, please regenerate ISE Root CA certificate.
%           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.

If you have the Primary Administration Node (PAN) auto-failover configuration enabled, disable it before you change the host alias and FQDN of an ethernet interface. You can enable the PAN auto-failover configuration after the host alias and FQDN configuration is complete.

If you have the PAN auto-failover configuration enabled in your deployment, the following message appears:

```
PAN Auto Failover is enabled, this operation is
not allowed! Please disable PAN Auto-failover first.
```

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.

Note We recommend that you include the host alias in the **ip host** command for Cisco ISE 3.1 and later versions.

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 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 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 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 Processor...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin(config)#
```

ip mtu

To set the maximum transmission unit (MTU) size of IP packets sent and received on an interface, use the **ip mtu** command in the interface configuration mode. To restore the default MTU size, use the **no** form of this command.

ip mtu *bytes*

no ip mtu *bytes*

Syntax Description

mtu	Configures the MTU on a Cisco ISE interface.

Command Default

The MTU is set as 1500.

Command Modes

Interface configuration (config-GigabitEthernet)#

Command History

Release	Modification
2.4.0.357	This command was introduced.

Usage Guidelines

If an IP packet exceeds the MTU set for the interface, the Cisco ISE will fragment it. All devices on a physical medium must have the same protocol MTU in order to operate.

Example

The following example shows how to configure the MTU on an interface:

```
ise/admin(config)# int GigabitEthernet 1
ise/admin(config-GigabitEthernet)# ip mtu ?
<1280-9999>  Recommended range VM:1280-9216;appliance:1280-9999
```

The following example shows the output you can see after configuring the MTU.

```
ise/admin# show run | in mtu
ip mtu 1350
```

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 any combination of IPv4 and/or IPv6 addres
Ensure that the ISE eth0 interface is statically configured with
IPv6 address if you want to add a name-server with an IPv6 addr

If you have the primary Administration node (PAN) auto-failover configuration enabled in your deployment, remove it before you run the ip name-server command and enable it after you configure the DNS server(s).

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.

If you have the PAN auto-failover configuration enabled in your deployment, the following message appears:

```
PAN Auto Failover is enabled, this operation is not
allowed! Please disable PAN Auto-failover first.
```

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 10.0.0.1 10.0.1.1
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

To configure a static IPv6 address based on an IPv6 general prefix and enable IPv6 processing for an interface, use the **ipv6 address** command in interface configuration mode.

ipv6 address *ipv6-address/prefix-length*

To remove an IPv6 address or disable IPv6 processing, use the **no** form of this command.

no ipv6 address *ipv6-address/prefix-length*

Syntax Description

ipv6-address	IPv6 address.
prefix-length	The length of the IPv6 prefix. A decimal value between 0 and 128 that indi how many of the high-order contiguous bits of the address comprise the pr (the network portion of the address). A slash mark must precede the decim value.

If you have the Primary Administration Node (PAN) auto-failover configuration enabled, disable it before you set the IPv6 address. You can enable the PAN auto-failover configuration after the IPv6 address is configured.

If you have the PAN auto-failover configuration enabled in your deployment, the following message appears:

```
PAN Auto Failover is enabled, this operation is not
allowed! Please disable PAN Auto-failover first.
```

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

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

Using the fe80 prefix assigns a link-local address. Assigning a global address to the interface automatically creates a link-local address.

Note If 'Ctrl-C' is issued during the CLI configuration change of **ipv6 address** command, in case of IPv6 address change, the system may end up in a state where some application components have the old IPv6 address, and some components use the new IPv6 address.

This will bring the Cisco ISE node into a non-working state. The workaround for this is to issue another **ipv6 address** command to set the IPv6 address to the desired value.

Example 1

```
ise/admin(config)# interface GigabitEthernet 1
ise/admin(config-GigabitEthernet)# ipv6 address 2001:DB8:0:1::/64
Changing the IPv6 address may result in undesired side effects on any installed
application(s).
Are you sure you want to proceed? Y/N[N]: y
........
Note: ISE Processes are initializing. Use 'show application status ise' CLI to verify all
processes are in running state.
ise/admin(config-GigabitEthernet)#
```

Example 2

```
ise/admin(config)# interface GigabitEthernet 1
ise/admin(config-GigabitEthernet)# ipv6 address fe80::250:56ff:fe87:4763/64
ise/admin(config-GigabitEthernet)#
```

ipv6 address autoconfig

To enable automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface and enable IPv6 processing on the interface, use the **ipv6 address autoconfig** command in interface configuration mode.

IPv6 address autoconfiguration is enabled by default in Linux. Cisco ADE 2.0 shows the IPv6 address autoconfiguration in the running configuration for any interface that is enabled.

ipv6 address autoconfig

Use the **no** form of this command to disable autoconfiguration of IPv6 addresses from an 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

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
!
```

ipv6 enable

To enable IPv6 on an interface, use the **ipv6 enable** command in interface configuration mode.

ipv6 enable

Use the **no** form of this command to disable ipv6 on an interface.

no ipv6 enable

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

Use the **ipv6 enable** command to enable IPv6 on an interface and automatically generate the link-local address based on the interface MAC address.

Example 1

```
ise/admin(config)# interface GigabitEthernet 1
ise/admin(config-GigabitEthernet)# ipv6 enable
ise/admin(config-GigabitEthernet)#
```

Example 2

By default, ipv6 is enabled on all interfaces. If you want to disable it, use the **no** form of this command.

```
ise/admin# show interface gigabitEthernet 1
GigabitEthernet 1
flags=4163UP,BROADCAST,RUNNING,MULTICAST mtu 1500
inet6 fe80::20c:29ff:fe83:a610 prefixlen 64 scopeid 0x20 link
ether 00:0c:29:83:a6:10 txqueuelen 1000 (Ethernet)
RX packets 11766 bytes 1327285 (1.2 MiB)
RX errors 0 dropped 13365 overruns 0 frame 0
TX packets 6 bytes 508 (508.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0


ise/admin# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ise/admin(config)# interface gigabitEthernet 1
ise/admin(config-GigabitEthernet)# no ipv6 enable
ise/admin(config-GigabitEthernet)# exit
ise/admin(config)# end
ise/admin# show interface gigabitEthernet 1
GigabitEthernet 1
flags=4163 UP,BROADCAST,RUNNING,MULTICAST mtu 1500
ether 00:0c:29:83:a6:10 txqueuelen 1000 (Ethernet)
RX packets 64 bytes 5247 (5.1 KiB)
RX errors 0 dropped 13365 overruns 0 frame 0
TX packets 3 bytes 258 (258.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

ipv6 route

To manually configure IPv6 static routes and define an explicit path between two networking devices, use the **ipv6 route** command in global configuration mode. Static routes are not automatically updated and you must manually reconfigure the static routes if the network topology changes.

ipv6 route *ipv6-address/prefix-length* **gateway** *route-specific gateway*

To remove an IPv6 static route, use the **no** form of this command.

no ipv6 route *ipv6-address/prefix-length* **gateway** *route-specific gateway*

To configure a default static route with an IPv6 address, use the **ipv6 route ::/0 gateway** *route-specific gateway* command in global configuration mode. To disable the default static route with an IPv6 address, use the **no** form of this command.

Syntax Description

ipv6-address	IPv6 address.
prefix-length	The length of the IPv6 prefix. A decimal value between 0 and 128 that i how many of the high-order contiguous bits of the address comprise the (the network portion of the address). A slash mark must precede the dec value.
route-specific gateway	IPv6 address of the next hop that can be used to reach that network.

Command Default

No default behavior or values.

Command Modes

Global 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 **show ipv6 route** command to view the configured IPv6 routes.

Example 1

```
ise/admin(config)# ipv6 route 2001:DB8:cc00:1::/64 gateway 2001:DB8::cc00:1::1
```

Example 2

```
ise/admin(config)# ipv6 route ::/0 gateway 2001:db::5
```

where ::/0 indicates a default route prefix.

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. (S 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 t 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
end	Exits the kron-occurrence configuration submode and returns you to EXE
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- • policy-list—Specifies a policy list to be run by the occurrence. Sup 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 occurrenc configuration for the scheduled backup is removed after it

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 alphanum characters.
do	EXEC command. Allows you to perform any EXEC commands in this
end	Exits from the config-Policy List configuration submode and returns you t 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 (en 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)#
```

ntp

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

ntp authentication-key <*key id*> <*authentication key encryption type*> **hash** | **plain** <*key value*>

ntp maxdistance <*maximum distance*>

ntp reselectdistance <*reselect distance*>

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

no ntp server

Syntax Description

authentication-key	Specifies authentication keys for trusted time sources.
maxdistance	Maximum allowed root distance of the sources to not be rejected. By default maximum root distance configured in Cisco ISE is 16 seconds.
reselectdistance	Fixed distance for sources that are currently not selected. By default, the dist is 100 microseconds.
server	Specifies NTP server to use.

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 **authentication-key**, **maxdistance** and **server**. For example, if you previously issued the **ntp server** command, use the **no ntp** command with **server**.

Example

```
ise/admin(config)# ntp ?
  authentication-key  Authentication key for trusted time sources
  maxdistance         Maximum allowed root distance of the sources to not be rejected
  reselectdistance    Fixed distance for sources that are currently not selected
  server              Specify NTP server to use
ise/admin(config)#
ise/admin(config)# no ntp server
ise/admin(config)# do show ntp
% no NTP servers configured
ise/admin(config)#


ise/admin(config)# ntp reselectdistance ?
```

```
  <1-10000000>  Reselect distance in microseconds
ise/admin(config)# ntp reselectdistance 3000
```

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*

ntp authentication-key <*key id*> **sha1 hash | plain** *key value*

ntp authentication-key <*key id*> **sha256 hash | plain** *key value*

ntp authentication-key <*key id*> **sha512 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 1–65535.
md5	The encryption type for the authentication key.
sha1	The encryption type for the authentication key.
sha256	The encryption type for the authentication key.
sha512	The encryption type for the authentication key.
hash	Hashed key for authentication. Specifies an encrypted (hashed) key that fol the encryption type. Supports up to 4112 length.
plain	Plaintext key for authentication. Specifies an unencrypted plaintext key tha follows the encryption type. Supports up to 1028 length.
key value	The key value in the format matching either <*authentication key encryptio type*>**plain** | **hash**, above. **Note** Hex key value can be added with the prefix **HEX:**. To create a *key value* for NTP authentication with the exclama symbol (!), you must first enter the backslash symbol (\), for example, **abc\!23**.

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     MD5 authentication
  sha1    SHA1 authentication
  sha256  SHA256 authentication
  sha512  SHA512 authentication
```

Example 2

```
ise/admin# configure
ise/admin(config)#
ise/admin(config)# ntp authentication-key 1 sha1 plain ?
  <WORD>  Plain text or hexadecimal number with the HEX: prefix key for a (Max Size - 1028)
```

Example 3

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

Example 4

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

ntp maxdistance

The **ntp maxdistance** command sets the maximum allowed root distance of the sources to not be rejected by the source selection algorithm. The distance includes the accumulated dispersion, which might be large when the source is no longer synchronised, and half of the total round-trip delay to the primary source.

By default, the maximum root distance configured in Cisco ISE is 16 seconds.

To reset to the default value, use the **no** form of this command.

ntp maxdistance

Syntax Description

maxdistance	Maximum allowed root distance of the sources to not be rejected.

Command Default

None

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

Setting **maxdistance** to a larger value can be useful to allow synchronisation with a server that only has a very infrequent connection to its sources and can accumulate a large dispersion between updates of its clock.

Example

```
ise/admin(config)# ntp maxdistance ?
     <1-128>
```

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*} **minpoll** <*minimum poll*> **key**<*peer key number*>

ntp server {*ip-address* | *hostname*} **trust**

Syntax Description

server	Allows the system to synchronize with a specified server.
ip-address | *hostname*	IPv4 or IPv6 address or hostname of the server providing the clock synchronization. Arguments are limited to 255 alphanumeric characters that the ISE eth0 interface is statically configured with an IPv6 address want to add an NTP server with an IPv6 address.
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. For authentication to work, the key and the key value should be the sam which is defined on the actual NTP server.
minpoll	Minimum interval between requests sent to the server as a power of 2 in s For example, **minpoll 5** would mean that the polling interval should no below 32 seconds. The default is 6 (64 seconds), the minimum is -6 (1/6 second), and the maximum is 24 (6 months).
trust	Assume time from this source is always true.

Note *key* and **minpoll** options can be interchanged.

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

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.

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

Example

```
ise/admin# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ise/admin(config)# ntp server 209.165.200.225 ?
  key            Peer key number
  minpoll        Minimum interval between requests sent to the server
trust        Assume time from this source is always true


ise/admin# show running-config
interface GigabitEthernet 0
  ip address 209.165.200.225 255.255.255.0
  ipv6 address autoconfig
  ipv6 enable
!
ip name-server 209.165.200.226
!
ip default-gateway 209.165.200.227
!
ip route 2.2.2.0 255.255.255.0 gateway 127.0.0.1
!
!
clock timezone Asia/Kolkata
!
ntp authentication-key nn md5 hash xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

ntp server 209.165.200.228 key nn
ntp server 209.165.200.229
!


ise/admin(config)# ntp server 209.165.200.225 trust
ise/admin(config)# ntp server 209.165.200.225 key 2 trust
ise/admin(config)# ntp server 209.165.200.225 key 2 minpoll 7 trust
ise/admin(config)# ntp server 209.165.200.225 minpoll 7 trust
ise/admin(config)# ntp server 209.165.200.225 minpoll 7 key 2 trust
```

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#
```

rate-limit

To configure the limit of TCP, UDP, or 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 name 250 ip-address net-mask port

Syntax Description

name	A name for the rate limit that you are configuring.
<1-10000>	An average number of TCP, UDP, or ICMP packets per second.
ip-address ***ip*** or ***ipv6***	The source IP address to which the packet rate limit must be applied. Enter for IPv4 addresses and **ipv6** for IPv6 addresses.
net-mask	The source IP mask to which the packet rate limit must be applied.
port	The destination port number to which the packet rate limit must be applied.

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.
3.2	The rate-limit CLI responses no longer display the rounded off rate limit va However, Netfilter continues to round off the rate limit value in implementa

Usage Guidelines

The actual rate limit that is set may differ from the number that you have configured due to the design of the netfilter hashlimit. The following is a list of how netfilter rounds off rate limit values, at the time of writing this document:

- For limit values from 5001/s to 10000/s, Netfilter rounds up the value to 10000/s.
- For limit values from 3334/s to 5000/s, Netfilter rounds up the value to 5000/s.
- For limit values from 2501/s to 3333/s, Netfilter rounds up the value to 3333/s.
- For limit values from 2001/s to 2500/s, Netfilter rounds up the value to 2500/s.
- For limit values from 1667/s to 2000/s, Netfilter rounds up the value to 2000/s.
- For limit values from 1429/s to 1666/s, Netfilter rounds up the value to 1666/s.
- For limit values from 1251/s to 1428/s, Netfilter rounds up the value to 1428/s.
- For limit values from 1112/s to 1250/s, Netfilter rounds up the value to 1250/s.
- For limit values from 1001/s to 1111/s, Netfilter rounds up the value to 1111/s.

- For limit values from 910/s to 1000/s, Netfilter rounds up the value to 1000/s.
- For limit values from 834/s to 909/s, Netfilter rounds up the value to 909/s.
- For limit values under 150, no rounding is done.

See netfilter documentation for more details on how hashlimits work.

To update the assigned values for a rate limit name, use the no form of the rate-limit command and then redefine the rate limit.

Example

```
ise242/admin(config)#rate-limit limit1 5500 port 6543
ise242/admin(config)#do show running-config | include rate
rate-limit limit1 5500 port 6543
```

password-policy

Note You can also configure the password policy from the Cisco ISE GUI. Note that if a password policy is configured through the Cisco ISE GUI, it overwrites and takes precedence over any password policy configured through the Cisco ISE CLI.

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 passw
disable-repeat-chars	Disables the ability of the password to contain more than four identical charac
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 charac
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 the other password-expiration commands.
password-expiration-warning	Number of days before expiration that warnings of impending expiratio 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 integ 20.
password-lock-timeout	Sets the time in minutes after which the account lockout is cleared. Suppo 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 th 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 Ta 4-5).
user	Configure the username and password for access. Supports up to 30 alphanun characters for username and supports 15 alphanumeric characters for passw Passwords can consist of the following characters: 0 through 9, a through z through Z, -, ., |, @, #, $, %, ^, &, *, (,), +, and =. **Note** The hash value of the repository password will be displayed as asterisks in the running configuration.

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. Suppo 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 th repository. **Note** All local repositories are created on the /localdisk partition you specify disk:// in the repository URL, the system creat directories in a path that is relative to /localdisk. For examp you entered **disk://backup,** the directory is created at /localdisk/backup.
ftp:	Source or destination URL for an FTP network server. Use url ftp://serv
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://serv
sftp:	Source or destination URL for an SFTP network server. Use url sftp://serv
tftp:	Source or destination URL for a TFTP network server. Use url tftp://serv **Note** You cannot use a TFTP repository for performing a Cisco I 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.

Usage Guidelines

When configuring **url sftp:** in the submode, you must first load the RSA fingerprint (AKA host-key) from the target SFTP host into ISE. You can do this by using the **crypto host_key add** command through the CLI. See the crypto command for more information.

To disable this function, use the command **crypto host_key delete** in the EXEC mode.

Cisco ISE displays the following warning when you configure a secure ftp repository in the Cisco ISE Admin portal in Administration > System > Maintenance > Repository > Add Repository.

The host key of the SFTP server must be added through the CLI by using the host-key option before this repository can be used.

A corresponding error is thrown in the Cisco ADE logs when you try to back up into a secure FTP repository without configuring the host-key.

Note Cisco ISE initiates outbound SSH or SFTP connections in FIPS mode even if FIPS mode is not enabled on ISE. Ensure that the remote SSH or SFTP servers that communicate with ISE allow FIPS 140-2 approved cryptographic algorithms.

Cisco ISE uses embedded FIPS 140-2 validated cryptographic modules. For details of the FIPS compliance claims, see the FIPS Compliance Letter.

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.
encryption-algorithm	Configures SSH encryption algorithms. The supported algorithms are a aes128-cbc, aes128-ctr, aes256-cbc, and aes256-ctr.
encryption-mode	Configures SSH encryption mode on system. The supported modes are ctr.
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
PubkeyAuthentication	Specifies that user authentication should take place using private key of **Note** Do not execute the command **service sshd PubkeyAuthent** if you haven't included the public key in the ZTP configura image file before installation. This disables password-base authentication and Cisco ISE will expect you to login using a key. If you do run into this issue, you need to use the conso to login into Cisco ISE and revert the configuration.

Command Default

No default behavior or values.

Command Modes Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.
3.2	**PubkeyAuthentication** keyword was added.

Usage Guidelines None.

Example

```
ise/admin(config)# service sshd
ise/admin(config)# service sshd enable
ise/admin(config)# service sshd encryption-algorithm
 Configure aes128-cbc algo
 Configure aes128-ctr algo
 Configure aes256-cbc algo
 Configure aes256-ctr algo
ise/admin(config)# service sshd encryption-mode
 Configure cbc cipher suites
 Configure ctr cipher suites
ise/admin(config)# service sshd key-exchange-algorithm diffie-hellman-group14-sha1
ise/admin(config)# service sshd loglevel 4
ise/admin(config)#
```

```
ise/admin(config)# service sshd
ise/admin(config)# service sshd enable
ise/admin(config)# service sshd encryption-algorithm
 Configure aes128-cbc algo
 Configure aes128-ctr algo
 Configure aes256-cbc algo
 Configure aes256-ctr algo
ise/admin(config)# service sshd encryption-mode
 Configure cbc cipher suites
 Configure ctr cipher suites
ise/admin(config)# service sshd key-exchange-algorithm diffie-hellman-group14-sha1
ise/admin(config)# service sshd loglevel 4
ise/admin(config)#
```

To enable public key authentication:

```
ise/admin(config)# service sshd PubkeyAuthentication
```

To disable public key authentication:

```
ise/admin(config)# no service sshd PubkeyAuthentication
```

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 enable

To enable the SNMP server on Cisco ISE, use the **snmp-server enable** command in global configuration mode.

snmp-server enable

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

Command Default

The SNMP server is enabled.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Example

```
ise/admin(config)# snmp-server enable
ise/admin(config)#
```

MIBs

The SNMP agent on the Cisco ISE provides read-only access to the following MIBs for all versions of SNMP:

- 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

You can query for the system object identifiers for SNS devices. The system object identifier for ISE 3315 is the default value displayed if a new device series has been introduced but is not updated in Cisco ISE release and patch releases.

For example:

```
ise/admin(config)# snmpwalk -v 2c -c snmpV2cCommunityString iseFQDN-or-IP
SNMPv2-MIB::sysObjectID.0SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.1426


Appliances  |  SysObjID
- - - - - - - - - - - - - - - - - - -
ISE 3315    | 1.3.6.1.4.1.9.1.1423
ISE 3395    | 1.3.6.1.4.1.9.1.1424
ISE 3355    | 1.3.6.1.4.1.9.1.1425
SNS 3495    | 1.3.6.1.4.1.9.1.2139
SNS 3415    | 1.3.6.1.4.1.9.1.2140
SNS 3595    | 1.3.6.1.4.1.9.1.2266
SNS 3515    | 1.3.6.1.4.1.9.1.2265
SNS 3615    | 1.3.6.1.4.1.9.1.2784
SNS 3655    | 1.3.6.1.4.1.9.1.2785
SNS 3695    | 1.3.6.1.4.1.9.1.2786
SNS 3715    | 1.3.6.1.4.1.9.1.3270
SNS 3755    | 1.3.6.1.4.1.9.1.3271
SNS 3795    | 1.3.6.1.4.1.9.1.3272
VM          | 1.3.6.1.4.1.9.1.1426
```

snmp-server user

To configure a new SNMP user, use the **snmp-server user** command in global configuration mode.

snmp-server user *username* **v3 sha1**{**hash** | **plain**} *auth-password priv-password*

snmp-server user *username* **v3 sha224**{**hash** | **plain**} *auth-password priv-password*

snmp-server user *username* **v3 sha256**{**hash** | **plain**} *auth-password priv-password*

snmp-server user *username* **v3 sha384**{**hash** | **plain**} *auth-password priv-password*

snmp-server user *username* **v3 sha512**{**hash** | **plain**} *auth-password priv-password*

Note This command must be used only for SNMP version 3.

To remove a specified SNMP user, use the **no** form of this command.

Syntax Description

user	Configure a new user.
username	The name of the user on the host that belongs to the SNMP agent.
v3	Version of the SNMP used to send the traps. Specifies that the SNMP Version 3 security model should be used for enabl the priv and the auth keywords.
auth-password	Specifies the authentication user password. The minimum length for a passv is one character; however, we recommend that you use at least nine charact for security . To create a password with the hash symbol (#) or exclamation mark (!), you first enter the backslash symbol (\), for example, **abc\!23**, **abc12\#**, and so **Note** If you forget a password, you cannot recover it, and must reconfig the user. You can specify a plain-text password or a localized dig The localized digest must match the authentication algorithm selected for the user, which can be either MD5 or SHA. When user configuration is displayed on the console or is written to a (for example, the startup-configuration file), the localized authentication and privacy digests are always displayed instead the plain-text password.

priv-password	Specifies the encryption user password. The minimum length for a pass one character; however, we recommend that you use at least eight chara security. To create a password with the hash symbol (#) or exclamation mark (!), y first enter the backslash symbol (\), for example, **abc\!23**, **abc12\#**, and **Note** If you forget a password, you cannot recover it, and must reco the user. You can specify a plain-text password or a localized The localized digest must match the authentication algorith selected for the user, which can be either MD5 or SHA. W user configuration is displayed on the console or is written (for example, the startup-configuration file), the localized authentication and privacy digests are always displayed ins the plain-text password.
sha1	Sha1 authentication type.
sha224	Sha224 authentication type.
sha256	Sha256 authentication type.
sha384	Sha384 authentication type.
sha512	Sha512 authentication type.
{**hash** | **plain**}	Password is in encrypted or plain format. Encrypted passwords must be hexadecimal format.

Command Default

Disabled.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

After you configure users, make sure to configure SNMP Version 3 hosts. Along with the target IP address, you must configure a username, because traps are only sent to a configured user.

Example

```
ise/admin(config)# snmp-server user testuser v3 ?
   hash   Hash Passwords
   plain  Plain Passwords
   sha1   Sha1 authentication
   sha224 Sha224 authentication
   sha256 Sha256 authentication
   sha384 Sha384 authentication
   sha512 Sha512 authentication

ise/admin(config)# snmp-server user testuser v3 hash authpassword privpassword
```

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

snmp-server host

To send SNMP traps to a recipient, use the **snmp-server host** command in configuration mode. By default, SNMP traps are enabled. By default, the UDP port is 162.

Note SNMP user needs to be created before using the `snmp-server host` command.

snmp-server host {*ip-address* | *hostname*} **version** {{*1* | *2c*} *community* | *3 username engine_ID* {**hash** | **plain**} *auth-password priv-password*}

snmp-server host {*ip-address* | *hostname*} **version** {{*1* | *2c*} *community* | *3 username engine_ID* **sha1** {**hash** | **plain**} *auth-password priv-password*}

snmp-server host {*ip-address* | *hostname*} **version** {{*1* | *2c*} *community* | *3 username engine_ID* **sha224** {**hash** | **plain**} *auth-password priv-password*}

snmp-server host {*ip-address* | *hostname*} **version** {{*1* | *2c*} *community* | *3 username engine_ID* **sha256** {**hash** | **plain**} *auth-password priv-password*}

snmp-server host {*ip-address* | *hostname*} **version** {{*1* | *2c*} *community* | *3 username engine_ID* **sha384** {**hash** | **plain**} *auth-password priv-password*}

snmp-server host {*ip-address* | *hostname*} **version** {{*1* | *2c*} *community* | *3 username engine_ID* **sha512** {**hash** | **plain**} *auth-password priv-password*}

To remove trap forwarding, use the **no** form of this command.

Note When SNMP Version 3 hosts are configured in Cisco ISE, a user must be associated with that host because traps are sent only to a configured user. To receive traps, after you have added the **snmp-server host** command, you must configure the user credentials on the NMS with the same credentials as those configured in Cisco ISE.

Syntax Description

host	Configures hosts to receive SNMP notifications.
ip-address	IP address of the SNMP notification host. Supports up to 32 alphanume characters.
hostname	Name of the SNMP notification host. Supports up to 32 alphanumeric ch
version {*1* | *2c* | *3*}	(Optional). Version of the SNMP used to send the traps. Default = 1. If you use the version keyword, specify one of the following keywords: • 1—SNMPv1. • 2c—SNMPv2C. • 3—SNMP v3.

community	Specifies the shared secret key between Cisco ISE and the NMS. Case-sens value that can be up to 32 characters in length. Spaces are not allowed. The de community-string is "public." Cisco ISE users this key to determine whethe incoming SNMP request is valid.
username	(Optional; required only if you choose SNMP version 3) Associates a user the host when SNMP Version 3 hosts are configured in Cisco ISE.
engine_ID	(Optional; required only if you choose SNMP version 3) Remote EngineID
auth-password	(Optional; required only if you choose SNMP version 3) Specifies the authentication user password.
priv-password	(Optional; required only if you choose SNMP version 3) Specifies the encryp user password.
sha1	Sha1 authentication type.
sha224	Sha224 authentication type.
sha256	Sha256 authentication type.
sha384	Sha384 authentication type.
sha512	Sha512 authentication type.

Command Default

Enabled.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

Cisco ISE sends a 'coldStart(0)' trap when the appliance boots up (reloads), if SNMP is already configured. Cisco ISE uses the Net-SNMP client that sends a 'coldStart(0)' trap when it first starts up, and an enterprise-specific trap 'nsNotifyShutdown' when it stops.

It generates an enterprise-specific trap 'nsNotifyRestart' (rather than the standard 'coldStart(0)' or 'warmStart(1)' traps) typically after you reconfigure SNMP using the **snmp-server host** command.

Note If the SNMP trap target is specified by hostname or FQDN and resolved by DNS to both IPv4 and IPv6 addresses, ISE sends SNMP traps to IPv6 dual-stack target receivers through IPv4 and not through IPv6. To ensure that the traps are sent through IPv6, an ISE admin may either resolve hostname or FQDN only to IPv6 by DNS, or specify the IPv6 address directly, when configuring SNMP traps.

Examples

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

```
ise/admin(config)# snmp-server host 209.165.202.129 version 1 password
ise/admin(config)#


ise/admin(config)# snmp-server host ise1 version 2c public
ise/admin(config)# snmp-server community public ro
2012-09-24T18:37:59.263276+00:00 ise1 snmptrapd[29534]: ise1.cisco.com [UDP:
[192.168.118.108]:44474]: Trap ,
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (29) 0:00:00.29, SNMPv2-MIB::snmpTrapOID.0
 = OID: SNMPv2-MIB::coldStart,
SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
ise/admin(config)# snmp-server contact admin@cisco.com
2012-09-24T18:43:32.094128+00:00 ise1 snmptrapd[29534]: ise1.cisco.com [UDP:
[192.168.118.108]:53816]: Trap ,
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (33311) 0:05:33.11, SNMPv2-MIB::snmpTrapOID.0
 = OID: NET-SNMP-AGENT-MIB::nsNotifyRestart, SNMPv2-MIB::snmpTrapEnterprise.0 = OID:
NET-SNMP-MIB::netSnmpNotificationPrefix


ise/admin(config)# snmp-server host a.b.c.d version 3 testuser 0x12439343 hash authpassword
 privpassword
ise/admin(config)#


ise/admin(config)# snmp-server host a.b.c.d version 3 testuser 0x12439343 ?
   hash   Hash Passwords
   plain  Plain Passwords
   sha1   Sha1 authentication
   sha224 Sha224 authentication
   sha256 Sha256 authentication
   sha384 Sha384 authentication
   sha512 Sha512 authentication
```

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 SN No blank spaces allowed. Supports up to 255 alphanumeric characters. To c a community string with the exclamation symbol (!), you must first enter th backslash symbol (\), for example, **abc\!23**.
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.

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. Suppo 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. Suppo 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)#
```

snmp-server trap dskThresholdLimit

To configure the SNMP server to receive traps if one of the Cisco ISE partitions reaches its threshold disk utilization limit, use the **snmp-server trap dskThresholdLimit** command in Configuration mode.

snmp-server trap dskThresholdLimit *value*

To stop sending disk threshold utilization limit traps, use the **no** form of this command.

Syntax Description

value	Number that represents the percentage of available disk space. The valu from 1 to 100.

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.1.0.474	This command was introduced.

Usage Guidelines

This configuration is common for all the partitions in Cisco ISE. If you configure the threshold limit as 40, then you will receive a trap as soon as a partition utilizes 60% of its disk space and only 40% of the disk space is available. That is, a trap is sent when the configured amount of free space is reached.

After you configure this command from the Cisco ISE CLI, a kron job runs every five minutes and monitors the Cisco ISE partitions one by one. If any one of the partitions reaches its threshold limit, then Cisco ISE sends a trap to the configured SNMP server with the disk path and the threshold limit value. Multiple traps are sent if multiple partitions reached the threshold limit. You can view the SNMP traps using the traps receiver in a MIB browser.

Example

```
ise/admin(config)# snmp-server trap dskThresholdLimit 40
ise/admin(config)#
```

snmp engineid

To change the existing engine ID to a new value, use the **snmp engineid command** in configuration mode. This command displays a warning that all existing users need to be re-created.

snmp engineid *engine_ID_string*

To remove the configured engine ID, use the **no** form of this command.

Syntax Description

engineid	Changes an existing engine ID to a new value that you specify.
engine_ID_string	String of maximum 24 characters that identifies the engine ID.

Command Default

No command defaults.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Example

```
ise/admin(config)# snmp engineid Abcdef129084B
% Warning: As a result of engineID change, all SNMP users will need
           to be recreated.
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 allowed per second.
?	The valid range is from 1 to 2147483647.

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.
3.2	The running-config response for synflood-limit no longer displays the r off limit value. However, synflood limits continue to be rounded off in implementation.

Usage Guidelines

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

The actual rate limit that is set may differ from the number that you have configured due to the design of the synflood limits. The following is a list of how limit values are rounded up, at the time of writing this document:

- For limit values from 5001/s to 10000/s, the value is rounded up to 10000/s.
- For limit values from 3334/s to 5000/s, the value is rounded up to 5000/s.
- For limit values from 2501/s to 3333/s, the value is rounded up to 3333/s.
- For limit values from 2001/s to 2500/s, the value is rounded up to 2500/s.
- For limit values from 1667/s to 2000/s, the value is rounded up to 2000/s.
- For limit values from 1429/s to 1666/s, the value is rounded up to 1666/s.
- For limit values from 1251/s to 1428/s, the value is rounded up to 1428/s.
- For limit values from 1112/s to 1250/s, the value is rounded up to 1250/s.
- For limit values from 1001/s to 1111/s, the value is rounded up to 1111/s.
- For limit values from 910/s to 1000/s, the value is rounded up to 1000/s.
- For limit values from 834/s to 909/s, the value is rounded up to 909/s.
- For limit values under 150, no rounding is done.

Example

```
ise49/admin(config)# synflood-limit 5099
ise49/admin(config)# do show running-config | include syn
synflood limit 5099
```

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 (“) are not allowed. Supports up to 31 alphanumeric characters.
password	Specifies password.
password	Password character length up to 40 alphanumeric characters. You must 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)#
```

Additional References

See Cisco ISE End-User Resources for additional resources that you can use when working with Cisco ISE:.